Practitioners' Guide to Securing the CPG Supply Chain

Welcome to the Practitioners' Guide to Securing the Consumer Packaged Goods Supply Chain

> *"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."*
>
> *—Andrew Stanley, Chief Information Security Officer & VP Global Digital Operations, Mars, Incorporated.*

Background

Our Community Investment

In a time of historic disruption, consumer packaged goods (CPG) have arguably become part of the critical infrastructure. Depending on the type of products, consumer reactions to disruptions to the CPG supply chain have ranged from annoyance (think Grape Nuts) to deep inconvenience (toilet paper and paper towels) to true hardship (baby formula).

As it becomes increasingly clear that CPG shortages can cause significant stress and disruption, the sector has become more of a target for cyber-attacks. It is worth noting that in, early 2020, a third of all cyber events occurred in the manufacturing sector, many targeting small businesses like the third-party suppliers on which the CPG industry relies. The sheer breadth of these suppliers poses numerous challenges for CPG companies' cybersecurity functions.

In this paper, we outline those challenges and provide recommended solutions across five critical areas related to third-party suppliers: Vendor selection and onboarding, Internal vendor assessment, External vendor assessment, Contracting, and Continuous monitoring and offboarding.

Many of the recommendations in this guide speak to the emerging need for CPG companies of all sizes and specialties to collaborate to present a united front against potential threat actors and raise the overall cyber maturity of the industry.

With that in mind, the Manufacturing ISAC spent the last year assembling a cross-organizational team of cybersecurity experts led by Mars and facilitated by KPMG. The team comprises subject matter experts from leading CPG companies Mars, Campbell Soup Company, Johnson & Johnson, and Procter & Gamble, as well as software company OneTrust and external assessors CyberVadis and Shared Assessments.

For guidelines relevant to your key area of interest, please select one of the topics from the menu on the left-hand side of the page.

Related summit sessions

Encouraging consistent third-party security protocols: A practical Framework

This session will showcase the current challenges and opportunities for practitioners in managing their third-party vendor ecosystem. Representatives from major consumer-packaged-goods organizations will participate in a roundtable discussion focused on each specific stage of the vendor lifecycle, from procurement to offboarding, to determine where collaboration across the industry can better facilitate secure third-party procedures. For shared challenges, the group will look to identify collective best practices, as well as novel approaches to better address the issues at hand.

Emerging security threats and industry-wide disruption: CISOs weigh in on the need for resiliency and cooperation

This session aims to provide a strategic view of the challenges in securing the supply chain from the perspective of CISOs at major consumer packaged goods organizations. Insights on the broadening and ever-changing supply chain threat landscape will be captured through questions posed to each of the participating CISO panelists. The panel's goals are to determine how organizations prepare for and respond to unpredictable disruptions that threaten business continuity and system security.

Practitioners' Guide to Securing the CPG Supply Chain

Contributors

Thank you

Our Thoughtful Contributors

We are so grateful for the support of our community partners, who are committed to the evolution of the people, processes, and products our organizations contribute to this industry. Together we put together what we hope you will find to be an insightful and relevant guide on securing the most critical components of the CPG supply chain.

Johnson & Johnson

- Marene Alison, CISO (J&J)
- Mike Wagner, Designate CISO (J&J Consumer Health)
- Steve Cohen
- Chris van Schijndel
- Harry Megerian
- Justin Boyee
- Karl D'souza
- Bahar Yazgan

MARS
Tomorrow starts today

- Andrew Stanley, CISO & VP Global Digital Operations
- William Dzmelyk
- Bryan Hubbard
- Kate Hanley
- Tandon Saket
- Elizabeth Zubiate
- Rafael Granjeiro

P&G

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

Campbell's

- Martin Bally, VP & CISO
- Mark Wehrle
- Kristine Campbell

cybervadis

- Tommy Maltezos
- Edouard Lacarriere
- Thibault Lapedagne

SHARED ASSESSMENTS

- Andrew Moyad

onetrust

- Matthew Moog

KPMG

- Jonathan Dambrot
- Mitushi Pitti
- Brad Raiford
- Donna Ceparano
- John Hodson
- Kristy Hornland
- Daniel Christman
- Kelsey Flynn
- Orson Lucas

Special thanks to Mark Orsi and the Global Resilience Federation for their insightful guidance and support.

