



Cybersecurity

Many are saying that, because of the presidential election in the U.S., these are “perilous” times. However, these are certainly perilous times in manufacturing and plant technology for an entirely different reason: leaky or nonexistent cybersecurity at a shockingly high number of facilities.

For example, one study, detailed in this eHandbook and [released in June by Fortinet](#), piled onto evidence from other studies this year that operational technology (OT) in factories of all sizes is extremely vulnerable to cyberattacks.

This obviously means that manufacturers need to double and triple their efforts to enhance their OT cyber defenses. This is a challenge considering that technology in plants can run the gamut – from “legacy” equipment that can be decades old and invisible to software monitoring for suspicious activity to the latest plant tech that is miles more advanced and more visible but also more connected to the outside world and thus more vulnerable.

Our sponsor Yubico emphasizes in this eHandbook some important defenses to staying secure from increasingly sophisticated attacks like phishing. Specifically, that modern cyber threats to factory technology necessitate modern practices like phishing-resistant authentication as a critical first step in mitigating risk, in securing a digital transformation and accelerating business effectiveness.

Yubico also recommends here the deployment of segmentation; establishing visibility and compensating controls for OT assets; integrating OT into security operations and incident response planning; and embracing OT-specific threat intelligence and security services.

This *Smart Industry* eBook also goes on to detail other top-line findings from Fortinet’s [2024 State of Operational Technology and Cybersecurity Report](#) and others that have illuminated the threat to OT this year.

For example, Copia Automation found in its [State of Industrial DevOps Report](#) that cybersecurity breaches are the most common cause of downtime; that 57% of studied manufacturers globally cannot track, control, and report on sensitive data sent and shared externally; and that 37% of organizations experienced seven or more data breaches in 2023. Separately, Kiteworks reported [similarly significant findings](#) about the inadequacy of factory cybersecurity.

Also this eBook notes that IBM’s [X-Force Threat Intelligence Report](#) found that manufacturing holds another dubious distinction as most-attacked by cybercriminals this year, for the third year in a row (that’s not a No. 1 anybody anywhere in business wants), so never has robust cybersecurity been more important on the plant floor than it is now.

In closing, this eBook also looks at a trend of abuse of artificial intelligence by cyberattackers and strategies to protect plant OT from the persistent threat of ransomware, which is a particular and expensive type of cyber intrusion and one of the most common today.

Scott Achelpohl, managing editor, Smart Industry

Sponsored by

yubico

Secure your digital transformation — stop account takeovers and prevent ransomware

Phishing-resistant users: The only way to remove phishing from your manufacturing environment and accelerate Zero Trust

As the cyber threat landscape evolves, hackers don't break in—they log in. Sophisticated phishing attacks target users, not devices, stealing credentials to infiltrate critical systems and compromising sensitive data. Safeguard your users with modern multi-factor authentication (MFA) that moves seamlessly with them, across devices, services and manufacturing business scenarios across IT and OT systems.

The YubiKey: Experience the most secure passkey authentication

Whether in an industrial environment or corporate office, the IP68-certified YubiKey—a hardware security key with multi-protocol support¹ offers the highest assurance AAL3, passkey authentication to secure user access. And the YubiHSM, the world's smallest hardware security module (HSM), protects servers, applications, and computing devices.

No matter where you are on your cybersecurity journey — we'll meet you there to secure the threats of today and tomorrow



