Manufacturers ALLIANCE FOUNDATION

IN PARTNERSHIP WITH FORTINET®

# Advancing Digital Transformation in a Time of Unprecedented Cybersecurity Risk

NOVEMBER 2023

# Overview

The manufacturing super cycle of investment in the U.S. is underway, bringing a wave of innovation and digital transformation. The smart factory is a question of when, not if, as manufacturers embrace new technologies to make themselves faster, more productive, and more competitive.

With this comes an additional dimension of connectivity and risk for manufacturers. Cybersecurity is no longer a theoretical threat affecting a few distant companies in other industries but a very real one, hitting their peers, their suppliers, and their own operations. Breaches are catapulting operations backwards to paper and manual processes used by past generations and costing quarters of growth.

Every manufacturer is at a different stage of cyber maturity. Some are advanced; others are just starting. Wherever they are on the cyber-preparedness spectrum, they have one thing in common: Their attack surface is increasing with every stage of digitalization. Attacks are more frequent, more sophisticated, and more damaging.

Manufacturers have made significant progress in the past few years in terms of prevention, monitoring, and analysis of their own systems. They are also scrutinizing vendors and service providers. But the question remains: Are they moving quickly enough to stay ahead of hackers and organized cybercriminals?

At this critical stage, the success of IT/OT collaboration may be the secret sauce deciding whether digital strategies are successful or painful. IT and OT teams need to find ways to share scarce skilled talent and get beyond the mindset of competitive interests to find mutual goals that balance security and operational priorities.

Sophisticated tools and best practices are expanding every day to make it easier to prevail as a defender. As manufacturers learn more about these technologies and practices, they will make it possible to tap into the benefits of digitalization while minimizing risks and becoming more competitive and resilient overall.

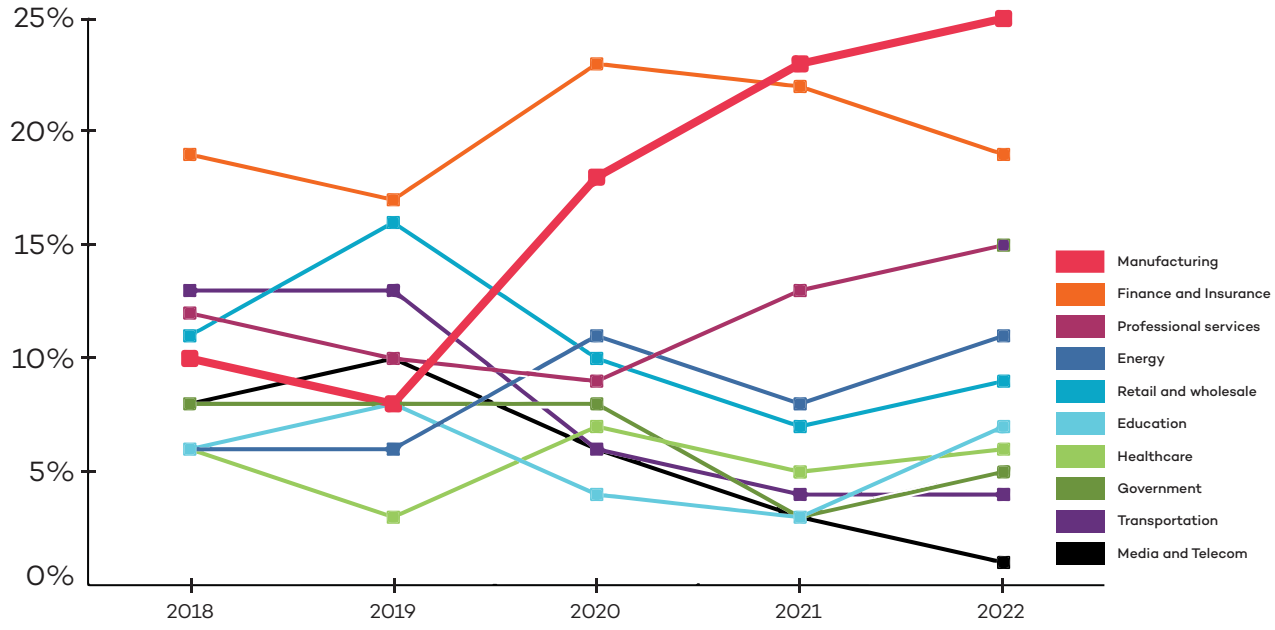
# Digital Transformation in Manufacturing

Industrial companies are breaking ground on new factories, adding capacity, and embracing innovative technologies at the fastest pace in decades. The numbers are breathtaking. Manufacturing construction climbed to $108 billion in 2022, the **highest annual total on record**. The share of Foreign Direct Investment going to manufacturing (excluding acquisitions) in 2022 was more than **double the average** seen in the previous seven years. Economists are calling it an **investment super cycle** and predicting it to extend well into the second half of the 2020s.

