THE SECURITY SCAN GUIDE FOR MANUFACTURERS

Manufacturing's Second Fight: The Risk of a Cyber Aftershock

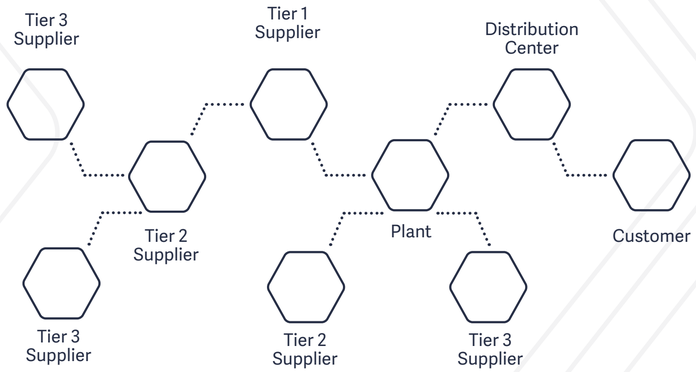
On Dealing with the Cyber Threat That Follows the Pandemic

zix

The Danger of a Double Dip

It is a curious fact that disasters often come in twos. Earthquakes are followed by tsunamis. Wars are followed by pandemics. And pandemics—including all the havoc they can wreak on supply chains—sometimes create immense, unseen vulnerabilities in other areas.

The 2020 pandemic is well underway and all things considered, manufacturers have responded admirably. Some have transitioned to producing life-saving medical supplies like respirators, masks, and sanitizers. Nearly all have peered deep into their supply chain to play a sort of three-dimensional chess. They've anticipated risks and picked out Tier 1 and Tier 2 suppliers hamstrung by lockdowns or logistics and replaced them with an ever more complex web of multi-tier supplier networks.



Technology has certainly helped, or so it seems. Manufacturers have embraced Industry 4.0. Nearly half use smart sensors and most have industrial control systems (ICS). They've moved to the cloud, deployed smart robots, and are networking nearly everything. That's helped relieve some of the present risks of disruption, but now they're facing a double dip: not just a resurgence in the supply-chain kinking and border-closing effects of COVID-19, but the twin disaster of cybersecurity.

> *Phishing attacks are up 350% since the pandemic.* -UNICRI

You see, the very connectedness of manufacturing operations plus the speed at which they've had to maneuver has lit up a vast constellation of new vulnerabilities. For manufacturers eager to avoid the double dip of surviving the COVID-19 logistics crisis only to be irreparably breached and lose vital intellectual property (IP), it's time to secure all those unconnected endpoints and channels. And in particular, the most sensitive one—email.

In this guide, we'll explain why manufacturing's largest threat, cybersecurity, is also its greatest opportunity. It's a massive issue for all. The winners in the coming months and years will be those who secure their emails and file transfers.

Fast facts because of COVID-19:

