intercity

SUPPLY CHAIN RISK MANAGEMENT

For small and medium enterprises

CONTENTS

The unique threats to Agriculture and food supply chains

How and why cyber criminals are targeting supply chains

What cybersecurity hygiene is, and how it can keep your business clean

Best methods to protect your business, suppliers, and customers

INTRODUCTION

When COVID-19 was at its peak, few industries could operate as usual. Companies were forced to transition to digital business processes and enable remote workers.

For organisations that were part of a supply chain ecosystem, the upheaval was greatest as distribution systems struggled to move goods, and order and payment processes, if not already digitised, simply stopped working.

One critical supply chain industry that was profoundly affected by the pandemic was agriculture and food production. Some workers in agriculture and food production were deemed essential and required to work in warehouses and manufacturing plants, farms, and distribution centres across the country. Others, for example, restaurant workers, were completely disrupted.

A CLOSER LOOK AT THE AGRICULTURE AND FOOD PRODUCT SUPPLY CHAIN

The critical nature of the agriculture and food production ecosystem means it is regularly targeted by various adversaries, from profit-seeking ransomware attackers to politically motivated nation-state attackers.

The Cybersecurity and Infrastructure Security Agency (CISA) defines agriculture and food production as one of 16 critical industry sectors. It is an enormous industry comprising approximately...

2.1 million farms

63,000 grocery stores[2]

200,000 production and processing facilities

930,000 restaurants

One would think that defending these industries and their many integrated supply chains should be a priority, but for many reasons of complexity, business size, and razor-thin operating margins it is not. This critical infrastructure is open to and too often falls victim to cyberattacks.

Growing Attacks Across Agriculture and Food production Align with COVID 19

Attacks against agriculture and food production organisations have been increasing. Ransomware attacks against JBS meat processing and AGCO, each netting over $11 million back in 2021[3], were just the tip of the iceberg. There were also multiple attacks against agricultural cooperatives during the 2021 harvest season, and in 2022, two cooperatives fell victim to attacks. There has even been an FBI advisory sent to US, Australian, and UK food and agriculture companies that are likely to be targeted by nation-state attackers during this harvest season.[4] The 2022 attacks (one in February and another in March) targeted grain processors and feed mills with Lockbit 2.0 ransomware.

Crystal Valley Minnesota Cooperative

In September of 2021, during harvest season, Crystal Valley Minnesota Cooperative was attacked, locking livestock feed orders for 25 million bushels of grain, and had to rely on other local cooperatives in the area to meet demand.

Crystal Valley worked closely with the FBI to recover from the attack and did not pay the ransom.[5]

NEW Cooperative

That same month in Iowa, the NEW Cooperative was also attacked by the BlackMatter group forcing the food storage and distribution to shut down their automated clearing house systems and shift to paper tickets for months while they recovered. As in most industries, most attacks (upwards of 75%)[6] on these smaller organisations go unreported.

Why is the food supply so at risk?

Risk across the agriculture and food production industry begins with complexity. As mentioned above, millions of organisations are involved in this supply chain; most are small and operate on low margins. Also, most of these organisations do not have dedicated cybersecurity analysts and few IT staff, nor do they have the resources to hire them. COVID-19 drove even faster digitalization in this ecosystem, and that speed of movement to technology reliance to meet supply needs left cyber defences a low priority. The result is risk and vulnerabilities across the entire sector.[7]

For many organisations, existing OT systems critical to production were connected to the Internet with no cyber defences[8]. The adoption of newer IoT and cloud systems are consuming budgets leaving little for cybersecurity tools. The worst scenario, feared by oversight agencies, is a major nation-state-sponsored attack against an entire country's agriculture and food production industry on a scale greater than NotPetya[9], which cost food-producing giant Mondelez over $100 million in lost revenue.[10]

The agriculture and food production ecosystems are an interesting point of reference, but in reality, they suffer the same struggles as most other supply chains; from oil and gas production to manufacturing, to automobile to retail, all major supply chains faced huge disruptions during COVID, and through rapid digital transformation, all have become more susceptible to cyberattacks.

HOW TO SECURE YOUR SUPPLY CHAIN

What can agriculture and Food Production, and for that matter, every supply chain organization do to secure your environment and ecosystem partners?

When we look at supply chain risk management (SCRM), point-in-time audits have some value when adding a new organisation into an ecosystem to ensure that the standards of cybersecurity hygiene are in place, but that is as far as the matter goes.