Manufacturers are deploying smart factory tools that enable them to deal with recent curve balls, such as supply chain delays, fluctuations in consumer demand, and the skilled talent crunch. Technologies like machine learning, Industrial Internet of Things (IIoT), digital twins, cloud, and artificial intelligence (AI) are just a few of the tools they're utilizing to cope with recent accelerations and disruptions. Collaboration between IT (information technology) and OT (operational technology) can mean the difference between success and failure for a new digital strategy.

While the benefits of digital transformation are undeniable, more connectivity equates to heightened vulnerability to cyberattacks. Smart and connected devices on the factory floor are high-value targets not only because of the intellectual property they contain but because one day of downtime can cost millions. Indeed, manufacturing has recently come into the crosshairs of organized cybercriminals making it the number one target for hackers. In 2022, **25% of all cyberattacks** were on manufacturing, up from 10% in 2018.

## Share of Cyberattacks by Industry 2018–2022




Source: **X-Force Threat Intelligence Index 2023**


Manufacturers are making OT cybersecurity a priority like never before, but are they doing enough to stay ahead of the threat? To better understand how companies are addressing these heightened risks, Manufacturers Alliance Foundation and **Fortinet** partnered to study their strategies for coping with the new threat landscape, the state of IT/OT collaboration, promising tactics, and barriers to progress.

This study is based on a survey of 155 U.S.-based mid-Cap to large-Cap manufacturing companies and interviews with IT and OT executives representing a variety of company sizes and industries. It builds on a related study published by our organizations in 2020, allowing us to track where companies have made progress and where they are stalled. In this 2023 study, we have placed particular emphasis on the state of collaboration between IT/OT teams and best practices to enhance OT security.

***Top-level findings reveal that companies have advanced in maturity in terms of security analysis, evaluation, monitoring, and assessment of their own operations and third-party vendors. At the same time, companies struggle with IT/OT collaboration and communication, the availability of skilled talent, and the galloping pace of change. That tempo is too often set by attackers with an appetite for profit and track record of innovation.***

Many companies are at the beginning of their OT cybersecurity journey and looking for insights and best practices about how to protect the OT space without hurting productivity. Others are well on their way with advanced programs and policies yielding impressive results. Regardless of their stage, the vast majority of the manufacturers who took part in our study express an increased awareness of the importance of cybersecurity as a business risk and the need to speed up IT/OT collaboration for a competitive advantage.

# Manufacturers Are More Focused than Ever on Cybersecurity

Cybersecurity is now front and center for manufacturing. In the past few years, we have seen high-profile attacks on food processing, consumer packaged goods, and energy companies. The risk of cyberattack has shifted from theoretical to real. As one IT executive put it, "My CFO is now sufficiently scared" because a major manufacturer nearby had been hacked. When asked to rank cybersecurity as a business risk, 78% put it in the top five, up from 70% in our 2020 survey. Over 80% experienced at least one breach resulting in unauthorized access to data in the previous year. Of those, 15% experienced six or more breaches. The most common types of security incidents they reported were phishing, malware, spyware, and ransomware.

Looking ahead 12 months, manufacturers identified extortion through ransomware as their top concern, outpacing their fears of nation-states and insider threats (both malicious and unintentional). Indeed, 36% fell victim to a ransomware attack last year, up significantly from the 23% in our 2020 survey. The rapid monetization of this tactic makes it a favorite in the world of organized cybercrime. Contrary to FBI warnings against meeting part or all of the ransom demands, more than 70% of organizations pay, according to **research by Fortinet**.

With threats surging, it is not surprising to see more manufacturers beef up their cybersecurity preparedness. In 2020, 10% said they were "just starting" to secure OT. In 2023, that number receded to 3%, a promising sign that many in the beginner class have advanced.

When asked how their OT security approaches will change over the next three years, more than 90% of respondents said they're focused on implementing new solutions to address risks specifically affecting OT. Increasingly, this preparation involves the use of security analysis, monitoring, and assessment tools, which 52% identified as "extremely important," a significant uptick from 45% in 2020.

**"Organizations in the manufacturing sector paid the requested ransom more often than those in other industries. And the amount requested was also typically higher—in fact, in 25% of breaches among manufacturing companies, the demanded ransom was $1M or higher."**

Source: The 2023 Global Ransomware Report

Ken Brown, Director of Cybersecurity and Governance at Milliken & Company, talked about the opportunity to gain additional transparency through passive vulnerability scanning, which tests security without any direct interaction with the targets, such as sending packets. "We are continuously discussing ways of increasing our visibility, particularly in the OT space. In a limited way, we are utilizing passive vulnerability scanning. By listening to network traffic, we can identify OT systems and their vulnerabilities without risk of causing disruption to them."