LEARN MORE AT

yubi.co/manufacturing-visualindustrybrief

yubico



YubiKey 5 NFC

YubiHSM



Protects across cloud, on-prem and isolated environments



Works with leading IDPs, IAM, PAM solutions & 1000+ applications



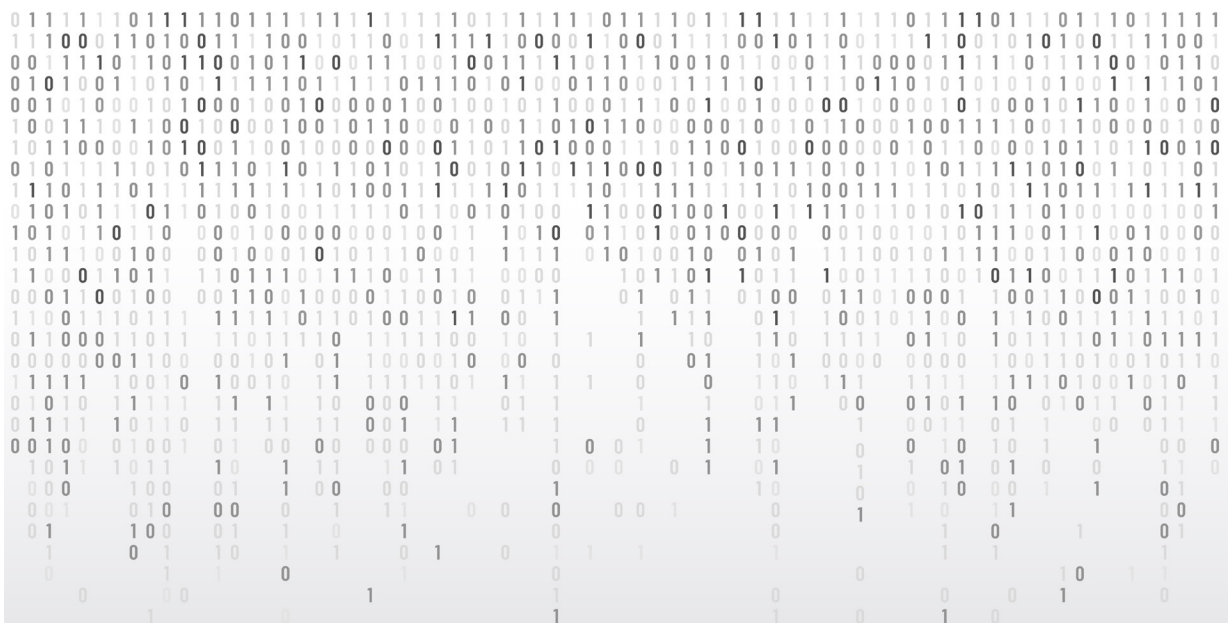
Proven to deliver 203% ROI²

¹ Supports a broad range of authentication protocols: FIDO U2F, WebAuthn/FIDO2 (passkeys), OTP/TOTP, OpenPGP and Smart card/PIV, and enables you to bridge to passwordless.

² Forrester Consulting Total Economic Impact (™) study, September 2022, metrics based on a composite organization

CONTENTS

Phishing, Ransomware, and OT, oh my?	4
How to choose security for your OT operations	7
Pair of new reports see glaring data, cybersecurity, content-sharing vulnerabilities	9
Cybersecurity report shows threats to OT skyrocketing	11
Manufacturing leads in cyberattacks for a third straight year, so what are some defenses?	13
Securing OT's future: Strategies to adapt in an evolving environment	14
AI abuse by cyberattackers is a people – not technology – problem	16
Protecting OT data under persistent threat from ransomware	18
Navigating red-alert security challenges in manufacturing	21



Phishing, Ransomware, and OT, oh my? Key insights and best practices for manufacturers to secure user access for IT and OT systems

By Josh Cigna, Enterprise Solutions Architect, Yubico

Manufacturers made up more than 25% of cybersecurity incidents in 2023, with malware attacks (primarily ransomware) making up most of them, ranking for the third straight year as the most-attacked industry.¹ Globally, critical infrastructure, including the manufacturing sector, continues to be targeted by cyberattacks with malicious actors trying to cause mass disruption to public life and safety.

EXPANDING RISK LANDSCAPE

Even a single compromised password can cause mass disruption, as evident in recent cyberattacks. Staggeringly, there has been a 71% year-over-year increase in cyberattacks that used stolen or compromised credentials².

As we move further into the era of Industry 4.0, smart manufacturing naturally increases the risk landscape because IT systems are becoming more intertwined with OT systems. Despite their interconnectivity

and convergence, OT systems are often overlooked, creating weaknesses that are causing manufacturers to be impacted by attacks. And further, now with AI-driven phishing attacks entering the fray, and other existing social engineering attacks, it is getting harder to discern genuine communication from malicious ones. Identities are truly being targeted at an alarming rate.

LEGACY MFA IS BROKEN

So, if we know that threats are evolving in sophistication, shouldn't we evolve the protection mechanisms we use to secure these critical systems and data?

