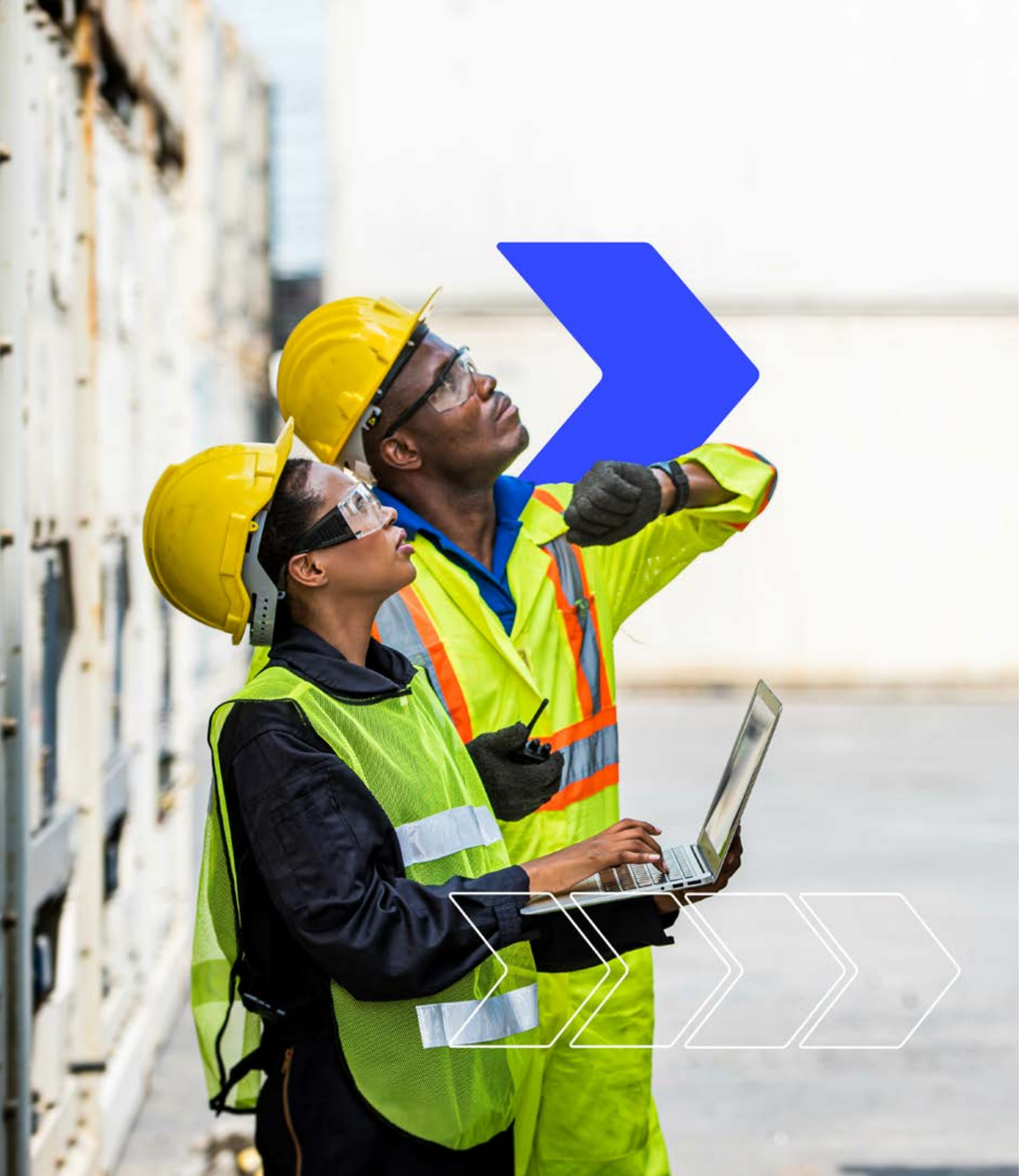
THE SECURITY SCAN PLAYBOOK FOR MANUFACTURERS

Manufacturing's Second Fight: How to Avoid Cyber Aftershock

A Step-by-Step Playbook for a Post-Pandemic Email Defense

zix



The Worst Is Avoidable

As we covered in the companion piece to this playbook, The Security Scan Guide for Manufacturers, disasters often come in twos. All the ways manufacturers have responded to the pandemic supply shock have created a cybersecurity shock, and now is the time to secure their endpoints and sensitive communication channels—especially email.