Practitioners' Guide to Securing the CPG Supply Chain

Manufacturing ISAC Practitioners User Guide

Guidelines for each area of consideration will reflect the following format to enable ease of use:

Overarching themes

Each area of consideration features three to five central themes that were identified as critical cybersecurity risks by Manufacturing ISAC roundtable participants.

Challenges

In this subsection, we present common challenges with which many CPG cybersecurity teams are grappling.

Recommendations

Recommendations and practices that have been employed to address these challenges are outlined here. Real-life applications of security controls should be of value to practitioners as they seek to address cybersecurity threats in their own organizations.

Choose a section

Introduction
Related summit sessions
Contributors

Choose a topic

User guide
Vendor selection and onboarding
Internal vendor assessment
External vendor assessment
Contracting
Continuous monitoring and offboarding

Vendor Selection and Onboarding

Introduction

While consumer packaged goods (CPG) direct vendors (i.e.,"suppliers") may not traditionally focus on handling sensitive data such as personally identifiable information (PII) or payment card/cardholder information but rather focus on supplying a good or service, they tend to have less mature cyber defenses than suppliers in other industries. When selecting vendors, there are a number of issues that must be addressed, ranging from identifying where they fall on the spectrum of criticality as it relates to the business, putting extra safeguards in place for niche suppliers that bring a level of innovation to the company and its products, ensuring that the cybersecurity team is brought into the procurement process at cadences that help minimize risk to the company, and responding to risks that arise during onboarding before engagements begin.

Overarching theme #1: *Identifying the most critical suppliers*

CPG companies can engage with tens of thousands of vendors in a year. With this is mind, how do companies identify the most critical suppliers? It is important to consider the context of the relationships and the criticality to the business.

Challenges

- Difficult to connect with the business on tens of thousands of suppliers.
- Too expensive to address all the most critical suppliers, so need to prioritize.
- Shifting status of suppliers, e.g., new vendors may become more, or less, critical over time.
- Insufficient time spent on assessing the cost to the business of losing a supplier.
- Myopic focus on largest and niche vendors results in less visibility over middle layer suppliers.

Recommendations

- Dedicate adequate time to evaluating middle-layer suppliers.
- Many programs tend to focus on Saas/PaaS vendors, and increasingly raw materials suppliers. A robust program should also include additional third parties in the value chain such as logistics and warehousing vendors.
- Leverage existing supplier data to identify which vendors are likely to be most critical.
  - Use several lenses to evaluate what makes a supplier critical, e.g., spend, bill of materials, impact on security of organization, etc.
  - Leverage multiple organizational data inputs from procurement data to RFPs.
  - Develop a common taxonomy for factors that are indicative of criticality.
  - Segment suppliers and put highest risk through the whole third-party risk management (TPRM) process.

Choose a section

Introduction >

Related summit sessions >

Contributors >

Choose a topic

User guide >

Vendor selection and onboarding >

Internal vendor assessment >

External vendor assessment >

Contracting >

Continuous monitoring and offboarding >

Vendor Selection and Onboarding

Overarching theme #2: *Aligning with business priorities*

CPG companies must consider business objectives when prioritizing their vendor-assessment processes during onboarding. Organizations focused on quick-to-market programs to remain competitive should view and utilize cybersecurity principles as enablers, as opposed to barriers.

Challenges

- Business-critical suppliers may appear on the surface to only fulfill a specific need.
- Lack of clarity on whether a new supplier engaged by the business will have a limited impact or become the "next big thing."
- Difficulty understanding interdependencies with critical business processes associated with a particular vendor, at onboarding and as services expand over time.
- Cultural belief at many organizations that cybersecurity is usually a barrier to operations and innovation.
- In the event of a change in the relationship with a supplier or the scope of an engagement, consider whether the supplier's risk profile has changed and whether it is appropriate to transfer the supplier from one business unit to another.

