KPMG

Global Resilience Federation

MFG-ISAC
Manufacturing Information Sharing and Analysis Center

The criticality of CPG

A guide for consumer packaged goods CISOs in the face of increased security threats to the supply chain

October 2022

kpmg.com

Table of contents

Introduction

Toilet paper. Disinfectant wipes. Ketchup packets. Grape Nuts. Pet food. Baby formula. At various points throughout the pandemic, consumer reaction to shortages of consumer-packaged goods (CPG) such as these has ranged from annoyance to deep inconvenience to true hardship. It's clear that, during the past two and half years, CPG companies have in many ways become part of the critical infrastructure. Consider the following:

- In 2020, demand for cream cheese rose 18 percent.[i] So when cream cheese plants and distribution centers were hit with cyber-attacks during the holiday season, the resulting shortages had an emotional impact on those who were taking comfort by baking at home instead of attending holiday parties and family gatherings.
- To make isolation more palatable, many people adopted pets for the first time in 2020: the number of dog and cat adoptions rose around 40 percent that year,[ii] while pet food sales rose 6.9 percent between late 2020 and late 2021.[iii] So when supply chain disruptions caused a shortage of certain pet food brands, more owners than ever had to face the inconvenience of putting their pets through an abrupt change in diet.
- While a lack of Grape Nuts may not seem like a hardship, for those who eat the iron-rich cereal to counter anemia, the shortages last year amounted to a not insignificant health issue.[iv] Some consumers were so desperate for the cereal that they were willing to pay up to $110 a box.[v]
- And finally, while perhaps not as life-sustaining as prescription drugs or medical devices, some consumer-packaged goods (CPG) come close. Take baby formula: The current shortage of a critical source of nutrition for babies in the first year of life[vi] is causing not only severe stress and anxiety among new parents, but also putting babies at risk of failure to thrive.

"Consumer packaged goods have become an integral part of protecting the health and safety of the country, which means that real care has to be taken to protect the supply chain from cyber-attacks and other disruptions," said Andrew Stanley, Chief Information Security Officer (CISO) & VP Global Digital Operations, Mars, Incorporated, one of the world's leading CPG companies. "Regardless of what kind of nutrition is in question, CPG companies maintain hygiene, nutrition, hydration, pet health and safety, and first aid. These are not luxuries or indulgences; they are real, baseline needs."

Cyber-criminals seek to disrupt daily life

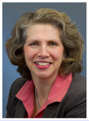
As it became clear that CPG shortages could cause consumers significant stress, the sector has become more of a target for cyber-criminals, many of whom seek to disrupt daily life. Consider that, in the second quarter of 2020, 33 percent of all cyber-events occurred in the manufacturing sector. And, of those, 28 percent were small businesses.[vii]

It is worth noting that the CPG supply chain for many food products can be more complex than the supply chains in other industries. The food supply chain includes a wide variety of third-party suppliers (many of them farmers), product delivery, food processing/manufacturing, and then a complex web of distribution avenues to get products into the hands of supermarkets and consumers. Each stage of this chain represents a potential vector for cybercrime.

According to Martin Bally, CISO at Campbell Soup Company: "Cyber-attacks on consumer-packaged goods companies have the potential to cause massive disruption. Given the essential nature of our sector, limiting interruptions to the food supply has become part of our mandate."

"Since water and food are part of Maslow's Hierarchy of Needs, the idea that those might be in jeopardy made people uncomfortable during the pandemic in unprecedented ways," said Marene Alison, CISO, J&J. "Over time, I think consumers will have more brand loyalty to those CPG companies that didn't let them down during COVID. CPG companies need to understand the importance of different products and brands to consumers and treat those products like their crown jewels."

> "You can't put an exact value on reliability in times of crisis, but it certainly drives brand loyalty."
>
> \- **Marene Alison,**
> CISO, J&J



Although some consumers are trading down from brand-name CPG products to store brands, many have a strong emotional connection to their preferred products and brands. Those CPG companies that can avert the prolonged shortages that can stem from a cyber-attack will be less vulnerable to lower-priced competitors.