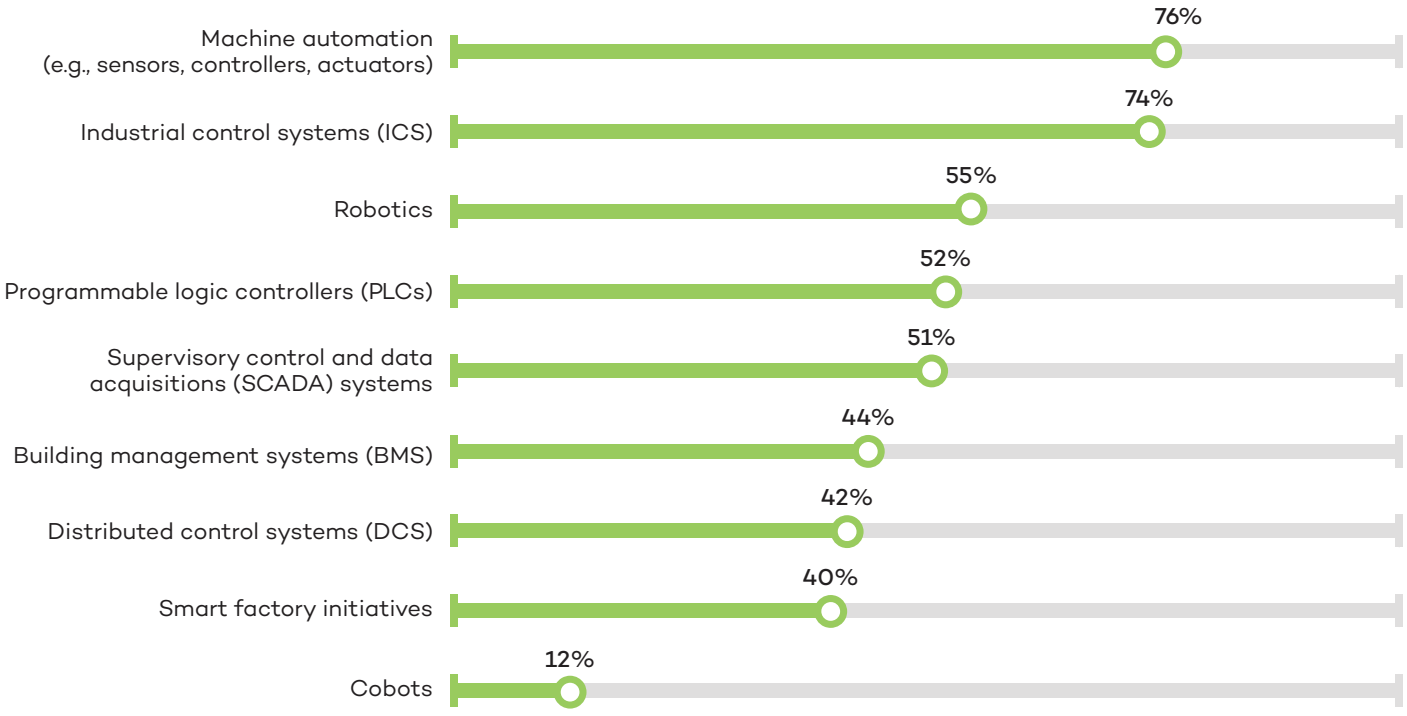
# Manufacturers Have Made Significant Progress in Important Areas

Without a doubt, securing the OT space requires visibility into the systems being used there. Rogue, insecure equipment on the plant floor is becoming less of a problem for the majority of companies. Prior to procurement, OT equipment is subject to IT or cyber review, according to 87% of the companies we surveyed.

With OT budgets set to rise significantly in the next 12 months, according to 32% in our survey, such reviews will play a pivotal role in ongoing cyber preparedness. Jicky Kong, Vice President of Manufacturing at **Simpson Strong-Tie**, talked about the importance of having "a robust, systematic process where we get the right people at the right level who deal with the equipment every day involved in the process. That's our philosophy here."

One cybersecurity executive for a manufacturer in the industrial material handling space told us his company is vetting and also quarantining all new OT equipment. "It's all about working with the facility groups. They're very positive. They understand that better OT hygiene and operational management will help them be more productive and improve uptime. So they get it."