> A vast majority of those attacks happen through business email. And most of those, via phishing attempts.

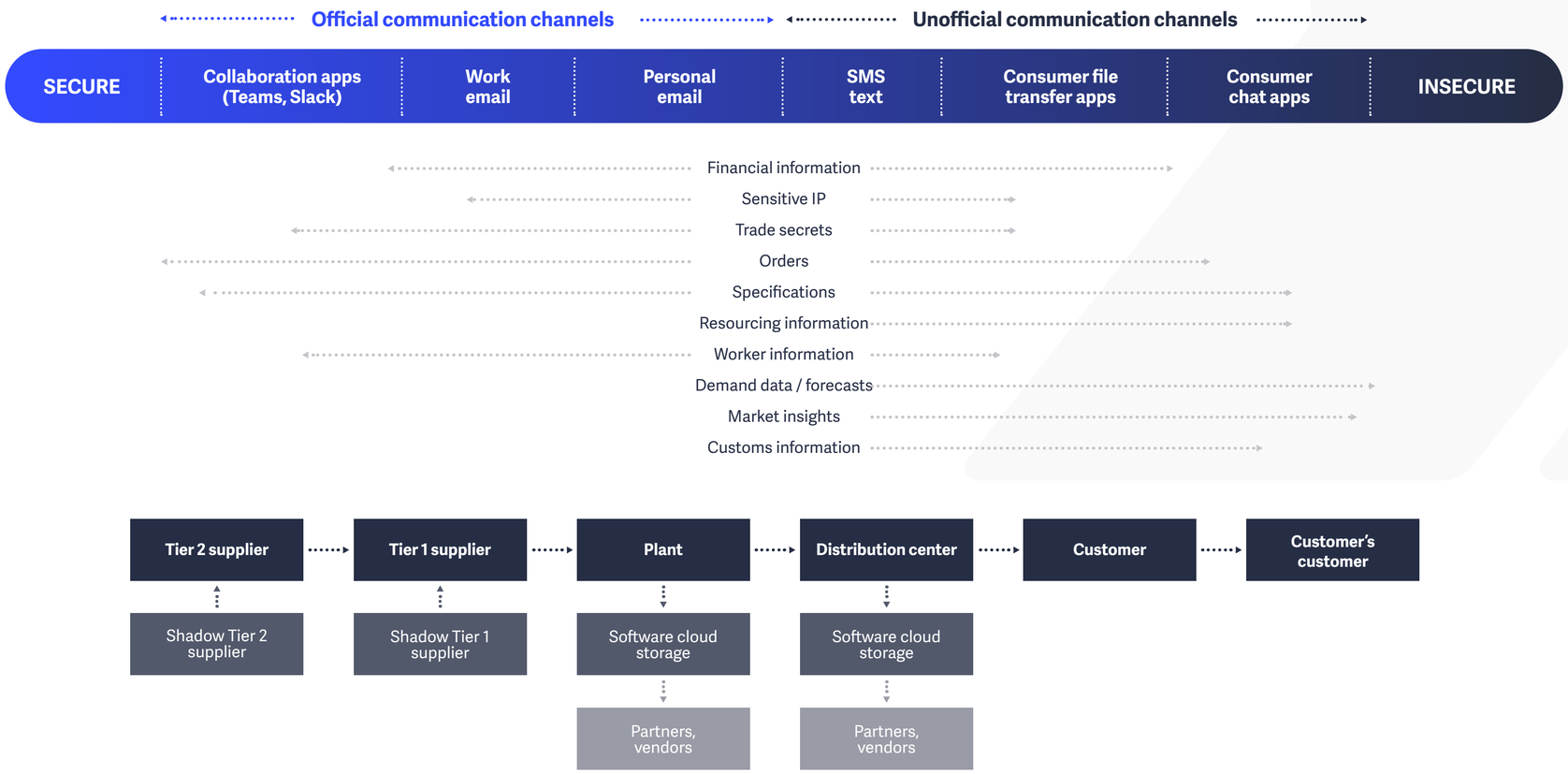
With more remote work, more complex multi-tier supplier networks, and more sensors on the shop floor, agile manufacturers are at risk of malicious attacks. A vast majority of those attacks happen through business email. And most of those, via phishing attempts.