The CISO's role evolves

In the past, CISOs at CPG companies were focused on defensive measures to ward off or respond to potential hacking. Today, given how integral cybersecurity is to protecting companies' most popular brands, the role of the CISO and cybersecurity team has shifted to be much more integrally bound to the business.

The reporting structure for CISOs varies widely across the CPG industry. CISOs can report to the CIO, CTO, COO, Chief Legal officer, Enterprise Risk Management, and others. According to Campbell Soup Company's CISO Martin Bally, who currently reports to the CTIO, "I believe the CISO and the cybersecurity team can be successful with any structure, as long as the team has the robust support from and visibility with the executive leadership team and the board. Conversely, if you get buried under infrastructure or somewhere else in IT, cybersecurity could be overlooked or wrongly classified as a pure IT problem."

"Our roles have evolved from being more of a shared service to be consulted in times of crisis, to having a seat at the table with responsibility for helping to bring value to the company and generate revenue," says Andrew Stanley of Mars. "We are viewed similarly to the CIO now. So, we have to understand how the business works and have more of an entrepreneurial perspective."

What are some ways that leading CISOs get the business to align with their way of thinking?

- Translate the risk landscape into a business context, i.e., speak to them in laymen's terms, be a good storyteller, and use analogies that make sense, all while stressing how cybersecurity is integral to the company's growth.
- Market the security organization internally by communicating across platforms with messaging around what's going on in the industry, weekly updates on global issues like the Russia-Ukraine war, etc.
- Solicit opinions and feedback from the business on issues like the reporting structure to give corporate leaders a much stronger sense of ownership of cyber issues and, in an ideal world, encourage them to champion cyber principles throughout the company.
- Remain flexible – sometimes the business needs to take the lead with cyber, and sometimes it's the opposite.

Marene Alison of J&J expands on this idea, stressing the importance of communication: "It is critical to have a cybersecurity leader who can communicate well and articulate risks to the business in ways they can understand and appreciate. For example, if senior executives appreciate that a cyber-attack can truly hinder their ability to manufacture and ship products, they will be much more likely to work with us hand in hand."

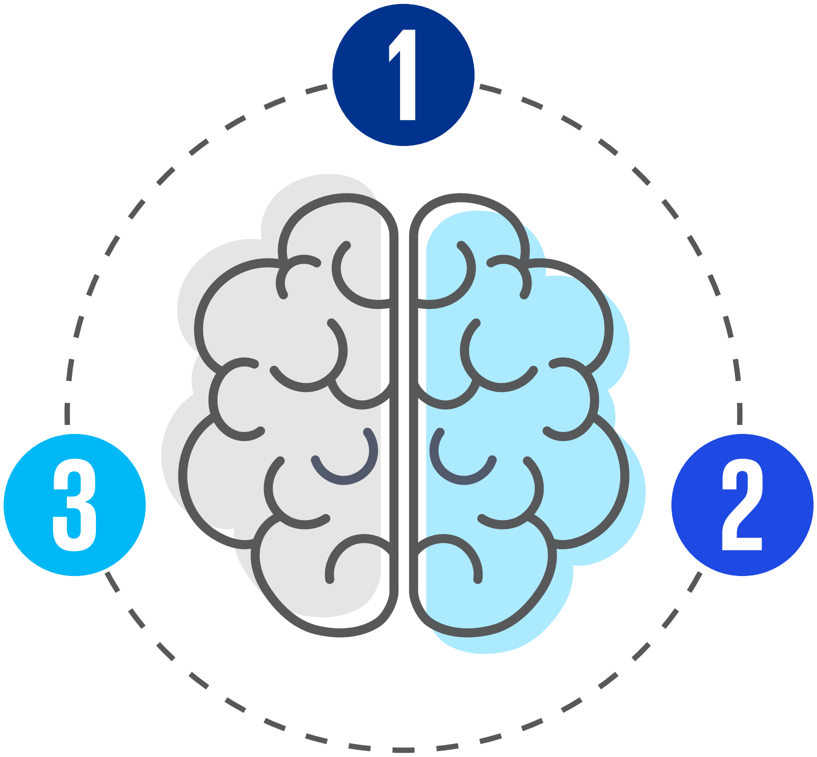
> "In CPG, as long as the company is focused on transformation, the CISO and the cybersecurity function will be prioritized."
>
> - **Martin Bally,**
> VP & CISO,
> Campbell Soup Company