## What OT Systems Are Included in Manufacturers' Growth Plans

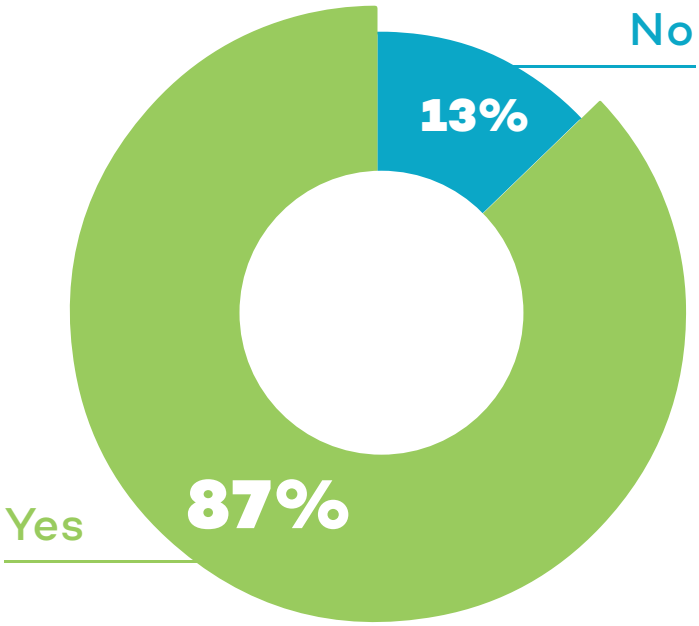



Source: Manufacturers Alliance and Fortinet survey

Controlling access to the network is another method of addressing a new piece of equipment that hasn't been vetted. "Deploying Network Access Controls has helped us maintain an accurate inventory. If an unknown device is added to our network, it is quarantined until it is approved by Cybersecurity. It cannot connect to our internal network unless we know about it." Ken Brown told us.

For equipment already in place, regular audits and assessments are critical elements in the cybersecurity equation. Manufacturers have stepped up their efforts here with 48% telling us that they have conducted audits or assessments related to OT security within the past six months, up from 44% in 2020. In terms of cadence, 23% perform these audits and assessments on a monthly basis, 49% quarterly, and the rest less frequently. To be able to conduct these assessments requires asset discovery and visibility into the operating environment, which 85% consider very or extremely important.

## Companies that Perform an IT or Cyber Review Before Purchasing OT Equipment




Source: Manufacturers Alliance and Fortinet study

## Selecting Middleware with Security Designed In

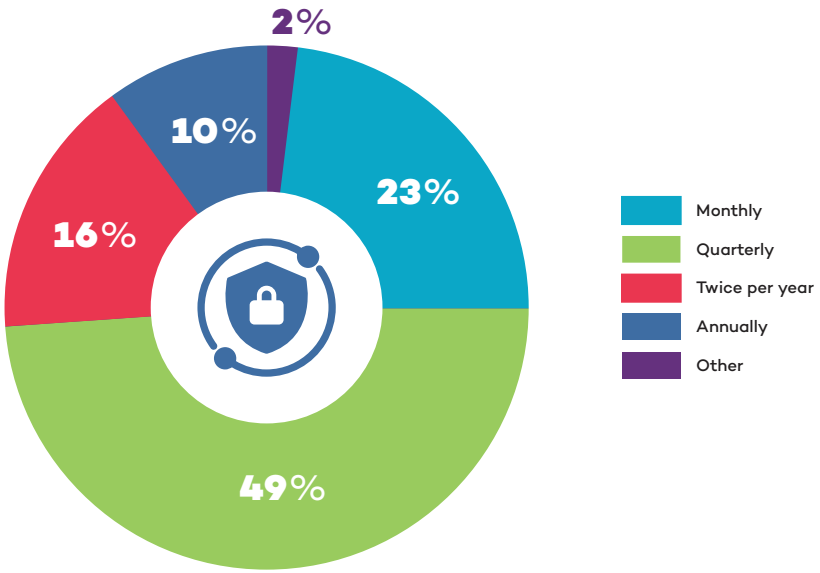
**Brian Cyphert, Chief Information Security Officer and Executive Director of Global IT Services at MSA Safety, told us how his company evaluates middleware applications and solutions for capturing data on older equipment. "We weave the review and assessment of the third-party application into the cyber program's risk management process. We look at the level of maturity in the vendor's security program, their different security controls, whether they have thought about security as part of the design of their application or if it was more of an afterthought for them. We have agreement among the groups internally that it must be security by design, and I think we have really good alignment there."**


Many manufacturers are applying this same rigor to their third-party vendors and service providers, such as system integrators, machine builders, and automation suppliers. The majority (54%) of companies we surveyed require third parties to undergo comprehensive assessment and management. The rest of the companies we surveyed say their assessments and management are partial (27%), limited (8%), or nonexistent (1%).

Methods of managing third-party vendor and service provider risk can take different forms. The prevailing approach is to require compliance with the manufacturer's own security policies. Other controls include regular security assessments of these vendors, data encryption, and monitoring for suspicious activities.