78% of manufacturers anticipate a financial impact

53.1% of manufacturers anticipate a change in operations

35.5% of manufacturers are facing supply chain disruptions

** Source: NAM*

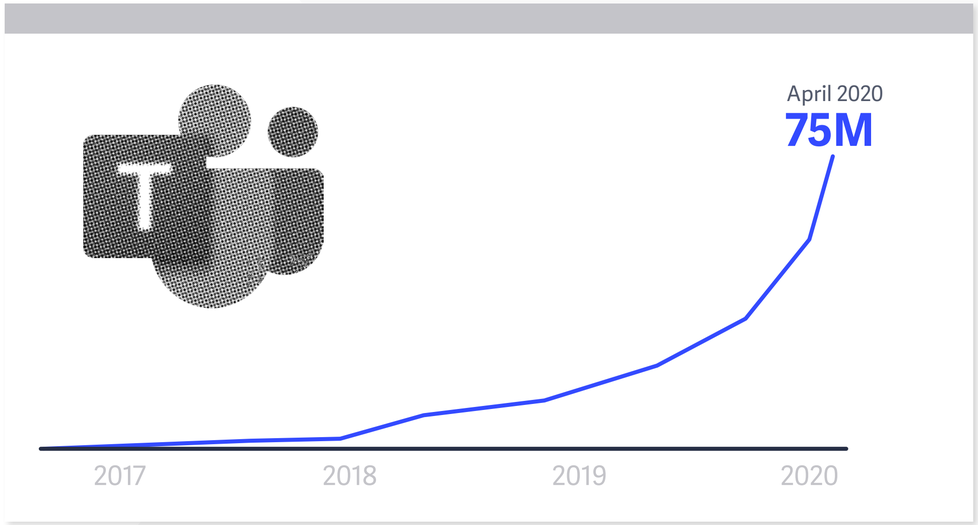
Part 1. Supply chain shock

Even before the pandemic, cybersecurity was manufacturing's top threat. More connectivity means more exposure, and the increase in connected devices is perfectly correlated with the increase in breaches. In 2010, the Department of Homeland Security issued 10 advisories to manufacturers to secure their equipment. In 2018, it issued 223. And despite the present crisis, the number of businesses with on-premise internet of things (IoT) platforms including 3D printers, assembly robots, and automated packaging will double by 2023.

The dangers of ineffective cybersecurity can be summed up in two words: theft and disruption. Once inside a network, cybercriminals commit financial crimes and extortion—sometimes by locking down equipment until a ransom is paid—and intellectual property (IP) theft. The latter is particularly harmful because a decades-long lead in development can be lost overnight. IP is notoriously difficult to suppress once it's out into the world. For pharmaceutical, high tech, and semiconductor manufacturers, such a loss can threaten the very existence of the business.

It has never been easier to steal IP, or to accidentally expose it. Workers in over 100 nations have been variously instructed to work from home, meaning more sensitive information is being transmitted via email and over collaboration platforms. Microsoft Teams, for instance, leapt from 14 million users in late 2019 to 75 million users in April 2020. New tools, new stressors, and a lack of conventions for how to safely transfer files creates a particularly inviting target for phishing attempts, which have increased 350% since the pandemic began. Rushed employees are more likely than ever to click malicious links.

It has never been easier to steal IP, or to accidentally expose it.



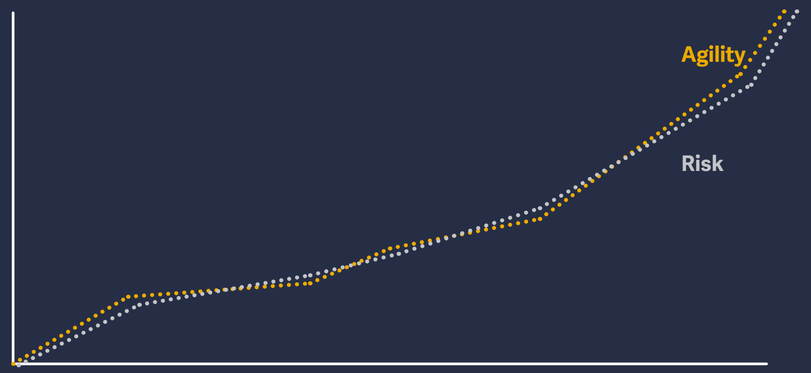
Collaboration platform Microsoft Teams leapt from 14 million users to 75 million in under six months.

Surface area = cyber risk

The way to think about securing your quickly expanding ecosystem is to think broad, not narrow. Your greatest risk factor is your total surface area. The more endpoints, the more sensors, the more emails, the more suppliers, and the more file transfers, the greater the number of weak links. And at present, the growth in those links appears exponential.

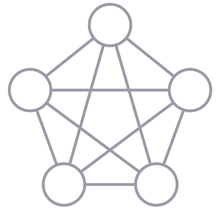
Consider the classic networking equation known as the N-squared problem. When you have five machines in an ecosystem, there are ten connections you must secure. But when you double the number of machines, you suddenly have 45 connections to secure. In a multi-tier supplier network that has become more complex in an effort to be more agile, the risk is far greater. In fact, the more agile an organization has become, the higher the risk.