Legacy methods of authentication are simply no longer enough to ensure a secure operating environment. These methods often do not support modern security controls applicable to a diversity of industries, and conditions such as restrictive production floor environments make it challenging to standardize, and create conditions where manufacturers

have to rely on local and traditional on-prem access instead. Now, when systems in the cloud are introduced into the equation, including their own unique complexities, third-party remote connections to control OT devices connected to an internal network become extremely difficult to manage. Additionally, the introduction of network connectivity demands a shift in mindset from risk awareness and risk tolerance to one of proactivity. In 84% of known critical infrastructure cyber incidents, the initial access vector could have been mitigated,³ so the power is truly in your hands.

But how do you weigh the risk of what is technically feasible, while also paving the way to a stronger cybersecurity infrastructure for your manufacturing organization and your supply chain?

HIGH ASSURANCE AUTHENTICATION FOUNDATIONAL TO ZERO TRUST

This is pivotal for the business continuity and cyber resiliency

¹Smart Industry, Manufacturing leads in cyberattacks for a third straight year, so what are some defenses, 2024

²IBM Security, X-Force Threat Intelligence Index 2024

³IBM Security, X-Force Threat Intelligence Index 2024

of your resources. Ultimately, the type of authentication plays a big role. A foundational aspect of a Zero-Trust approach involves multifactor authentication (MFA), which mandates two or more different methods to verify the user during the authentication process. The core parts of MFA include something you know (PIN, password), something you have (cryptographic identification device, token), or something you are (biometric).

While any form of MFA is better than password verification alone, it has become clear that older forms of basic MFA, such as SMS or mobile authentication apps, are proving easy to bypass by malicious actors. Not only is the strength of an MFA method important, you also need to consider an approach that works well across both complex legacy infrastructure and modern cloud environments, and in restrictive and rugged work spaces such as production floors, remote and industrial environments, and areas where mobile phones simply aren't even allowed. Ultimately, the modern MFA approach needs to be able to secure both IT and OT systems effectively, without making it hard or time-consuming for users. Importantly, it also should enable employees to move freely regardless of how they work.

CREATING PHISHING-RESISTANT USERS

Manufacturers need to prioritize securing their users as cyber threats target users. Therefore, the tech that you empower your users with should provide them with phishing-resistance regardless of how they work. The National Institute of Standards and Technology (NIST) Special Publication 800-63B-4 defines phishing-resistance as “the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber.” Only two forms of authentication currently meet the mark for phishing-resistant MFA: solutions based on PIV/smart card or modern FIDO2/passkey authentication standards.

To build on phishing-resistance, passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are two different passkey implementations:

- Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. Potentially suitable for lower security assurance scenarios since

ownership is being delegated to a cloud provider/third party.

- Device-bound passkeys, on the other hand, offer enterprises greater control of their FIDO credentials compared to synced passkeys since ownership resides with the hardware. It should be noted that there are even different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Providing phishing-resistant authentication that moves with the users.

GLOBAL LANDSCAPE

We are seeing regulations and standards increasingly push for stronger means of authentication to secure access and digital identities. As part of the Enduring Security Framework (ESF) for critical infrastructure, the [Identity and Access Management: Recommended Best Practices for Administrators](#) presents a distillation of IAM and cybersecurity guidance based on NIST standards recommending phishing-resistant MFA.

THE POWER OF CHOICE

The future for online security is passwordless, and beginning the journey should be a key part of your digital transformation. Even

in the OT space, where legacy systems may weigh down plans and rollouts, planning for the future sooner rather than later is an important process to go through. In reflecting on your own organization and supply chain, here are four best practices you should consider in strengthening your authentication defenses:

1. Weigh the risk:

Define what is feasible to mitigate risk by following cybersecurity frameworks and best practices like NIST and utilizing the technologies they classify as phishing-resistant where possible.

2. Protect high risk users:

As with most attacks, after malicious actors steal a compromised credential, they move laterally, and then expand vertically to cause more harm and look for the most valuable data. You

need to be protective of your crown jewels and high value targets. So, start there, by protecting them with phishing-resistant authentication creating phishing-resistant users, then expand to the rest of the organization.

3. Risk preparedness


An attack on one of us is an attack on all of us, since we live in an interconnected society, so being strategic is critical. Think about who has third-party access and what your chain of communication and access points looks like. Ultimately, the goal should be to secure user access across the entire spectrum with phishing-resistant authentication to protect business continuity and be cyber resilient.