Given the scope of OT cybersecurity, from vetting new equipment to responding to breaches, fewer than one in 10 companies handle all aspects of OT security with in-house resources. The majority (66%) tap into a combination of internal and external security expertise, and 18% rely on third-party service providers for most of their OT security needs. Some manufacturers outsource security for OT specifically because their teams don't have the relevant skills or the bandwidth.

## Frequency of OT Cybersecurity Risk Audits and Assessments




Source: Manufacturers Alliance and Fortinet study

Third-party security providers are often the go-to vendor for responding to a breach. Companies are looking for outside expertise to cope with and recover from an attack. In 2020, one-third of companies handled breaches entirely with internal resources; in 2023, that share dropped to one-quarter.

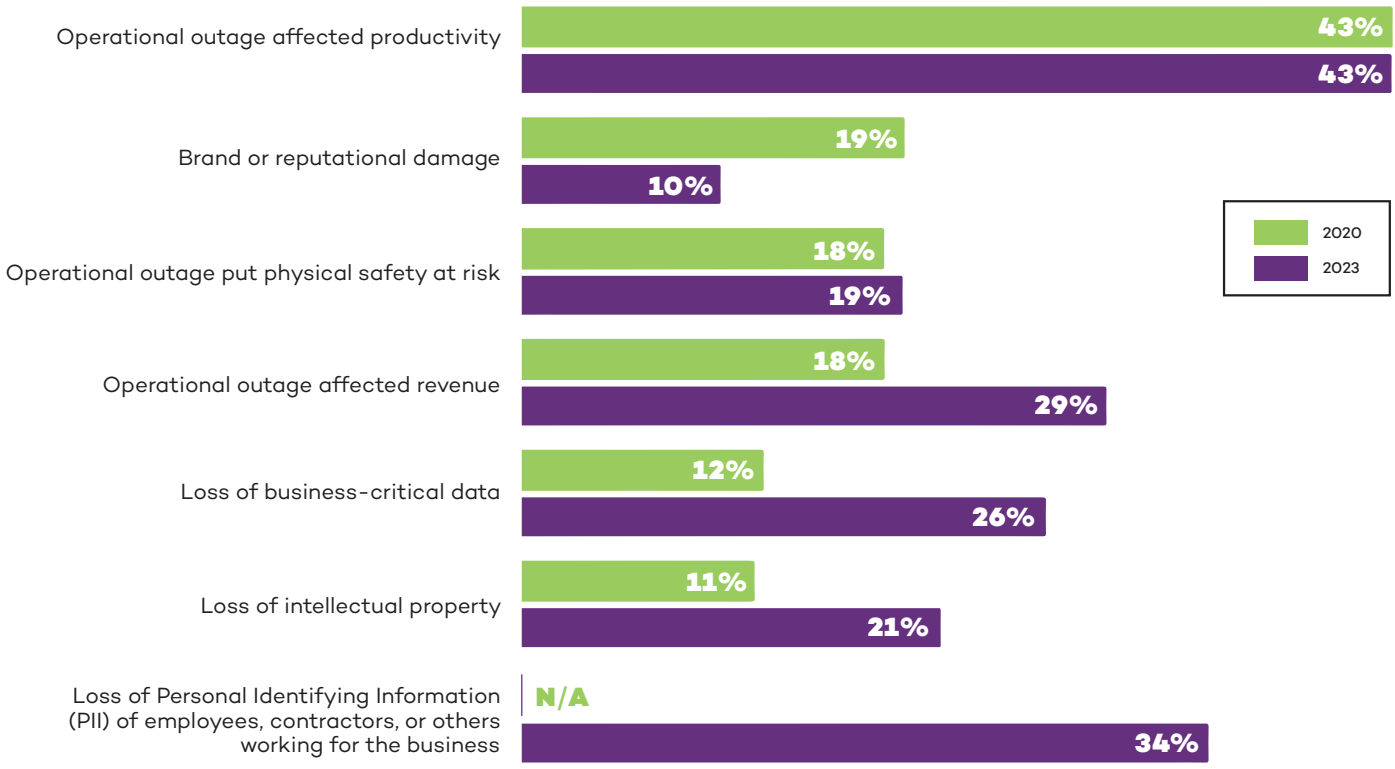
# Places Where Manufacturers Are Stalled or Losing Ground

Despite their progress over the past few years, manufacturers may not be moving fast enough to stay ahead of the threat to OT. Only 21% of companies reported being breach-free in our 2023 survey, a deterioration from the 26% in 2020. What's worse, there is evidence that businesses as a whole **underreport cyberattacks**. Breaches are becoming more frequent, sophisticated, and damaging. In 2023, more companies report seeing impacts on revenue, business critical data, and intellectual property than in 2020.