The total breadth of your defense matters. Cybercriminals are looking for weak, unsecured connections—email correspondence with overseas suppliers, Microsoft Teams chats with improperly trained contractors and the like. They'd much rather pass through an open digital door than have to break a lock.



N2 problem diagram

2 endpoints
1 connection



5 endpoints
10 connections

10 endpoints
45 connections

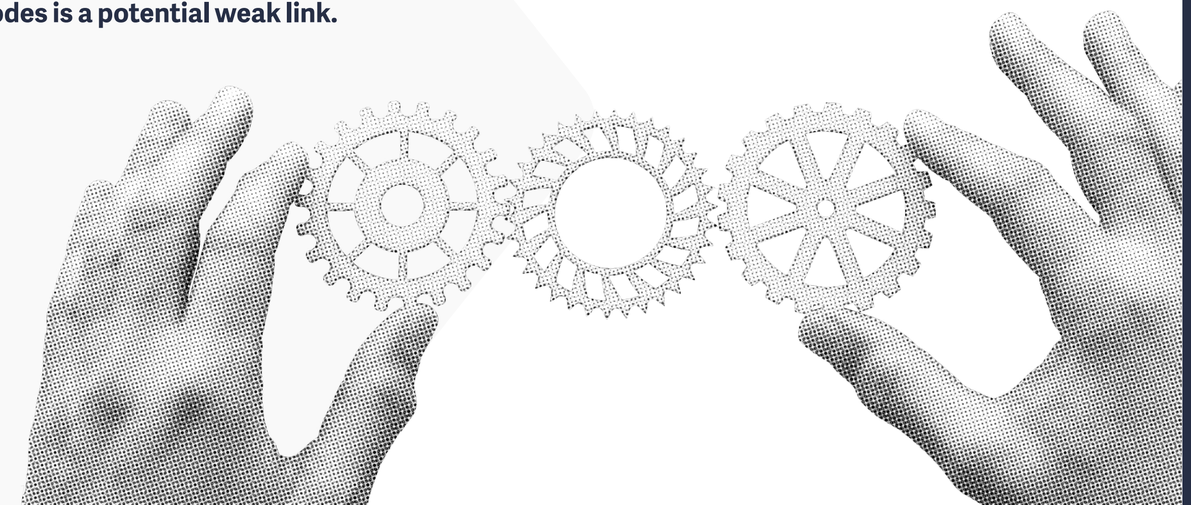
So what does your surface area look like?

The same diagram you've created to harden your supply chain and identify risks and potential supplier disruptions is just as useful for assessing your cybersecurity risk. Supply networks are communication networks. Anywhere there is an exchange of goods, there's an exchange of emails and files.

Supply networks are communication networks.

To assess your risk, identify what sensitive information your organization receives, generates, holds, and processes. Identify the channels each of those types of information are supposed to be communicated across, and then identify all the ways they're actually being communicated. Is a machine operator sending a picture of diagnostic data via SMS text because it's easier than finding a desktop terminal? Is an ordering manager sending financial information via personal email because the supplier lacks a secure portal? Are engineers transferring schematics to a new supplier over the public cloud with a service like WeTransfer because of email file size limits?

Each of these nodes is a potential weak link.