In this playbook, we provide step-by-step instructions on how to conceptualize your new, expanded defense, and actions you can take to harden your network continuously.

Part 1. How to Organize Your Defense

Your supply chain is also a communication chain. Anywhere supplies flow, so does information—some of it, sensitive. Every channel and touchpoint in that chain is potentially a weak link where information is either exposed or gaps are left open for malicious actors to enter. To understand the areas where your communication is soft and prone to intrusion, diagram it.

Below, a model of a typical supply chain and what types of information travels where.



Attack Surface Area

To reduce your vulnerability, think about reducing your attack surface area. More endpoints and more moving parts means more risk. Some manufacturers might consider starting by standardizing their communication channels. For instance, if different business units use different email clients, some hosted and some on-premise, it's more difficult to secure.

They should also standardize their security audits and response plans, and have one plan to encompass the entire business. Industry 4.0 has created a fragmentation of responsibility where security teams often aren't responsible for securing sensitive IP, or for evaluating shop floor machinery. This is a mistake. Plans must be holistic to be effective.

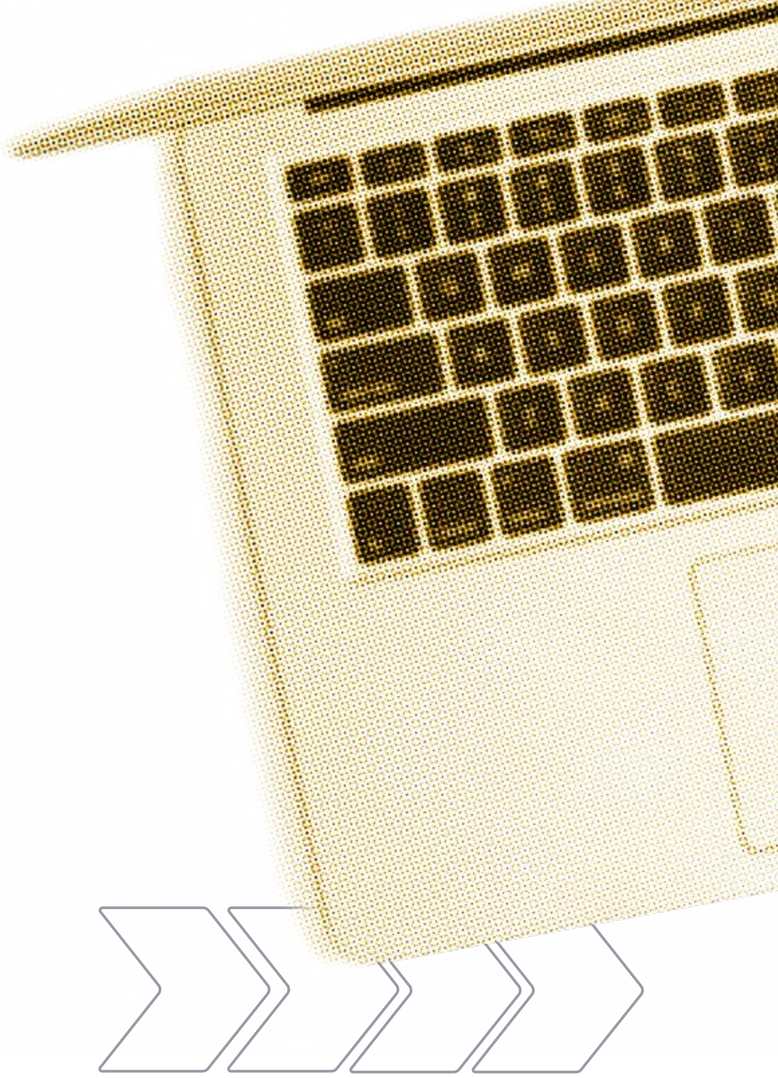
Take time to craft your own supply chain communications diagram, and to check in with different teams, departments, and plants. What unofficial communication channels do they rely on? Why? What do they transmit over it?

In the next chapter, we detail the challenges that come out of insufficiently secure communication chains, fixes, and the opportunities they create for better financial performance.

> To reduce your vulnerability, think about reducing your attack surface area. More endpoints and more moving parts means more risk.