Top three threats on CPG CISOs' minds

The issues affecting availability in the CPG industry are as widespread and differentiated as they come—with current threats ranging from geopolitical instability, to supply chain disruptions, to the energy crisis in Europe, to demands for ransomware from both domestic threat actors and hostile nation states. [For more on this, see our companion publication, "The Practitioners' Guide to Securing the CPG Supply Chain."]

Although the most acute security threats are constantly evolving, there are some risks that are more likely to keep CISOs up at night. Here are the top three cited by the CISOs interviewed for this paper: (1) Although cyber-criminals are, of course, targeting CPG companies directly, the sheer breadth of third-party suppliers makes it more likely that threat actors will target these smaller, more vulnerable suppliers first. (2) Although there are certainly CPG companies that refuse to do business with suppliers in volatile regions or in countries that were less than reliable during the pandemic, for those companies that continue to do so, flexibility and readiness to pivot their supply strategies are critical. (3)The CPG industry is unique in that it has a mix of outdated legacy technology and cutting-edge technologies that foster connectivity between disparate nodes in the supply chain. Even as companies move toward integration between IT and OT and the real-time insights this fosters, the way CPG technology stacks are structured means than cyber-criminals have a wealth of attack vectors to exploit.

Internal teams taxed by range of third-party suppliers



Gaps in the technology stack open attack vectors

Geopolitical disruption threatens supplier reliability

1. Internal teams taxed by range of third-party suppliers

> If a transportation provider goes offline, it can disrupt our ability to ship our products. This is a nexus point that is largely underappreciated.
>
> \- **Andrew Stanley,** CISO & VP Global Digital Operations, Mars, Incorporated

Consumer packaged goods (CPG) companies need to prioritize continuous operations so they can meet the production demands of their target customers. In a time that consumer packaged goods are considered more of a critical infrastructure component than ever, CPG companies must ensure the availability of not only their own corporate IT and site-specific OT, but also that of their key suppliers.

An overview of potential attack vectors includes: the Internet of things and GPS technologies farmers are using in the field to control irrigation and fertilizing systems and, thereby, optimize their output; the Industrial Internet of Things (IIoT) technologies employed in production, warehousing, and transportation to increase efficiency; possible introduction of malware at labs and third-party logistics companies due to insufficient staff training; and, of course, ransomware attacks at any type of supplier, direct or indirect. Such threats could waylay the transportation of materials and ingredients from suppliers to manufacturers, delay shipments to customers, re-route deliveries to the wrong locations, or jeopardize the safety of food and beverage products.

Complicating matters is the fact that, from initial vendor selection to internal and external assessments to continuous monitoring, it isn't possible for any CPG company to stay abreast of the cyber posture of all their vendors. Having a myopic focus on only the largest and niche vendors can leave the critical middle layer largely unprotected. And as new products are introduced, long-term suppliers may become more, or less, critical than they had been in the past. "Even with a growing number of suppliers, many cybersecurity functions have to do more with less," says Mike Wagner, Designate CISO for J&J's planned New Consumer Health Company. "For example, we are looking to automate more of the vendor selection and assessment processes. With our traditional manual survey process, the responses simply don't come back as quickly as the business wants to do a deal."

Key messages for the business: For the cybersecurity function to prioritize vendor assessments and continuous monitoring, it is critical to have visibility into business priorities, upcoming projects in the pipeline, and the vendors the business views as most critical to manufacturing its most lucrative products. In turn, cybersecurity can help the business prioritize by illustrating the business impacts of disruptions in particular suppliers' operations.

[For more, see "Segment and prioritize suppliers," page 9.]