New Industry, New Endpoints

Industrial control systems (ICS), smart sensors and IoT present new vulnerabilities -Deloitte

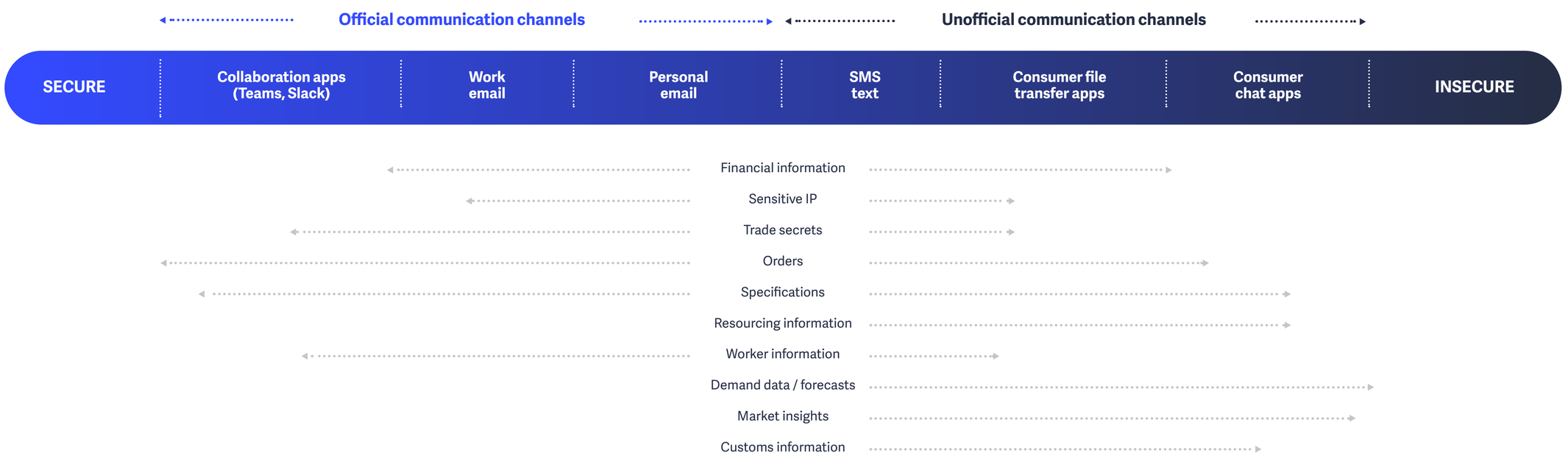
35-45% use sensors, smart products, or mobile apps

52% say connected products transmit confidential data like banking info, SSN

Only 55% encrypt the data

Supply Chains: More Complexity, More Cyber Risk

Where does sensitive information travel in your supply chain?



Can your business put on a united front?

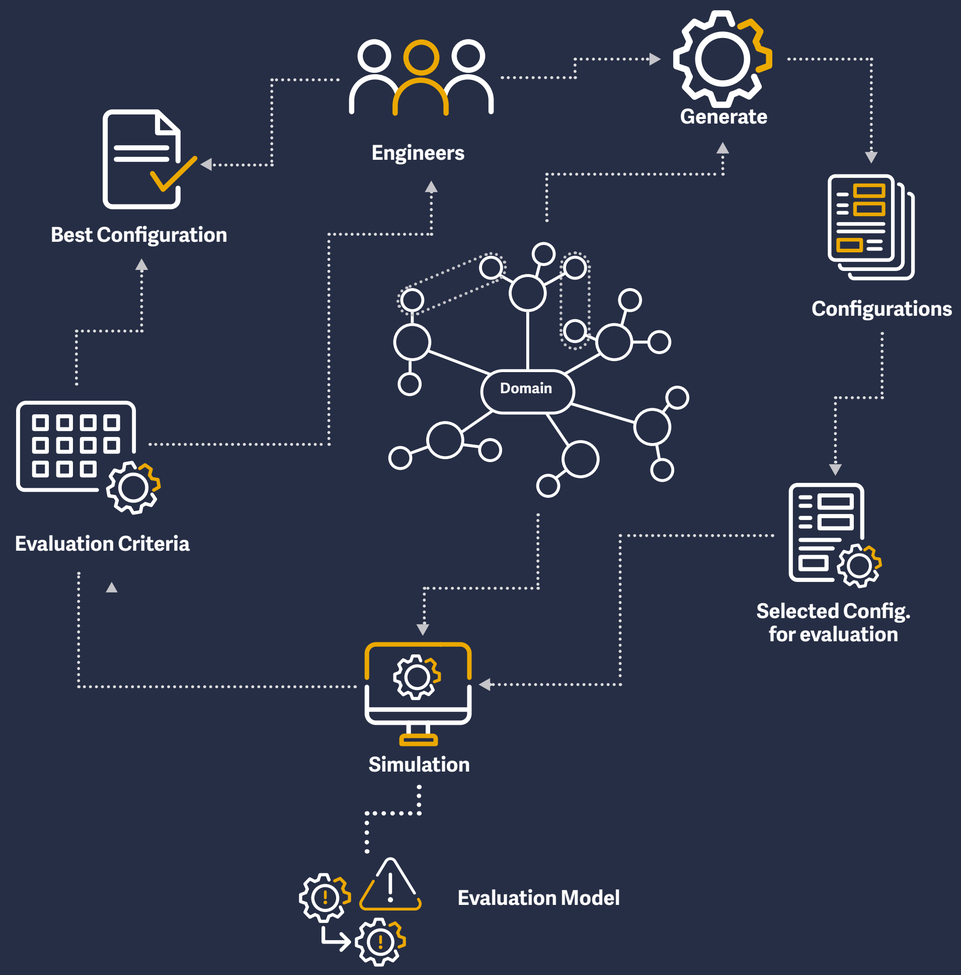
The issue of increased surface area might be manageable were most manufacturers able to present a united security front. But due to a long history of silos, most experience what's known as the IT/OT gap. That is, the company's IT team and the operational technology (OT) teams fail to coordinate in precisely the areas they'd need to if they wanted to secure the business.