In many cases, vulnerabilities can be traced to lack of transparency about the assets in the OT environment. Legacy equipment spread out over multiple geographies makes building an inventory of assets a time-consuming task and a problem area for several manufacturers we spoke with. As one executive complained: "Plants tend to hoard equipment because they're under-capitalized. They don't want to give things up or they might need them for spare parts. So there are multiple layers of hoarding and that contributes to the challenges of OT." As another IT professional put it: "OT area has always been a black hole for my department."

## Impact of OT Security Breaches – 2020 Versus 2023

If your company experienced an OT breach, what impact did it have on the organization?




Source: Manufacturers Alliance and Fortinet study

Many manufacturers with legacy equipment in use mistakenly believe that air gaps will protect them from intrusions. Richard Springer, Director of Product Marketing, OT Solutions at Fortinet, underscored that this is a myth: "Air gaps were how security was done 30 years ago. Back then, there was nothing that could even be connected, and the internet wasn't robust enough for us to connect to it. But today most people have smartphones and flash drives. If they walk into a factory with USB ports open, that factory is connected."

In a plant where machines are old but still operational, there may be a "run it until it dies" mentality. Patching older machines is a known obstacle because of short maintenance windows and risks from patching. "In some cases, our devices are 20 or 25 years old, and the manufacturer no longer supports the product," a cybersecurity executive told us. In these cases, OT vulnerability management tools come into play. "Where there are vulnerabilities that you can't do anything about, these tools catch risks as they occur within the device. In other words, vulnerability management, but at the OT level. This way, you're aware of the vulnerabilities and they're documented," he continued.

**"I don't have an inventory. And we all know that security starts with an inventory. You can't secure it if you don't know about it, and you can't say you're secure if you've secured everything except for those two machines in the corner that never have been patched. Until I have an inventory, I'm just kind of shooting in the dark."**

*— Information Security Executive at a Specialty Manufacturing and Engineering Company*

Incrementally addressing legacy equipment is the only way to make progress for many companies. As Brian Cyphert explained, "We're a 109-year-old manufacturer with systems and devices that have been in place for 20 or 30-plus years. So we're taking a very methodical approach. The assessment is going to be the most time-consuming. Some of it may even be manual—somebody walking through the factory and saying, show me this piece of equipment and what it is connected to. That's why we're looking at pilot projects to locate quick wins and help us identify the processes that we can roll out globally."

## Getting Ready for New Regulations

New U.S. regulations for cybersecurity come online in late 2023 and 2024, affecting publicly traded companies and those classified as critical infrastructure. More than eight in 10 of the companies we surveyed said they feel well-prepared or very well-prepared to comply with relevant regulations and standards. With the Securities and Exchange Commission's new **Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure** rules for public companies coming into force in December 2023, manufacturers must provide more information to the public about processes and incidents. Disclosures must occur within 72 hours of determining the incident is material, unless an extension has been authorized by the U.S. attorney general.

# The Talent Crunch Is a Structural Barrier Blocking Progress

Cybersecurity is about having not only the right technology stack but also the right human capital. The skilled talent shortage is making it harder to fill open OT security positions, which cascades to team burnout and increases risk overall. When asked if they expect to have the right talent in place to address OT cybersecurity risks within the next three years, 22% of respondents said they are not confident, marking a slight deterioration since our 2020 survey (20%).

This pessimism about the availability of skilled talent also affects manufacturers when they need it most urgently—after an intrusion. When asked about barriers to effective breach response within the last year, 78% pointed to scarcity of talent and expertise. It's not surprising that knowledge of cybersecurity threats and vulnerabilities was cited as the number one skill sought by manufacturers.

Revenue plays a decisive role in perceptions of the availability of talent. Companies with revenues of $10 billion or higher are more likely to perceive OT security talent as "abundant," while companies with revenues of less than $1 billion are more likely to say it is "scarce." This suggests that companies with more resources are in a much better position to recruit, train, develop, and compensate the skilled talent needed to staff the OT security environment.

Just as revenue turns out to be a good predictor of whether you perceive talent to be abundant or scarce, so does your side of the org chart: IT and OT teams have opposite views again. When we asked IT professionals, 31% characterized availability of OT security talent as abundant, versus 16% of OT professionals.

Scarcity aside, the problem may not be confined to the question of which companies and departments can attract and retain this talent. As John Bartho, CIO at **Hyster-Yale** put it: "I wouldn't say finding talent has become harder. It's just as hard as it's always been. What I would say is that tasks requiring digital skills used to belong to the IT leader, but now digital is everybody's job, so the businesses want my people. They need data analysts, technology project managers, and people trained in specific domains. We're competing for more of these same skills across the entire business as the company tries to become more digital."