2. Geopolitical disruption threatens supplier reliability

If it wasn't clear already, the pandemic underlined the interdependencies of countries across the globe. Perhaps the most salient example was the supply chain disruption experienced by U.S. pharmaceutical companies when China and India stockpiled certain ingredients that were critical to manufacturing life-saving drugs.

When it comes to CPG companies, the geopolitical situation in other parts of the world—from the Russia-Ukraine war, to the European energy crisis—is raising the specter of a whole new host of nation-state-based cyber-attacks.

For CPG companies, responses and/or remediation must be immediate in the aftermath of a cyber-attack, or there will be a significant risk of spoilage of food in production. On the other hand, shifting relationships away from suppliers is a longer-term proposition. Gaining visibility into some of these companies and being agile enough to change suppliers are challenges all CPG companies face.

Clearly, U.S. companies in the CPG sector and beyond are taking these threats seriously. Over a quarter of organizations in North America said that they took some degree of action on cybersecurity in response to Russia's invasion of Ukraine.[vii]

Key messages for the business: While cybersecurity teams support the commitment to shifting supplier relationships when necessary,organizations should be judicious about where they cut ties, because they also need to consider their obligation to serving the needs of innocent consumers.

[For more, see "Be prepared to pivot," page 10.]

3. Gaps in the technology stack open attack vectors

It is well known that the CPG sector is saddled with a wide spectrum of legacy technologies – from software used in the back office to Programmable Logic Controllers (PLCs) on the factory floor to original enterprise resource management (ERP) systems to Industrial Control Systems (ICS). These technologies are often kept in place as they are critical to the CPG manufacturing process and difficult to replace. However, they are now being connected to newer technologies, which opens the possibility of new risk vectors emerging in an otherwise disconnected environment.

"The scariest of these attacks is when malware is introduced into ICS and SCADA that run and manage manufacturing facilities because they have the potential to shut down entire production lines," says Marene Alison of J&J.

At the same time, CPG companies are investing in cutting-edge technologies to foster scale, growth, and efficiency. For example, to compensate for persistent labor shortages, some manufacturing functions are being automated, and advanced sensors, drones and autonomous vehicles are being used as well. However, since many of these technologies are not yet "battle tested," the spectrum of potential attack vectors is largely unknown.

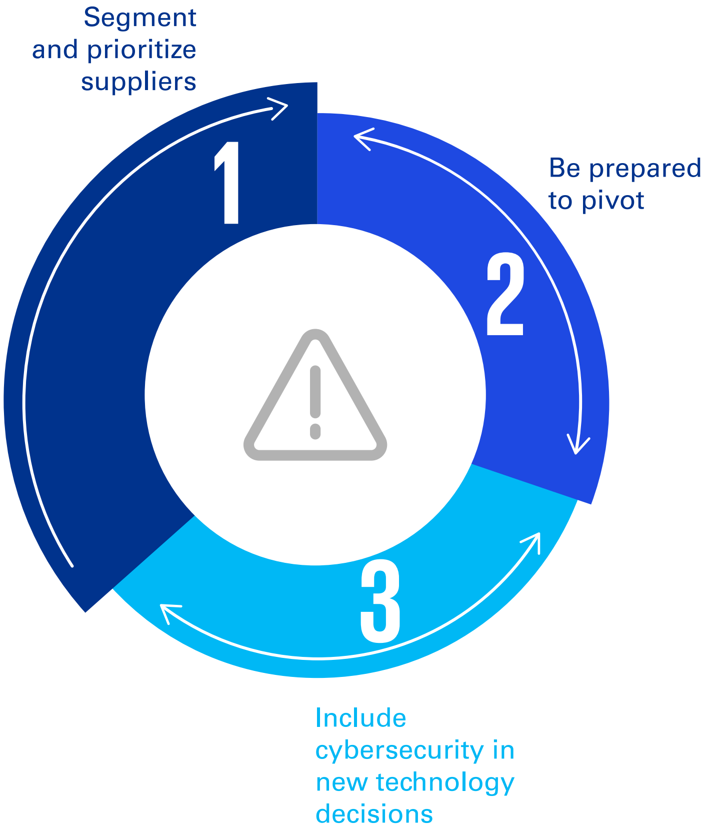
Further, information technology (IT) and operational technology (OT) are converging at many companies. This connectivity is valuable in that it allows insights from, say, research & development to be directly accessible on the factory floor. However, at the same time, if a cyber-criminal gains access to OT, they could by connection gain access to a CPG company's entire network.