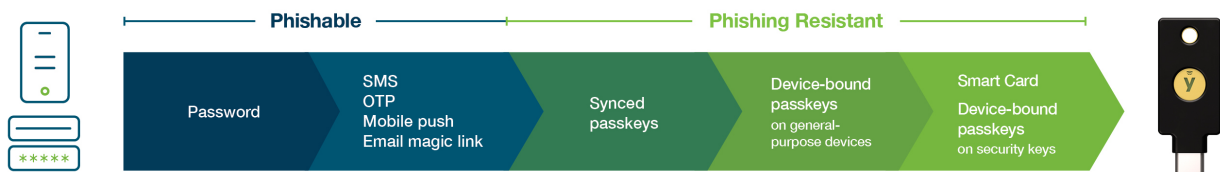
4. Risk acceptance

Ultimately, given the diverse infrastructure of your

manufacturing environments, there may be scenarios in which you might not be able to modernize fully with phishing-resistant and passwordless technologies yet. In this case, it is important to work closely with your cyber insurance provider to understand what you're willing to risk.

LAST REMARKS

When evaluating the methods to secure user access and critical systems, consider what would help your business maintain availability and reliability. Modern cyber threats necessitate modern cybersecurity practices. To effectively protect your organization, consider modern phishing-resistant authentication as a critical first step in mitigating risk, in securing digital transformation and accelerating your business. 



Comparative assurance and usability levels of different MFA technologies.

How to choose security for your OT operations

An effective OT security regimen must be able to secure the entire environment at a plant—the “legacy” machinery as well as the latest devices.

By [Ilan Barda](#)

■ In a recent survey conducted by ABI Research, three-quarters of industrial organizations reported that they had detected malicious activity within their OT network, and 24% of them were forced to shut down OT operations within the last year due to a successful attack.

If that’s not enough to have OT companies looking for new cybersecurity solutions, European Union companies have the added pressure of NIS2’s looming October deadline. Essential and important entities are on the hunt for cybersecurity solutions that will meet their security needs while boosting their compliance.

See also: [Cybersecurity report shows threats to OT skyrocketing](#)

OT security is complicated. Manufacturing plants and critical infrastructure facilities frequently maintain equipment that is so old it hasn’t been made in decades, working alongside modern connected machinery. An effective OT security regimen must be able to secure the entire environment—the “legacy” gear as well as the latest devices.

The good news is a lot of OT cybersecurity solutions on the market deliver parts of the security solution manufacturers need. Then again, part of a solution is not the whole solution. And not all OT security tools purported to be solutions are created equal.

For example, some products deliver network visibility but lack threat-detection capabilities, while others are strong in threat detection but unwieldy and difficult to manage. In this article, we’ll look at the capabilities your OT cybersecurity platform should have to put you on the path to NIS2 compliance.

START WITH FULL NETWORK VISIBILITY

OT cybersecurity begins with network visibility. After all, you can’t secure network connections, zones, and devices that you aren’t aware of. Your OT security solution should include non-intrusive monitoring capabilities that allow it to automatically create a visual model of your devices, protocols, and links. Active scanning, where acceptable, is a great supplement.

Your monitoring tool should automatically establish a baseline of normal behaviors. Anomalous behaviors should be detected as potential indicators of compromise (IOC).

For example, if one machine transmits a message to the network at 20-minute intervals, and the message is now being sent every 60 minutes, there is cause for investigation. The monitoring tool should keep up with the latest threat intelligence, so it can identify new publicly known vulnerabilities (CVEs) and recommend patches and workarounds to secure those issues.

See also: [Pair of new reports see glaring data, cybersecurity, content-sharing vulnerabilities](#)

Monitoring should feed into your alert management system or have one of its own. The most effective OT monitoring tool will not only send alerts on IOCs and potential cyberattacks, but will let you know about business policy violations, abnormal topology changes, new device connections, and other changes to the network. Each alert should be prioritized automatically based on perceived severity.

Look for a solution that offers active scanning in addition to passive scanning. Active scanners are useful in discovering additional assets and data collection from components that are silent on the network. They also can help detect vulnerabilities in firmware and other components.

These capabilities help boost operational resilience against cybersecurity risks and threats, helping to bolster operational security posture and compliance with directives, security requirements and frameworks, and industry best practices.