## Top 5 Skills for OT Security Professionals

1. KNOWLEDGE OF CYBERSECURITY THREATS AND VULNERABILITIES
2. KNOWLEDGE OF INDUSTRIAL CONTROL SYSTEMS (ICS)
3. PROFICIENCY IDENTIFYING ABNORMAL PATTERNS OF OT SYSTEMS
4. ABILITY TO ASSESS AND MANAGE RISK SPECIFIC TO OT
5. EXPERIENCE WITH NETWORK SECURITY ASSESSMENT AND REMEDIATION

## The College-to-Internship Pipeline

"We have a really strong intern program, so I want to build up relationships with the local colleges. I have a never-ending supply of candidates coming off of these intern programs and being in the Northeast, there is no shortage of colleges."

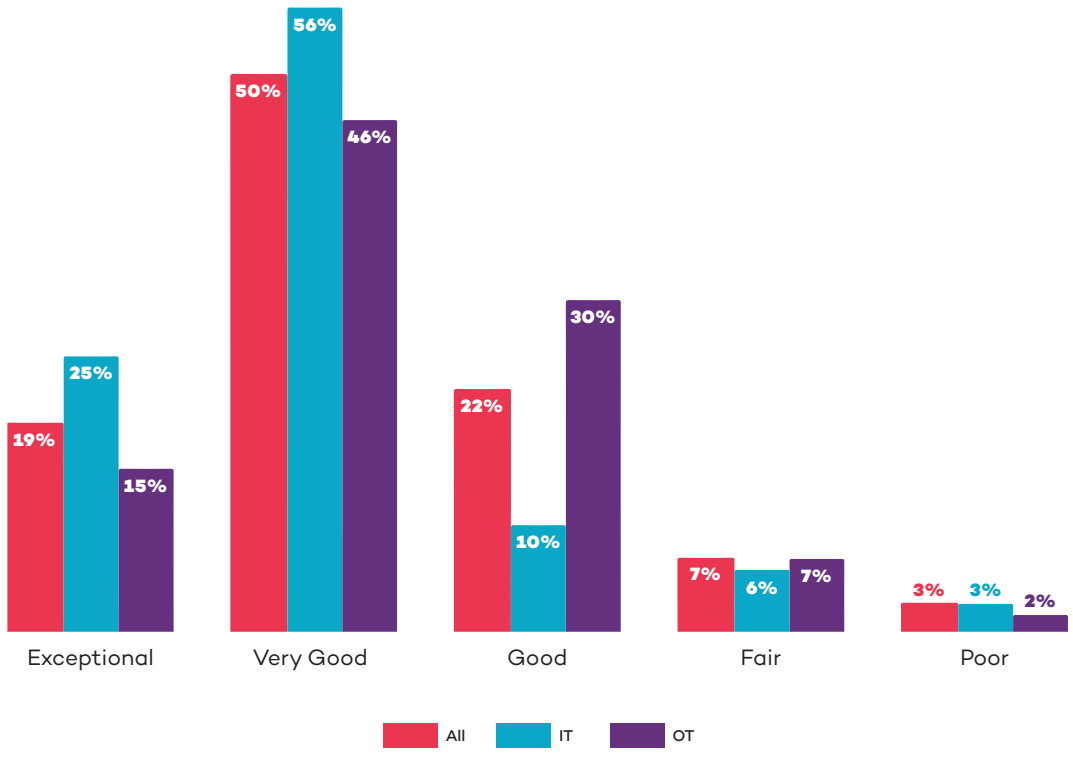
*– Doug Schaible, Manager, Information Security and Identity Access Management at* ***Victaulic***

# IT/OT Collaboration: A Shared Goal, but Progress Is Mixed

While the vast majority of companies we surveyed (84%) envision their companies' IT and OT teams working more closely together in the future, what is happening today may fall short of that. IT respondents were much more positive than their counterparts in OT about the quality of IT/OT collaboration.

Solid communication between IT and OT is a precondition for successful cybersecurity collaboration. But manufacturers are struggling with precisely this skill in the aftermath of a breach. Ineffective communication between IT and OT was ranked as a barrier to effective breach response by 82% of the companies we surveyed. Significantly, when we asked manufacturers to rank the skills needed for OT security professionals, strong communication and interpersonal skills ranked dead last. Finding talent with the right blend of skills for IT, OT, and communication is a tall order in this talent-constrained environment.

## How Manufacturers Rate Their Company's Collaboration Between IT and OT Functions as It Relates to OT Security




Source: Manufacturers Alliance and Fortinet study

In addition to the survey data, the long-standing cultural divide between IT and OT teams also surfaced repeatedly during our interviews. One professional described OT as "the Wild West," saying "my goal eventually is to have them reporting to my group in some way, shape, or form. But that's a down-the-road task." Most executives were looking for best practices about how to increase IT/OT collaboration and seeking insights into whether other manufacturers are using governance or reporting structures (direct line, dotted line, matrix) to align teams and policies.