Key messages for the business: Adopting cutting-edge technologies is, of course, key to innovation and our continued growth into new markets. However, modernizing our systems can be a double-edged sword in terms of security. Therefore, it is strongly recommended that the cybersecurity team be brought into discussions about technology transformation while the organization is still in the ideation stage. That way, these systems can be built and architected with the most advanced cybersecurity principles already in place.

[For more, see "Include cybersecurity in new technology decisions," page 11.]

Key cybersecurity principles for countering the top three threats

The knowledge that CPG companies have become more of a target for threat actors—at the same time as their products have taken on increased significance to consumers—is driving CISOs' conversations with the business about increasing supply chain security. These conversations are key to securing additional investments in talent, resources, and a corporate structure that integrates cybersecurity more closely with the business.


Segment and prioritize suppliers
1
Be prepared to pivot
2
3
Include cybersecurity in new technology decisions

> We have to look very carefully at industry data, as well as signals from our suppliers and how they relate to the type of business we want to do with them. It is critical to understand whether there is privacy data, intellectual property, or strategic manufacturing information involved. We have to stay several steps ahead on these issues so we can move quickly for the business."
>
> \- **Mike Wagner,**
> Designate CISO for J&J's
> planned New Consumer
> Health Company

1. Segment and prioritize suppliers

Among all industries, consumer packaged goods may be managing the largest number of third-party suppliers. Particularly in the food segment of the industry, many of these suppliers are small companies and/or have no clear competitors when it comes to providing a niche ingredient. In effect, this puts CPG companies in the position of taking on the cyber risks of hundreds of suppliers at once. It would be nearly impossible to stay on top of the cyber posture of all of these suppliers, so cybersecurity teams need to work with the business to determine which are most critical to protect – either because they supply an ingredient for one of the company's more lucrative products, or because having them out of commission could effectively shut down the CPG company's production line.

In efforts to get their arms around this challenge, CISOs and their teams can:

- **Protect** the company's "crown jewels" by prioritizing the most lucrative – and risk-prone – products.
- **Find** common ground between business priorities and cyber priorities.
- **Automate** cybersecurity questionnaires administered to third-party suppliers to ensure a more real-time accounting of the risks they face.
- **Determine** which suppliers hold the most sensitive data.
- **Emphasize** business continuity and disaster recovery by mapping potential connections between suppliers and the CPG company's OT and IT systems.
- **Consider** instituting an annual certification process through which suppliers can demonstrate the level of consistency and integrity they've been able to maintain in their cybersecurity protocols.
- **Determine** whether more risk lies with indirect or direct vendors.
- **Partner** with procurement and legal on contractual language that specifies the timeline for suppliers to report and remediate potential breaches.