24x7 Cybersecurity Hygiene

Supply chain ecosystem members must maintain cybersecurity hygiene standards while the supply chain is operating, and in today's world, that is a 24X7 process. To achieve 24X7 cybersecurity hygiene standards, organisations must be able to continuously monitor and show their environments are protected and safe and that they are not putting anyone else in the supply chain ecosystem at risk. This is the basis for continuous compliance.

Continuous Compliance

As discussed above, we are seeing the more prominent vendors in the ecosystem (the ones with the most significant risk) pushing the need for continuous compliance out to the other vendors in the ecosystem as a "cost of doing business" with them.

We also see supply chains that have created ecosystem organisations to standardise continuous compliance requirements. Standardisation is beneficial because some supply chain members are asked for dashboards and reports from multiple companies in the ecosystem, often with variations in the cybersecurity requirements.

A company audited by multiple vendors, with numerous control variations and little preparation time, must have a mature cybersecurity program with integrated dashboards and reports. If they do not, continuous compliance will become onerous and costly. We have one customer who shares dashboards that contain 48 different variations on required controls across 55 different ecosystem partners.

FIVE BEST SECURITY PRACTICES

So how does a medium or smaller-sized organisation with finite resources meet these continuous compliance requirements, upgrade its cybersecurity hygiene, and afford it all? Here are five best practices that our customers shared.

1. SUPPLY CHAIN DEFENSE REQUIRES PROCESS-FOCUSED CYBERSECURITY

Many companies overlay security silos over their IT system and processes instead of deploying them to operate within the supply chain process. A good example is deploying endpoint detection and response agents on your laptops and workstations while not considering the defence of IoT systems, even though those systems are more integral to the supply chain process.

Best Practice

Map out supply chain processes and the IT systems involved. Supply chain process managers work with cybersecurity and IT teams (or partners) to map threat surfaces based on process, not on technology. Risk score all threat surfaces to determine which are at the greatest risk to attack and choose the best technology and method to protect them. Deploy defensive programs focusing on areas of greatest risk.

Consideration

That IoT system, or newly connected OT system to the Internet, may very well be the best starting point as opposed to adding new endpoint EDR tools or deploying new cybersecurity awareness programs. Start with the supply chain process and risk, not technology stacks or the latest hyped cybersecurity technology.

2. DEFINE AND DEPLOY CYBERSECURITY CONTROLS CONTINUOUS DEFENSE AND COMPLIANCE

A simple way to say this is to monitor everything. Have systems that watch critical systems and critical controls 24X7. This does not mean reducing or replacing existing security controls like multifactor authentication, but it does include watching those controls to ensure they are operating correctly.

Best Practice

Utilise AI, specifically supervised and unsupervised machine learning, to watch for anything that changes or does not match normal operations. Critical monitoring areas include your internal network traffic, all internet gateway traffic, directory systems (cloud and on-premise), and any device you can place a monitoring agent on (AV, EDR, etc.).

Consideration

A new ransomware variation in Europe called 'Prestige,' a supply chain attack striking at logistics and transportation companies. It uses sophisticated payload delivery strategies, and one of those includes copying the payload directly to an Active Directory Domain controller. The AD domain controller logs are amazingly noisy and challenging to monitor manually, and the adversary knows and exploits this. The good news is that there are reliable, affordable AI-based tools to monitor AD systems, including from our partner CyGlass.

Supply chain processes never stop, so your cybersecurity defences must always be on.

3. EXTEND CYBERSECURITY THROUGH EVERY STEP OF THE CONTRACT LIFECYCLE

Just as you took a "process-centric approach to your cybersecurity controls," do the same with all of your supply chain ecosystem contracts. When awarding a contract, stipulate compliance with necessary cybersecurity controls in the supplier contract. This step is well defined in a National Cyber Security Centre (NCSC) download you can find **here** and in the references. While the NCSC steps differ slightly from the Intercity & CyGlass list developed by our customers, it is equally valuable.

Best Practice

Ensure the contracts and any new agreements with suppliers, outsourcers, and contractors your organisation works with to support supply chain operations include provisions around cybersecurity expectations. These expectations should be defined regarding incident alerting, remediation capabilities, and threat and vulnerability data sharing. Also, clearly define reporting time expectations.

Consideration

Do not forget that terminating a contract also means removing all process and access integration created for the supply chain process defined in the contract. Make sure you regain control of your assets and remove all user and system access. This process is much easier when your contract clearly defines the systems, data sharing, and access that was created.