Recommendations

- Clearly identify business priorities and identify ways that assessing and addressing cyber risk can help enable the business to achieve its goals.
- Ask the business for critical vendors that support business priorities and conduct a deep dive to show the value of addressing their cybersecurity challenges.
- Illustrate downsides of supplier risks by communicating to the business vivid postmortem examples of business impacts of cybersecurity incidents that occurred.
  - Plan to engage your executive leadership team in tabletop exercises that present realistic cyber-event scenarios for better understanding and buy in from the organization.
- Gain insight into upcoming projects in the business's pipeline that could impact the security of the supply chain.

Choose a section

Introduction

Related summit sessions

Contributors

Choose a topic

User guide

Vendor selection and onboarding

Internal vendor assessment

External vendor assessment

Contracting

Continuous monitoring and offboarding

Vendor Selection and Onboarding

Overarching theme #3: *Managing sole and niche suppliers/ innovation vendors*

To remain competitive, CPG companies are always searching for new ways to evolve the products they bring to market. This requires bringing innovation partners on board that can help with ideation. While this is great for business, many of these supplier partners can introduce new risks.

Challenges

- Suppliers that bring significant innovation to the CPG industry are often more focused on speed and disruption than on security.
- It can be prohibitively expensive to put backup suppliers and contingency plans in place for all key suppliers.
- Risk of significant monetary loss if key niche suppliers can't defend themselves against a potential breach or cyber-attack.
- CPG companies have insufficient motivation to make significant cyber investments when it comes to suppliers that are high volume and low margin.

Recommendations

- Document where the business is dependent on sole suppliers.
- Determine with the business where alternative suppliers are appropriate.
- Assess and document the risks if the business goes forward with engagements with high-risk sole suppliers.
- Assist the business in weighing trade-offs between innovation and secure development.

Choose a section

- Introduction
- Related summit sessions
- Contributors

Choose a topic

- User guide
- Vendor selection and onboarding
- Internal vendor assessment
- External vendor assessment
- Contracting
- Continuous monitoring and offboarding

Vendor Selection and Onboarding

Overarching theme #4: *Addressing a lack of standardization in procurement processes*

Coordinating interactions among the business, procurement, and cybersecurity team requires a delicate balance in terms of who owns which aspects of a supplier relationship. By developing repeatable, automated processes, organizations can help smooth the hand off and collaboration among teams to best fit the organization's needs.

Challenges

- Multiple intake points for procurement across many CPG organizations.
- Variety of teams engage in procurement depending on the country, region, or business unit.
- Unclear when best to insert the cyber perspective.
- Cyber can become a bottleneck if the function comes into the process after the contract is signed.

Recommendations

- Centralize intake points so there is an official path through procurement.
- Extend centralization beyond indirect procurement to include direct procurement.
- Consider that relationship management, training, and awareness are as important as processes when it comes to procurement.
- Utilize connected systems and process flows to trigger automatic involvement from third-party security teams.

Choose a section

Introduction >

Related summit sessions >

Contributors >

Choose a topic

User guide >

Vendor selection and onboarding >

Internal vendor assessment >

External vendor assessment >

Contracting >

Continuous monitoring and offboarding >

Vendor Selection and Onboarding

Overarching theme #5: *Responding to issues that arise during onboarding*

Organizations that fail to recognize the relationship element of onboarding will struggle to collaborate with their suppliers for better security practices and transparency. Teams must be aware of the potential challenges that could arise for suppliers if processes are not well defined and managed.

Challenges

- Frustrating lack of standardization in the onboarding process.
- Time-consuming process when suppliers have to undergo a risk check before completing their registration with a CPG company.
- Potential risk of relationship erosion if cyber is brought in too late to the supplier evaluation process.

Recommendations

- Establish safety nets around cyber events that happen repeatedly at certain suppliers.
- Put high-risk suppliers through third-party risk management (TPRM) process before contract signing.
- If information security issues arise in the onboarding process, dedicate the time to help suppliers address issues, or ensure the business has identified an alternate supplier.
- Look at material changes in existing suppliers' risk profiles, as they could change the scope of what the company buys from the supplier and related risks.

Internal Vendor Assessment

Introduction

When cybersecurity teams at consumer packaged goods (CPG) companies have the internal resources in place to conduct supplier assessments on their own, there are a number of challenges they have to navigate. These range from managing and prioritizing an extensive crop of suppliers, dealing with multiple procurement organizations within the company, determining the ability of smaller suppliers to accurately answer upfront questionnaires, and determining whether it might be more expeditious to triage after the fact than to invest time in administering questionnaires that yield inaccurate results.