"Cybersecurity experts and engineers trained to operate specialized equipment often don't share data with each other, and details about corporate and industrial operations are siloed," reports The Wall Street Journal. "That means employees might be poorly equipped to deal with hackers intent on damaging industrial plants."

Case in point: Some 40% of manufacturing CISOs report to someone other than the CEO or CIO. Often, the industrial control system (ICS) that includes a majority of the company's smart sensors, does not fall under their purview. The same goes with sensitive IP controlled and secured by the research and development (R&D) team.

If the people evaluating, installing, and operating new shop floor machines are not included in security audits and incident response plans, manufacturers are vulnerable. For security, the left hand must know what the right is doing.

> *Only 33% of manufacturers said IP protection falls under the CISO -Deloitte*



Part 2.
The unguarded door

In this chapter, we've summarized all the aforementioned issues into four major challenges that manufacturers face. Together, they present a threat of double dip—a looming disaster of breach or IP theft that could be as bad as the supply-chain issues caused by COVID-19. However, as we will explain near the end of this chapter, these four major challenges also present tremendous revenue growth opportunities.

The Challenges Summarized:

1 No plan to deal with the impending cyber shock

COVID-19 has exposed organizations that have not put a disaster preparedness plan in place. According to Gartner, 50% of manufacturers will have failed to recover from the impacts of COVID-19 due to inconsistent analysis of ecosystem dependencies. These organizations have had to cut, divert, and deprioritize resources and personnel without fully understanding the long-term effects, much less the impact on their cybersecurity.

Many of the solutions to disruption have involved more software, more partners, new partners, and greater flexibility. This has created more endpoints and dependencies that cybercriminals are already exploiting. **To adapt, manufacturers must now secure their most vital channels of communication: email and file transfer.**

2 More endpoints and a fragmentation of responsibility

Manufacturers that have embraced Industry 4.0 technologies, combining the internet of things (IoT) with the Internet of Systems to create smart factories. Shop floor robots communicate with an industrial control system (ICS) and can order their own parts, or alert partners of supply issues. These digital sensors are often poorly protected and not included in security audits or incident response plans.