Part 2. Challenges and Solutions

For each challenge, we detail steps to remediate and provide ongoing protection. For more details on the challenges, revisit this playbook's companion piece, The Security Scan Guide for Manufacturers.



1 Challenge: No plan to deal with the impending cyber shock

Solution: Secure your email communications and file transfers

- **Impersonation protection.** Should offer a proactive approach that accurately halts impersonation attempts and threat actors.
- **Deep-level attachment and URL analysis.** Should stop known threats and zero-hour malware through static and dynamic analysis.
- **Compliance-grade email encryption and secure file sharing.** Should secure your email and file transfers with one platform that provides 1) email encryption, 2) email threat protection, and 3) secure, large file transfers. When your email software includes a feature to transfer large files it reduces the chance that employees turn to unsecured, third-party apps like Dropbox and WeTransfer.
- **Integrated email continuity.** Should maintain business communication even when under a severe DDoS attack.
- **Simplify your email security infrastructure.** Where possible, consolidate cybersecurity vendors and give preference to those that offer multi-function platforms, such as ones that offer both encryption and threat protection. This prevents coverage gaps.
  - Scan all mailboxes for suspicious permissions
  - Lock inactive mailboxes
- **A proactive partner.** Your email security provider should employ a 24/7 threat analyst team to identify emerging issues for you.

Benefit: ✓ Adapt to changing threat landscape ✓ Lower risk of IP loss

2 Challenge: More endpoints and a fragmentation of responsibility

Solution: Scale security with software, empower the CISO or CIO

- **Centralize security responsibility under the CISO or CIO.** The more you can standardize security responsibility under one title, the more effective it will be. A common choice is the CISO or CIO. They should be responsible for IP security and the security aspects and response planning for operational technologies (OT).
- **Coordinate security with suppliers.** Network security is no good if suppliers or contractors aren't also secure. Push to standardize partners on an email encryption network or a supplier-approved file sharing solution.

Benefit: ✓ Invent better processes ✓ Lower risk of IP loss ✓ Faster innovation

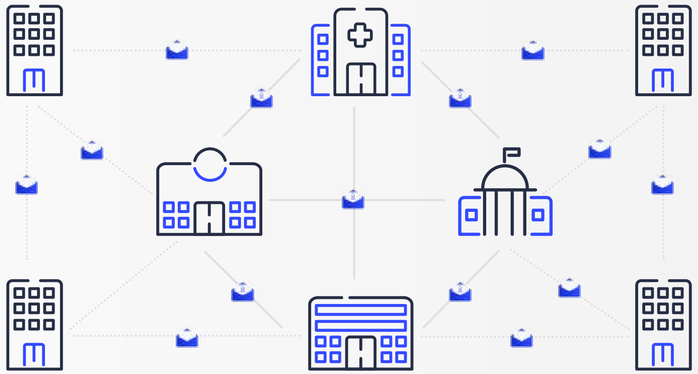
3 Challenge: More remote work

Solution: Launch a remote work plan that includes cybersecurity

- **Provide an intuitive email security software.** Even better than training, seek out email security software that is easy to use. The more intuitive the software, and the fewer decisions it forces upon users (such as requiring them to press a button to encrypt an email), the safer everyone is by default.
- **Provide phishing awareness and cyber threat training.**
- **Standardize on communication channels.** Get all business units using the same email client, secure file sharing solution and the same collaboration platform. The fewer systems, the fewer weak links.
  - Where possible, securely incorporate suppliers and vendors into collaboration software like Microsoft Teams, to prevent sensitive communications from happening over SMS text.