Overarching theme #1: *Extensive breadth of vendors*

Organizations see tens of thousands of new vendors a year for assessment, which is further multiplied by recurring continuous monitoring needs surrounding existing vendor relationships. The overall volume of vendors and breadth of services offered can make it challenging for third-party security teams to keep up.

Challenges

- Overwhelming number of small and niche suppliers siloed throughout the company.
- Risk level doesn't necessarily align with the suppliers' size.
- Multiple stakeholders that could potentially kick off a supplier assessment.

Recommendations

- Ensure you have an accurate inventory of all vendors with which the company does business.
- Stratify vendors according to both cyber risk and criticality to the business.
- Assess each supplier's level of integration with the company and which of your products may be impacted by a breach at a particular supplier.
- Use risk analyses to determine how extensive assessments should be, up to and including putting a supplier through a full third-party risk management (TPRM) program.
- Utilize data exchanges managed by third party assessors to gather assessments that can supplement the work done by your internal team.
- Identify the number and types of vendor risks and display on a "risks-metrics dashboard."

Internal Vendor Assessment

Overarching theme #2: *Multiple procurement organizations*

When the procurement function is decentralized, a vendor assessment can be an intricate process, particularly if there is no clearly defined cadence for when to assess vendors' security postures.

Challenges

- Multiple siloed procurement organizations might make it difficult to assess which suppliers have access to sensitive customer data, e.g., SaaS vendors engaged by the marketing organization.
- It is sometimes difficult to identify the appropriate internal stakeholder once the procurement process has been initiated.
- Different procurement organizations may engage cybersecurity at different points in time, leading to inconsistent supplier experiences and frustration.

Recommendations

- Codify the onboarding process for suppliers no matter which department they are associated with.
- Develop security training for all departments—marketing, manufacturing, legal, etc.—so they understand data protection protocols and consult with the cybersecurity function before sharing potentially sensitive data.
- Capture business relationship owners and determine who has responsibility for engaging a third-party security team member.

Internal Vendor Assessment

Overarching theme #3: *Efficacy of questionnaires*

Not all suppliers are well prepared to answer security questionnaires accurately or thoroughly. Organizations must take an honest look at the efficacy of their questionnaires and identify multiple routes to understanding the potential risk of a supplier to their operations.

Challenges

- Difficult to apply the same security questions with a broad variety of suppliers that may have access to different levels of PII and other proprietary data.
- The use of multiple risk-scoring tools with different interfaces makes it difficult for CPG companies to aggregate results and for suppliers to keep their responses consistent within multiple inquiry formats.
- Suppliers may not agree to complete an assessment questionnaire.
  - Smaller suppliers may not have the technical expertise to answer complicated questionnaires (SIG, CAIQ, etc.)
  - Larger suppliers may only provide their standard questionnaires and not complete customer-specific questions.
- There tends to be a lack of evidence confirming the state of cyber maturity reflected in the questionnaires suppliers complete.
- Many third-party suppliers outsource some of their functions to 4th and 5th parties that are even less cyber mature.

Recommendations

- Consider automating the assessment platform and use an exchange model where CPG firms share supplier assessment results.
- Supplement questionnaires for high-risk suppliers with efforts to gather evidence in a variety of ways.
- Collaborate with the Manufacturing ISAC to drive consistency in supplier requirements, including the possibility of certification required to do business with CPG companies.
- Commit to educating suppliers on what is required to complete questionnaires effectively, to the degree feasible
  - Remember that assessed security requirements must be simple enough for even the smallest suppliers to understand, respond to, and comply with.
  - Keep in mind that, while common security requirements must be relevant and understandable by all suppliers, some level of education may be required to reach the broader supplier community.
  - Support the Manufacturing ISAC in efforts to educate 3rd- and 4th-party suppliers.