2. Be prepared to pivot

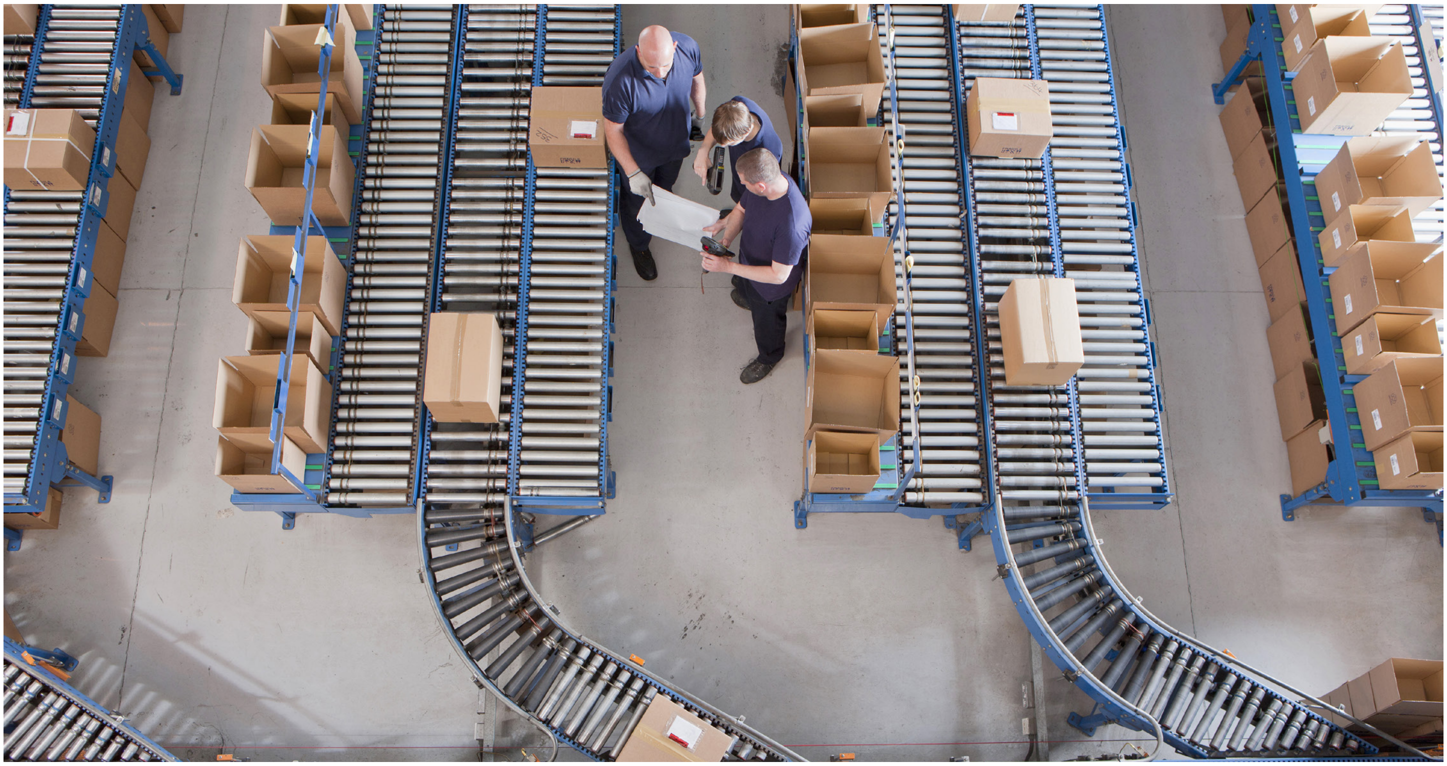
In an ideal world, CPG companies would be familiar with all the intricacies of their suppliers' operations across the globe. However, the reality is that, as difficult as it is to get domestic suppliers to align their cybersecurity protocols with that of a large CPG company, the challenge multiplies exponentially when dealing with suppliers in certain regions of the world. Complicating matters is the need to stay abreast of potential global threats or trends that could impact supply chain delivery. Today's CISOs and their teams have a unique set of challenges driven by complex happenings on the world stage, which require them to:

- **Customize** cybersecurity protocols by region to account for geopolitical tensions and the viability of pivoting to a new vendor when needed.
- **Remain** flexible when dealing with foreign suppliers to balance what might be a sensible response to a political issue with the ethical obligation to meet the needs of the local populace.
- **Understand** the degree to which interdependencies might limit your company's ability to change suppliers expeditiously.
- **Educate** the business about the concentration risks associated with overdependency on particular suppliers.
- **Define** the scope of relationships with overseas suppliers clearly, e.g., whether the supplier is only being used for manufacturing in certain regions.
- **Partner** with local region teams to gain an understanding of the regulatory and legal landscape as it relates to cybersecurity standards.
- **Review** and block known threat actors' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs).
- **Enhance** your threat intelligence and incident response capabilities and view the results through a business lens.