4. DEPLOY "PLATFORM OR COMPLETE" SYSTEMS THAT MONITOR OR WATCH OVER MANY THREAT SURFACES

This is the old cybersecurity strategy battle of "best-in-breed" versus "complete integrated platform" applied to SCRM. If you have a large cybersecurity team of 20 or more staff, best-of-breed technology with custom integration is possible. But an integrated platform is the way to go if you have a smaller team and limited resources. Regarding SCRM, look for a platform that covers the most threat surfaces possible. Be sure not to fall for vendor marketing hype; for example, Gartner places extended detection and response (XDR) at the apex of messaging hype with low actual value. Many vendors offering XDR only cover limited threat surfaces and have limited response capabilities, even though they claim otherwise.

Best Practice

When choosing technology, look for coverage of cloud, IoT, network, directory, data centres, remote locations, endpoints, etc. Utilise the processes-focused threat surface list from step one in this blog to create your requirements checklist and find your optimal tool. Use the requirements checklist to determine winning outcomes from vendor "proof of concept" trials.

Consideration

Deployment models for cybersecurity tools are changing, and new technologies deliver greater capabilities at lower costs. For example, CyGlass runs in the Amazon Web Services Cloud (AWS), eliminating the need for onsite hardware and software, thereby reducing management and updating costs. At the same time, using the AWS Cloud Platform adds instant scalability and AI computing power. New cloud-based deployment models are game changers for cybersecurity tools.

5. IMPLEMENT AUTOMATED, SHAREABLE DASHBOARDS AND REPORTS THAT REFLECT OPERATIONAL STATUS

The final step on our list can be considered the reverse side of the coin from step three. While you require your suppliers to meet and prove cybersecurity hygiene standards, your ecosystem partners will require the same of you. We hear from our customers that partners will need everything from daily access to threat and risk dashboards to on-demand audits completed by the partner's internal audit team or third-party auditors they contract with. The goal is to utilise automation to keep reporting requirements as straightforward as possible, especially for teams with limited resources.

Best Practice

Utilise cybersecurity tools with automated reporting capabilities in their product and include them in the base licence. Ensure that the reporting tool is easy to configure and that access to or PDR versions of the required reports can be created and sent out quickly and efficiently. Platforms incorporating correlated reporting capabilities across threat surfaces and integrated technologies are an even better choice as they reduce the number of reports that need to be generated.

Consideration

In some more complex supply chain ecosystems, customers have reported that they need to create hundreds of variations on a core set of control effectiveness reports. These variations can range from mixing control sets to adjusting the parameters on control effectiveness scoring levels. If you utilise a managed service partner (MSP, MSSP, MDR), ensure your contract includes reports and required configuration change capabilities at a cost within your budget. If you attempt this internally, your cybersecurity tool must consist of an easy-to-use reporting configuration manager. Doing this manually will be untenable.

CONCLUSION

Our final best practice comes from NIST [11] – continuous improvement applies to any SCRM program. Do not let your SCRM program stagnate, and encourage your ecosystem partners to keep improving their security measures. Create improvement and reporting plans with your suppliers to achieve improvements along agreed timelines. Remember, our adversaries do not rest, and neither can we.

References

1. https://www.cisa.gov/food-and-agriculture-sector
2. https://www.ibisworld.com/industry-statistics/number-of-businesses/supermarkets-grocery-stores-united-states
3. https://www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html
4. https://www.cybersecuritydive.com/news/food-supplier-cyber-risk-spreads-jbs/
5. https://www.food-safety.com/articles/7556-covid-19-the-food-supply-and-cybersecurity-coalescing-concerns
6. https://www.cybersecuritydive.com/news/senate-ransomware-cisa/624369/
7. https://eandt.theiet.org/content/articles/2022/05/agricultural-sector-at-risk-of-cyber-attacks-researchers-warn/
8. https://www.foodengineeringmag.com/articles/99362-control-system-vulnerabilities-put-food-beverage-at-serious-risk
9. https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html
10. https://www.foodbusinessnews.net/articles/9725-mondelez-not-yet-back-to-normal-from-cyber-attack
11. https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf

About Intercity

We've been enabling the highest quality of communication for businesses since we started back in 1986. Having accumulated the most exceptional people and technology to support our list of treasured and trusted partners, we have a strong foundation to stabilise and build businesses upon during the changing landscape of 2022–2023, as well as beyond.

Get in touch to learn more about how Intercity can help your business remain a strong link in any supply chain.

intercity

DO MORE

Contact us
on 0330 332 7933 or email
info@intercity.technology
intercity.technology