Internal Vendor Assessment

Overarching theme #4: *Balancing upfront assessments vs. remediation and response*

Across a wide variety of suppliers there is inconsistency in the level of cybersecurity expertise, willingness to give CPG companies full transparency into their operations, or ability to apply security controls appropriately in their own environments. Organizations must find methods of meeting smaller suppliers where they are in regard to assessment, remediation, and response protocols.

Challenges

- Not always clear what would happen to a CPG company if a particular supplier had an IT or financial breach.
- Since smaller suppliers can't always answer the questionnaires, CPG companies are compelled to formulate response programs instead.
- Smaller suppliers may not have the skillset inhouse to apply cybersecurity controls in their environments.

Recommendations

- Hold regular internal discussions on business continuity related to each supplier, especially single source and critical suppliers.
- Accept the fact that, with some tiny suppliers, it may be more sensible to triage after the fact, have safety stock, institute vendor diversification, or invest in cyber insurance than to administer upfront assessment questionnaires.
- Look at proxies for cyber maturity, including SOC 2 evaluations, score cards, and continuous monitoring services.
- Convene a pilot group of small vendors to gain insights into how they would prefer to be assessed.
- Create a partnership with the smaller/less mature vendors to assist in guiding them to low-cost or no-cost options to improve security.

External Vendor Assessment

Introduction

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 CPGs 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. For CPG companies to assess the ever-increasing volume of required vendor assessments, they often partner with external assessors to supplement their third-party security programs. External assessors can help CPG companies onboard suppliers, support suppliers in answering questionnaires and providing evidence, and analyze the results.

Overarching theme #1: *Complexity and uncertainty in the CPG industry*

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. Teams must prioritize mechanisms that allow for better resiliency of operations and that protect the most critical assets—the "crown jewels," if you will—that allow products to reach the market in a timely manner.

Challenges

- Unstable supply chain given global events, relative resilience of different CPG companies, and suppliers with varying scale and cyber maturity.
- Need to prioritize potential global threats or trends impacting supply chain delivery based on a spectrum of considerations including:
  - Privacy implications in different regions
  - Availability of supplies in different regions in the event of a war—physical or cyber-based
  - Product demand is increasing as the U.S. bounces back from the height of the pandemic
- With global suppliers, there could be varying cybersecurity protocols, legal structures related to data handling, and site-level nuances, even when an enterprise security policy is in place.
- Cumbersome to track the extent to which global suppliers are handling employee PII.

Recommendations

- Raise the probability of informed risk-management decisions by extending the input to suppliers' risk profiles beyond traditional assessments to an agile, data-driven approach that could include other internal and external data sources.
  - For example, SRS tools can help clarify questions that are being asked, as well as how to aggregate and integrate with CPGs' other platforms.
- Take special care to address the risks of working with global suppliers
  - Ensure the scope of engagements with global suppliers is clearly defined, e.g., the types of data the supplier is approved to handle.
  - Partner with local region teams to gain an understanding of the regulatory and legal landscape as it relates to cybersecurity standards.

External Vendor Assessment

Overarching theme #2: *Inconsistent assessment methodologies from external assessors*

Cybersecurity teams that leverage external assessors have many reasons to do so—such as the abundance of assessments that need to take place, limited internal bandwidth, and cost benefits to the company. However, many are currently facing a unique point-in-time challenge: Since many CPG companies use the same assessors, it may not continue to make sense to spend the time and resources to conduct the same evaluations multiple times. Therefore, there is currently a call to action to create an exchange that allows for suppliers to be assessed once and leveraged across many companies and even industries. This effort will require industrywide standardization on the types of security issues to be assessed.

Challenges

- While CPG companies tend to agree on general security principles, there is a lack of standardization when it comes to specific security requirements.
- The extent to which assessments are customized to meet one CPG company's needs can render results unusable by another company trying to leverage the results.
- Many of the suppliers that are assessed are small and medium-sized enterprises (SMEs), which are typically not ready to align with a CIS or NIST framework.
- There is an ever-increasing number of players in the external vendor assessment space, each offering different methodologies and service levels.