3. Include cybersecurity in new technology decisions

Growth in the CPG industry depends to a large degree on technology transformation that facilitates everything from efficient manufacturing processes and real-time insights into inventory needs to market and competitive intelligence and the development of innovative intellectual property. While CPG companies are certainly prioritizing technology transformation and digitalization, they are in many cases attempting to integrate new platforms, software products, and apps with outdated legacy technology. To move their companies toward modernization and growth, while protecting against the introduction of new attack vectors, CISOs and their teams can work with the business to:

- **Emphasize** business resiliency and continuity by mapping potential connections between suppliers and the CPG company's OT and IT.
- **Coordinate** efforts between IT cybersecurity teams (that focus on security for ERP systems, email, HR, CRM and other office systems) with OT cybersecurity teams (that focus on security for such factory-floor technologies as PLCs, SCADA/HMI systems, and sensors).
- **Evaluate** the degree to which IT and OT networks can be separated to help keep bad actors from infiltrating the entire network with one attack.
- **Inventory** where and how data is collected, transferred, and stored to help minimize vulnerability to attack.
- **Introduce** tooling and curating capabilities, as well as relevancy analyses, to determine what data is included in the company's security investigation pipeline so you can separate real insights from chatter.
- **Upgrade** cybersecurity protocols when new third-party suppliers are brought onboard or new equipment is introduced on the factory floor.
- **Assist** the business in weighing trade-offs between innovation and secure development.
- **Assess** the range of available Cloud providers for their commitment to security, inclusion of all ISO standard features, intrusion detection programs, dedicated incident response team, patching on a regular cadence, and more.



Conclusion

Demand for consumer-packaged goods is higher than ever. However, awareness of that increased demand has made the industry a more attractive target for cyber-criminals—from nation states seeking to disrupt stability to threat actors vying for ransom payments to malicious competitors seeking to sideline the competition.

At this unique point in history, CPG companies are more open to the idea of collaboration to help bolster the entire industry again cyber-crime. The framework that underlies this paper and the accompanying practitioners' guide is a perfect example of CPG companies lowering their boundaries for the greater good. The vision is that this effort, pursued under the auspices of the Manufacturing ISAC, will be a work in progress and that other members of the ISAC community—and the CPG industry at large—will join the effort.

In the name of collaboration, CPG CISOs may want to pursue the following:

- Consider working with the Manufacturing Information Sharing and Analysis Center (ISAC) to create an annual certification program through which third-party suppliers can attest to their cyber fitness.
- Establish a clearinghouse of best practices and persistent threats that all companies in the CPG industry can access.
- Share education and training resources to eliminate duplication of efforts.
- Collaborate on questionnaires and baseline standards that are administered to third-party suppliers.
- Identify strategic collaborators from third-party suppliers that partner with multiple CPG companies and figure out how they can share information to hold each other accountable.
- Establish a CPG industry analysis/research team that can help better prepare the entire industry for contagion threats.
- Encourage the Manufacturing ISAC to house up-to-date contact information for security peers and vendors throughout the CPG industry.
- Engage with peers on at least a monthly basis to undertake joint tabletop exercises and information sharing.

And finally, remember that sharing knowledge about cybersecurity isn't going to give your peers a competitive edge. In contrast, the benefits of a joint line of defense against threat actors will make the entire CPG industry that much stronger.

[i] Ramishah Maruf, The surprising reason you can't find cream cheese anywhere, CNN Business, December 18, December 18, 2021.

[ii] U.S. pet adoptions still strong as cats, dogs melt stress, Reuters, May 3, 2021.

[iii] Jaewon Kang, The Pet-Food Shortage Is Real, and Owners Are Scrambling. 'It's Been a Waking Nightmare,' Wall Street Journal, December 21, 2021.

[iv] Kelly Tyko, Grape-Nuts shortage: Are you having trouble finding the cereal? You are not alone and here's why, USA Today, January 27, 2021.

[v] Kelly Tyko, Grape-Nuts shortage: Are you having trouble finding the cereal? You are not alone and here's why, USA Today, January 27, 2021.

[vi] Information for Families During the Formula Shortage, U.S. Department of Health and Human Services, https://www.hhs.gov/formula/index.html.