In addition, many manufacturers have multiple, overlapping response plans that don't always take each other into account. A CISO may have overall responsibility for company security, but no control over shop room floor systems, sensors, or the ICS. **To adapt, companies must centralize security under one title, and standardize systems across the business. Ideally, they'd even standardize across partners.**

Most common threat vector: **business email compromise** (BEC). -Verizon

35-45% of manufacturers use sensors, smart products, mobile apps. -Deloitte

52% say connected products transmit confidential data like banking info, SSNs. -Deloitte

Most manufacturers experience the IT and OT split. -Chief Executive

3 More remote work

More sensitive data is being shared across more media and networks, from email to collaboration apps. That could include design files, sensitive IP, and the like. Poorly secured communication networks are a top attack vector, and negligent employees are a leading cause. **To adapt, manufacturers need to weave cybersecurity into their remote work policies and provide secure file transfer tools.**

Only 52% of surveyed executives are confident or extremely confident in their organization's security. -Deloitte

4 in 10 threats involve employees; **75%** lack skilled resources. -Deloitte

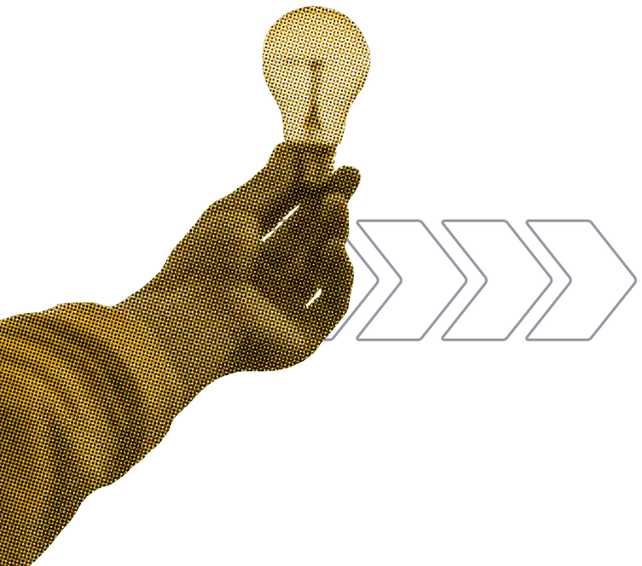
4 Financial and liquidity limitations

Disruption means many manufacturers are in a precarious financial position. Few can afford the complete security overhaul necessary to secure all their endpoints—in particular, the systems of contractors, suppliers, and customers, which may not be as hardened, and present a backdoor for cyber threats. **To adapt, manufacturers need cybersecurity systems that are cost-effective and allow them to scale seats up and down, to accommodate fluctuations in the business.**

The opportunity in all this

There is good news after all. If a manufacturer can solve the aforementioned four issues easily and affordably, they're at a competitive advantage. Whereas competitors face risk and exposure, those who have addressed cybersecurity are more agile, more profitable, and more able to swiftly enter new markets without incurring unacceptable risk.

Specifically, dealing with these issues allows manufacturers to:



Free up budget:

If manufacturers find affordable cybersecurity platforms and partners, they free up capital, and can reallocate it to operations. For instance, an email encryption service that also offers threat protection may allow them to consolidate vendors, and add or subtract seats in real-time.

Adopt new technologies faster:

IT and OT teams that are more aware of their cyber risks can seize upon hyper-growth opportunities. For instance, if they can freely and securely communicate with new suppliers, they can more quickly cut costs, or spin up product lines like sanitizers or surgical masks.

Invent better processes:

With more elastic software services, manufacturers are freer to scale up or down business units quickly, or reallocate head count.

Lower risk of IP loss:

Manufacturers with uniform email and file transfer security are better able to avoid existential risk, like IP loss or financial fraud.

Faster innovation:

When manufacturers can communicate with greater freedom and security, innovation happens faster. Employees aren't hamstrung by file send limits, and files aren't as susceptible to interception.

How to seize the opportunity?

In the next resource in this series, **The Security Scan Playbook for Manufacturers**, we provide a step-by-step checklist for manufacturers to address these issues, and seize the opportunity.

The Security Scan Playbook for Manufacturers

Access my copy of the playbook