Recommendations

- Maintain an open communication pathway between ISACs to ensure alignment on critical security requirements and flexibility as external factors and technologies evolve.
  - Create a formal definition for how CPG companies expect to receive evidence that suppliers meet security requirements, e.g., a tangible demonstration of security practices rather than simple attestation.
- Advocate for the Manufacturing ISAC to coordinate the establishment of industrywide security requirements for suppliers and create a data-sharing exchange.
  - Agree on an industrywide range of security requirements based on the criticality of vendors.
  - Achieve scale across CPG companies and dependably exchange assessment data by coordinating with the numerous external assessors in the market.
  - Create a framework and automated interface that accounts for assessors' proprietary methods of assessment, scoring, dashboards, etc.

External Vendor Assessment

Overarching theme #3: *Surplus of potential external assessments and subscriptions*

Both CPG companies and their suppliers can be overwhelmed by the pure volume of external assessors. Each party has specific expectations, but both expect a positive cost/benefit equation when it comes to engaging with these firms. CPG companies want accurate assessments and the ability to integrate findings from multiple assessors that may use different tools and formats. Meanwhile, due to time, resource, or budgetary constraints, suppliers would like to avoid having to complete duplicative assessments with disparate external assessors.

Challenges

- Each CPG company may partner with one external assessor to supplement their third-party risk management (TPRM) mix, but this may not translate into an equally straightforward process for suppliers being assessed.
- Some suppliers may try to compel their CPG customers to accept assessments from different external assessors as they are unwilling to go through additional security assessments.
- Suppliers may face different questions based on which external assessor a CPG company brings in.
- The cost/benefit of engaging an external assessor could be eroded if the CPG company purchases licenses across multiple external assessors' platforms but only receives assessments for a handful of vendors.

Recommendations

- Determine which are the strongest external assessors that stand out and lead the network.
- Work with the ISACs on guidance for leveraging external assessors that best fit the needs of the CPG industry.
- Remember that sustainable external assessors offer services that are of value to all CPG suppliers and buyers.
- While external assessors will standardize some of the questions being asked, each specific CPG company should identify which questions are most relevant given the risk profile of a supplier and the business context.

Practitioners' Guide to Securing the CPG Supply Chain

Contracting

Introduction

Consumer packaged goods (CPG) companies have long prioritized indirect suppliers in the contracting process due to their potential handling of PII, CCI, proprietary, or otherwise regulated data. However, in a more recent trend, companies are beginning to bake cybersecurity considerations into their contractual agreements with direct suppliers as well, particularly when the suppliers are critical to product manufacturing (e.g., ingredients for food products).

Overarching theme #1: *Contract approach for direct vs. indirect suppliers*

It is important to differentiate between how contracts are handled with indirect vs. direct suppliers. Since indirect suppliers have more exposure to sensitive data, as well as experience reporting on their cybersecurity practices with buyers, much of the language in their contracts can be standardized.

Challenges

- Direct suppliers may require more specific contract language and attention to detail to ensure the CPG company and its operations are protected.
- The contracting process is usually owned by global procurement without much transparency to the cybersecurity team unless indirect suppliers ask for changes to their standard contract language.

Recommendations

- Although some indirect suppliers offer CPG companies more transparency through point-in-time attestations, e.g., SOC reports, when it comes to the higher risk ones, it is advisable to advocate for bringing cybersecurity into the contracting process.
- For the most critical and/or riskiest direct suppliers, work with the Chief Legal Officer and procurement to add stricter contract language and include a column that explains the spirit of the clause.
- Include in the contract targeted timelines for suppliers to provide assurance that they are actively mitigating or addressing new risks that arise.
- Ensure "right to audit" is included in standard contract language, even if it is only invoked in the instance of an actual incident.
  - Divide auditee language into two paths: (1) standard language that says the CPG company can audit if there's an incident, and (2) security-oriented language that allows audits every couple of years.
  - Consider accepting SOC 2 or ISO certification reports in lieu of an audit, when available.
- Use standard language for run-of-the-mill direct suppliers that do contract manufacturing or those that manufacture small batches or packaging.
- Consider standardizing controls for direct-supplier interactions not only across individual CPG companies, but also for the CPG community as a whole.