[vii] Charlotte Atchley, More automation brings cybersecurity to the forefront, Baking Business, September 29, 2021.

[viii] How Geopolitics Impacts the Cyber-Threat Landscape: Q&A with Paul Proctor, Gartner, June 10, 2022.

Participating CISOs

Marene Allison

CISO, Johnson & Johnson

Marene is responsible for protecting J&J's Information Technology systems and data worldwide through elimination and mitigation of cybersecurity risk. This includes ensuring that the J&J information security posture supports business growth objectives, protects public trust in the J&J brand, and meets legal/regulatory requirements. With 265 companies in 60+ countries, J&J is a leader in consumer health, medical devices, and pharmaceutical products worldwide.

Andrew Stanley

CISO & VP Global Digital Operations, Mars, Inc.

Andrew Stanley has served as the Chief Information Security Officer (CISO) & Global Digital Operations VP for Mars, Inc. since early 2022, and as CISO since 2017. He has led the transformation of cybersecurity at the company, integrating security from across the enterprise into one function. Previously, Mr. Stanley served as CISO for Philips, where he initiated and delivered a two-year improvement program for cybersecurity that created an enterprise-wide information security function. He has also worked with the World Economic Forum and the Coalition for Responsible Cybersecurity and has served as a CISO Ambassador for the US Federal Bureau of Investigation, and, currently, as a research affiliate at the Massachusetts Institute of Technology Sloan School of Business.

Martin Bally

Vice President and CISO, Campbell Soup Company

Martin Bally is the Vice President and Chief Information Security Officer (CISO) of Campbell Soup Company and has over 23 years of experience in cybersecurity. Martin has global experience in Information, Cyber, Manufacturing, Digital, and Product Development Security. He has held the Global CISO position at Stellantis, formally Fiat Chrysler Automotive (FCA), American Axle & Manufacturing, Diebold, and TRW Automotive. He has prior experience in manufacturing, legal, and fintech industries. He has also managed a P&L of 20+ million for security services. In 2020, Martin was recognized as a top 100 CISO by Cyber Defense Magazine.

Mike Wagner

Designate CISO, J&J New Consumer Health Company

As the VP, Information Security & Risk Management (ISRM) for Consumer Health, and Designate Chief Information Security Officer for the planned New Consumer Health Company, Mike leads a global team to develop the strategic Cyber priorities, operating plans, and organizational model for J&J's planned new Consumer Health company. He has held a variety of leadership roles including serving on the Board of Directors for the Health Information Sharing and Analysis Center (H-ISAC), leading the H-ISAC Pharma Supply Chain Steering Committee, as well as being the Executive sponsor for the JJT Veterans Employee Resource Group for the last 10 years.

Contributors

Jonathan Dambrot
Principal, Cybersecurity Services, KPMG
T: 908-361-6438
E: jdambrot@kpmg.com

Mitushi Pitti
Managing Director, Cybersecurity Services, KPMG
T: 848-247-8445
E: mitushipitti@kpmg.com

Kristy Hornland
Director, Cybersecurity Services, KPMG
T: 425-281-5251
E: khornland@kpmg.com

We would also like to thank the following individuals for their invaluable contributions:

KPMG

Brad Raiford
Donna Ceparano
John Hodson
Daniel Christman
Kelsey Flynn

Mars

William Dzmelyk
Bryan Hubbard
Kate Hanley
Tandon Saket
Elizabeth Zubiate
Rafael Granjeiro

Campbell Soup Company

Mark Wehrle
Kristine Campbell

Procter & Gamble

Brian Beck
Franky Milants
Sandi Pickens
Antonio Sannino
Nicholas Shah
Robert Schofield

Johnson & Johnson

Steve Cohen
Chris van Schijndel
Harry Megarian
Justin Boyee
Karl D’souza
Bahar Yazgan

Additional Contributors

- Mark Orsi (Global Resilience Federation)
- Tommy Maltezos (CyberVadis)
- Edouard Lacarriere (CyberVadis)
- Thibault Lapedagne (CyberVadis)
- Andrew Moyad (Shared Assessments)

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.