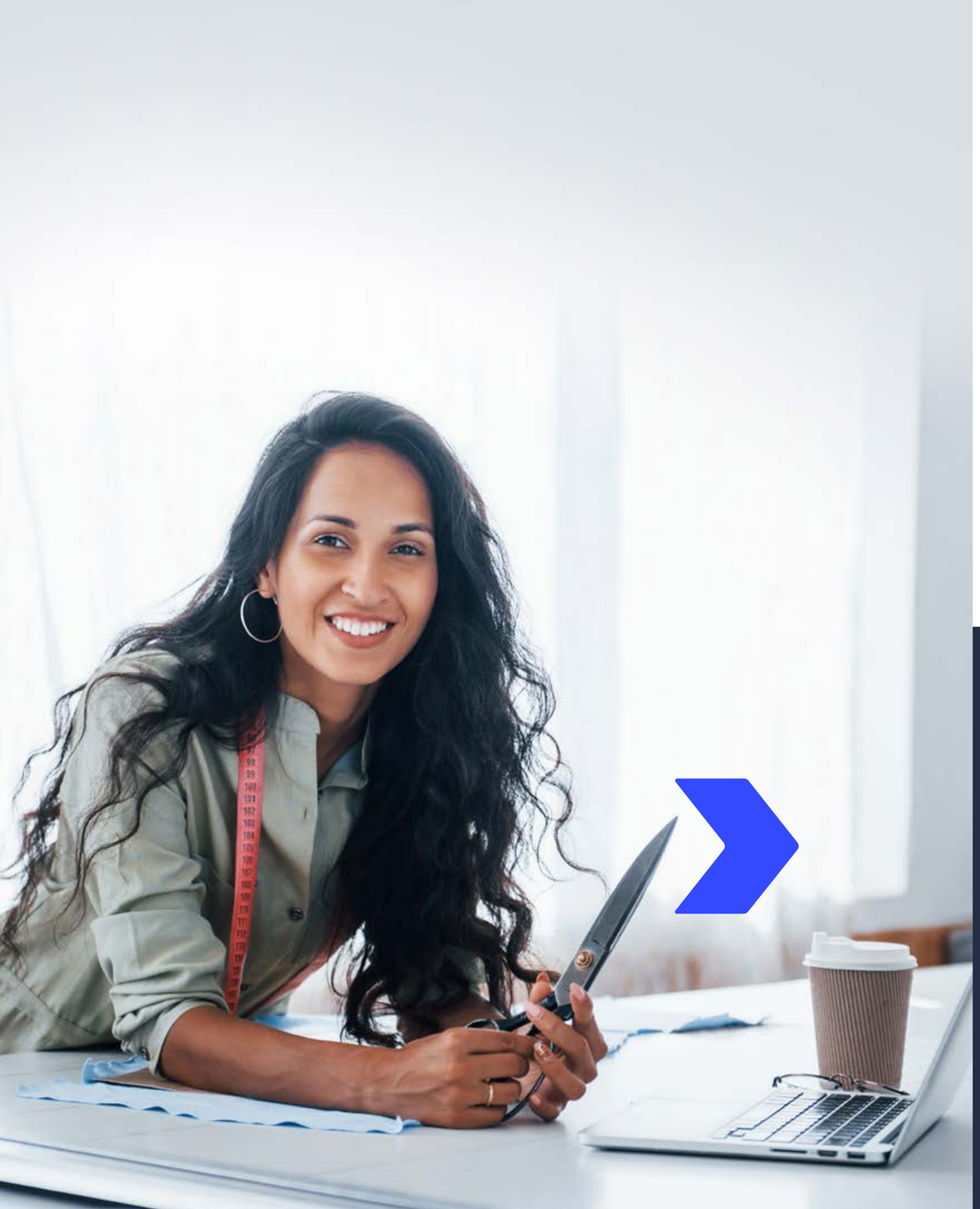
Benefit: ✓ Lower risk of IP loss ✓ Faster innovation

Zix Encryption: Some encryption vendors, like Zix, offer an entirely secure network, so messages between two Zix customers never touch the open internet.



4 in 10 threats involve employees. -Deloitte

75% of companies lack skilled resources. -Deloitte



4 Challenge: Financial and liquidity limitations

Solution: Consolidate cybersecurity vendors to cut costs

- **Aggressively-priced solution.** Email Security is a mature market, so top-tier vendors like Zix, Mimecast, and Proofpoint can maintain effectiveness and protect email without much user intervention. The difference is price. With budgets as thin as ever, Zix offers the best price hands down.

Benefit: ✓ Free up budget

From Double Dip to Rising Revenue

The coming cybersecurity double dip threatens manufacturers who've had to grow more agile as a result of the pandemic. It affects nearly all—and by that token, presents a massive opportunity.

Those manufacturers that are able to affordably scale their email and file transfer security across their operations and through their supply chain come out ahead. They're better able to reallocate much-needed capital, seize on hyper-growth opportunities, and communicate freely and securely with new suppliers.

It's an agile manufacturer's world, and in it, the secure will dominate.

Learn more at Zix.com/manufacturing.