Choose a section

Introduction
Related summit sessions
Contributors

Choose a topic

User guide
Vendor selection and onboarding
Internal vendor assessment
External vendor assessment
Contracting
Continuous monitoring and offboarding

Contracting

Overarching theme #2: *Managing attestation (including remediation or acceptance of risk)*

Most consumer packaged goods (CPG) companies devote significant resources to managing a heavy volume of security assessments outside of the initial contracting process. Considering that many suppliers may be transactional rather than recurring in nature, it can be difficult for organizations to validate the attestations they receive on vendors' security postures.

Challenges

- Most cybersecurity functions have insufficient resources to monitor direct suppliers after attestation that the supplier's environment meets requirements.
- Since supplier relationships are typically "owned" by the business, there can be quite a bit of leg work required to track down relationship owners.
- The process of tracking whether suppliers are fulfilling contract terms from the security side can be onerous.
- Data on the current state of security is almost always based on attestation and not validated by evidence.

Recommendations

- Ensure that "right to audit" and "right to remediation evidence" are both built into contracting language as they relate to a security event resulting in a loss.
- Balance the need for due diligence with protecting long-term supplier relationships, particularly if suppliers are volatile or resistant to answering security questions.
- Include in contract language that says suppliers must notify the CPG customer of a confirmed incident within 24 hours, and include target remediation dates for assurance that the risks are actively being mitigated or addressed.
  - Contract should specify that supplier must provide proof of root causes, signatures, and remediation activities in the event of a security incident, as well.

Contracting

Overarching theme #3: *Growing need to account for resiliency*

Ransomware attacks—such as Kronos in December 2021—brought to light the need for greater resiliency among critical suppliers, as well as the need to cover how to manage such risks in service-level-agreements and contracts. For CPG companies, it is a priority to ensure operations remain available—one of the three key components of cybersecurity's CIA triad along with confidentiality and integrity.

Challenges

- Suppliers may not have formal documentation around their business continuity and disaster recovery (BC/DR) plans to share with the buyer.
- The cybersecurity team must be able to identify which suppliers are interacting with critical business processes so security measures can be prioritized.
- It may be difficult to gain a line of sight into suppliers' cybersecurity KPIs/KRIs, which are key indicators of their current state.
- Vendors' SLAs may only be provided to the IT points of contact rather than to cybersecurity third-party risk teams as well.

Recommendations

- Align with IT to understand key suppliers' SLAs and level of cyber resiliency.
- Emphasize business continuity by mapping potential connections between suppliers and the CPG company's OT and IT.
- Work with suppliers to gain access to their security KPIs/KRIs, even if not formally built into the contract.
- Considering building into the contract "right to invoke" visibility into security KPIs/KRIs, as well as BC/DR plans.
- Ensure that supplier reviews and architecture reviews are conducted separately so the cybersecurity team doesn't need to manage intake for all of IT.

Practitioners' Guide to Securing the CPG Supply Chain

Continuous Monitoring and Offboarding

Introduction

Historically, there have been some barriers to continuous monitoring of suppliers' security profiles during the course of an annual or multi-year contract. Consumer packaged goods (CPG) companies don't always have sufficient resources to assess more than the most critical suppliers on a regular basis. On the supplier side, many have been resistant to the idea of being assessed multiple times, particularly in the case of direct suppliers that may not have publicly available security reports as indirect suppliers would. However, in today's constantly evolving threat environment, annual updates are no longer sufficient. Therefore, both sides need to find ways to facilitate some level of monitoring throughout the engagement.

Overarching theme #1: *Complete and reliable data*

Since continuous-monitoring data comes from different sources and there are no common standards, CPG companies can't always rely on the accuracy of their suppliers' risk profiles.

Challenges

- Accuracy of supplier security data can vary based on the questions asked in the SIG questionnaire, Security Rating Services (SRS) tools used, understanding of the business relationship, and the context of the specific engagement.
  - False positives, which are most prevalent when security ratings are conducted at the URL or domain level, can take up to two weeks to surface given the time needed for research and inquiries.
  - Given the varying levels of cyber maturity among suppliers, it may be difficult to determine if red flags that surface during continuous monitoring are indicative of systemic issues or just anomalies.
- There may be overlap on either the CPG or the supplier side that makes it difficult to get an accurate picture of a supplier's security profile:

Recommendations

- To improve the quality of current state assessment data from external sources, consider using artificial intelligence (AI) and/or machine learning (ML) to weed out false positives from SRS solutions.
- Build relationships with your most critical suppliers to increase cooperation when it comes to supplying data on a regular basis and ensure that potential security issues are related to the services being provided.
- If the CPG company has multiple divisions, make sure you identify whether another business function is doing a higher risk engagement with the same supplier, e.g., shared data lake.
- If a supplier is involved in more than one engagement at the same CPG company, be sure to account for varying levels of risk depending on the criticality of the supplier to operations in each division, as well as on whether varying regions are involved.