Ken Brown talked about the evolution toward greater IT/OT collaboration at Milliken. "Many years ago, there was not a lot of communication between IT and OT. Corporate IT provided central shared services and OT was supported locally. But, IT and OT are interdependent. We all work for the same organization and share the same goal of keeping our critical systems up-and-running. To be successful, we had to open lines of communication and build trust."

Collaboration means understanding that "there has to be a balance between security priorities and operational priorities," Richard Springer stressed. "IT and OT should not have competing interests because their most important shared interest is what's important to the company. It's a matter of dual prioritization."

## Driving IT/OT Collaboration at Milliken

"We have a Cybersecurity Council, and a few years ago we added manufacturing leadership to that council. We also have a weekly cadence set up with key contacts at our locations to talk about cyber threats, best practices, and how we best protect our critical manufacturing systems. Once a year, we have an IT/OT workshop where we host our plant contacts at the corporate headquarters and spend the day discussing a variety of topics related to IT and OT. Our IT/OT collaboration is continuing to grow. But, it does not happen by accident. It takes deliberate, continuous effort to bring the IT and OT groups together."

***– Ken Brown, Director of Cybersecurity and Governance, Milliken & Company***

# Technology for Growth and Threats on the Horizon

Stronger IT/OT collaboration means better tools and processes to protect security as well as productivity and ultimately competitiveness. As manufacturers evaluate how to blend new technologies for competitive growth, they must build security into that overall scenario planning.

Travis Ward, Director of IT Security and Compliance at **ConMet**, a subsidiary of Amsted Industries, talked about a three-year time horizon for studying the threat landscape and factoring in an increase in sophistication of threat actors and technologies, as well as the growing OT attack surface. "We ask ourselves if we can be prepared for what we see and talk about how we need to respond from the people, process, and technology perspectives."

"We are investing in OT system modernization, not only for cybersecurity, but for digital transformation. Some of our goals around Industry 4.0 cannot be accomplished with the older technology. This modernization is providing opportunities to transform the business, increase our visibility, and improve our OT cybersecurity.," Ken Brown mentioned.

Manufacturers are building controls right into plans for future technology investments. Several executives talked about putting a cap on equipment life cycles whenever this is possible in the OT environment. "Life-cycling is an axiom. For new items in the IIoT space, you're probably looking at 10-year life cycles. Acquisition agents need to understand that they will have the device for 10 years and be required to touch it in some major way (such as a refit) within five," one executive said.

Whatever timeframe organizations adopt in the future, it is important that legacy equipment not be the elephant in the room now. As Ken Brown described it: "For older OT systems, our divisions put together replacement plans that are discussed at a Cybersecurity Council meeting.  Are we going to replace the potentially vulnerable system within two years, within five years, or will it be longer? Are we okay with accepting the risk in the meantime or do we need to move faster? After putting in mitigations, if we are willing to accept residual risk, we want to do so as a conscience business decision. We do not want to accept risk by default because no one is talking about it."

Cybersecurity risks are by no means an excuse to delay digitalization. Rather, they are a reminder that holistic approaches are required. As Richard Springer put it: "From a modernization and an Industry 4.0 perspective, you have this factory that has been operating for a long time. And sure, maybe it's pretty competitive as-is. But the tools are now available to process all of that factory's information and reap more production capabilities. And where you do that is by leveraging the data from the factory, sending it to the cloud, going to your AI models, and doing all of this with security built in. There's just so much potential."

# Best Practices Checklist

- Complete a basic asset inventory and segmentation, including hyper-segmentation on legacy machines.
- Use network access controls to manage new devices trying to connect with or communicate on your network.
- Continuously verify all users, applications, and devices seeking access to critical assets, regardless of where they reside.
- When acquiring new OT devices and middleware, make sure that security and resiliency are built into the design of the product, not built on as an afterthought.
- Follow the principle of least privilege. Only allow the traffic or the data flow that is needed to accomplish the task. Do that for every single scenario.
- Create a criticality roster that ties equipment to a criticality rating from an operations perspective. Address high-risk, high-value assets first.
- Look at best practices from other industries, especially those particularly advanced in cybersecurity, such as the defense industry and utilities.
- Incorporate respected cybersecurity maturity models, such as **CIS Critical Security Controls** and the **NIST Cybersecurity Framework**. Replace self-assessments with properly scoped assessments from third-party experts to establish a true baseline of your preparedness.

Manufacturers Alliance Foundation is the 501(c)(3) partner of Manufacturers Alliance®. The Alliance Foundation provides educational opportunities for the manufacturing community and its stakeholders through insights, events, and tools for today's most critical business decisions. The Alliance Foundation focuses on talent, technology, digital transformation, and competitiveness.

For more information, visit **ManufacturersAlliance.org/foundation**.

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future.

For more information, visit **fortinet.com**.