Continuous Monitoring and Offboarding

Overarching theme #2: *Appropriate cadence of monitoring*

By creating consistent monitoring expectations, suppliers (and direct suppliers in particular) may be more willing, prepared, and understanding about continuous monitoring by CPG companies.

Challenges

- Increasing the frequency of monitoring is hindered by the sheer supplier volume.
- Suppliers have historically pushed back on the idea of being assessed multiple times.

Recommendations

- Determine whether the internal cybersecurity team has the resources to actively monitor suppliers' security ratings on a continuous basis and determine the best path to augment with external assessor services or automation, if appropriate.
- Consider a tier structure that varies the frequency of monitoring according to supplier risk level determined during the onboarding process:
  - High risk: Annual review, including a deep dive for the most critical risk suppliers at the end of the first year
  - Moderate risk: Bi-annual review
  - Low risk: Every three years, or just at onboarding
  - Look at suppliers retrospectively if you have been doing business with them for many years.
- Use Security Rating Services (SRS) platforms, which allow review of original security assessments, security audit reports such as ISO/SOC, and any noted increases in risk caused by organizational changes, leadership turnover, or high-profile breaches at other firms.
- Advocate for a supplier relationship owner within the business to allow:
  - Ongoing management of the continuous monitoring process
  - Transparency to the cyber team on any volatility in the relationship
  - A contact for the cyber team if supplier scores are trending negatively
- Collaborate with other CPG companies on a common definition of continuous monitoring and on standards for how suppliers communicate with customers in the event of a breach.
- Identify the number and types of risks for each business unit and display on a "risks-metrics dashboard."

Choose a section

Introduction
Related summit sessions
Contributors

Choose a topic

User guide
Vendor selection and onboarding
Internal vendor assessment
External vendor assessment
Contracting
Continuous monitoring and offboarding

Continuous Monitoring and Offboarding

Overarching theme #3: *Staying abreast of potential supplier incidents*

Challenges

- Third-party suppliers that subcontract to numerous 4th- and 5th-party vendors may not have enough bandwidth to keep CPG clients informed of all cyber-incidents that occur.
- Suppliers that have direct connectivity to CPG companies systems need to be monitored carefully to avoid the introduction of malware that could spread through the CPG company.

Recommendations

- Rein in the need for continuous monitoring by encouraging suppliers to adopt a standardized process for notifying CPG customers and the sector at large when an incident occurs.
- Codify actions to be taken if a supplier is breached.
- Immediately disconnect any connectivity and disenable user IDs if a vendor is attacked with ransomware
- Combine the expertise of the cyber team and the vendor to determine if remediation is needed as a result of increased risk uncovered during continuous monitoring.

Continuous Monitoring and Offboarding

Overarching theme #4: *Risks associated with offboarding*

Some cybersecurity teams leave offboarding to procurement and only get involved to the extent of removing a supplier from their list. Since there are security considerations at the end of an engagement, companies should consider moving toward looping the cyber team in as necessary.

Challenges

- Suppliers may hold sensitive or confidential supplier data that has to be destroyed before offboarding.
- A period of inactivity between a CPG company and particular suppliers could obscure whether the two sides are still doing business.
- Discontinuation of a supplier relationship can occur without informing the cybersecurity team, leading to wasted efforts and unnecessary costs for continuous monitoring (licensing).

Recommendations

- Remove suppliers' access to the CPG company's systems and require proof of removal and destruction of data at offboarding.
- Standardize contract terms around the data-destruction process and then customize by supplier.
- Use workflow automation software to track contract end dates and to trigger the cybersecurity function to work with IT vendor management or global procurement on offboarding.
- Identify mechanisms for procurement to report to the cyber team when a supplier is offboarded.