ADD IN OT RISK MANAGEMENT

Monitoring your OT network is a major function of a healthy OT security program. Another is risk management. Risk management tools help you proactively manage risk and build resilient operations. Look for a data-driven solution that conducts automated risk assessments through breach simulations to detect vulnerabilities in your network and to advise you on what to do about them.

This tool should help you measure the gaps between your existing security controls and compliance with NIS and/or other standards. Running frequent assessments makes it easy for security teams to stay on top of risk while measuring their progress over time.

See also: [Securing OT's future: Strategies to adapt in an evolving environment](#)

Look for a risk management tool that not only offers recommendations for securing vulnerabilities but takes budget into account. It's easy for a simulator to find a vulnerability and give a laundry list of network change recommendations. However, leading tools include budget information for each change, and quantifies the reduction in risk for full and partial fixes.

For example, if a simulation detects vulnerabilities that lower a manufacturing site's risk score to 43, it should also include multiple mitigation options to drop it even further. Replacing machinery, which might cost millions of dollars, could improve a risk score a lot, but installing a free patch would improve the risk score most of the way. Each option should include associated costs, allowing stakeholders to make budget-based risk assessments.

MULTISITE MANAGEMENT WITH CENTRAL MONITORING

Organizations that operate multiple sites should look for solutions that include central monitoring and management for the entire OT estate. The convenience of these platforms is invaluable, providing visibility into OT networks regardless of their location.

Centralized platforms are cost-effective. Rather than having multiple security teams monitoring

the network at each site, a single security team at an SOC can oversee and manage the entire security regime. Alerts generated at any of the sites come to the central management location, where they can be investigated and remediated.

Centralized platforms also improve security effectiveness. Organizations can implement policies across their sites from a central point, ensuring consistency.

FINDING A SUITABLE OT VENDOR

OT security is critical for the continued operations of manufacturing plants, critical infrastructure, and other OT environments. To be effective, organizations should look for solutions that provide full visibility into their network and applies data-driven risk management tools automatically. Organizations with multiple sites should require solution that provide central security monitoring and management.

See also: [In reader survey, wide majority worries about OT vulnerabilities](#)

While some organizations might prefer mixing and matching solutions from different vendors, this best-of-breed approach often leads to security gaps and complications in interoperability. A security platform from a single vendor—as long as it meets all requirements—is typically the best approach. ■

Pair of new reports see glaring data, cybersecurity, content-sharing vulnerabilities

Surveys from Copia Automation and Kiteworks of manufacturing stakeholders join others, from Fortinet in June and Ponemon/Cyolo in February, that point to large, exploitable holes in plant software, strategies, practices, and programming.

By [Scott Achelpohl](#)

Two new reports, [one by Copia Automation](#) that found millions of dollars in losses per hour from cyber breaches and coding problems, and [another by Kiteworks](#), which revealed most industrial organizations can't track and control sensitive content shared externally, show that manufacturers continue to have glaring data, security, and content-sharing vulnerabilities that are ripe for exploitation by bad actors and cost them a lot in lost revenue.

Released July 9 as part of its first State of Industrial DevOps Report, the Copia survey of 200 U.S. executives reveals half of all plant downtime is caused by programming mistakes and shows the shutdowns due to coding errors last 30 hours on average, costing \$4.2 million per hour and \$126 million per shutdown.

Half of all downtime is caused by industrial code changes, code confusion, lack of visibility into industrial code, and issues with programmable

logic controllers, according to the new Copia report.

See also: [Securing OT's future: Strategies to adapt in an evolving environment](#)

In its own 2024 Sensitive Content Communications Privacy and Compliance Report, released July 2, Kiteworks, which surveyed 572 IT, security, risk management, and compliance leaders, found:

- 57% of organizations globally cannot track, control, and report on sensitive data sent and shared externally.
- 32% of organizations experienced seven or more data breaches last year.
- 34% of respondents generate audit log reports more than eight times per month to meet compliance requirements.
- 66% of organizations exchange sensitive content with 1,000 or more third parties, posing significant risks.
- 27% of North American organizations reported litigation costs exceeding \$5 million due to data breaches.

COPIA: CYBER BREACHES THE NO. 1 CAUSE OF DOWNTIME

The most common cause of unplanned plant downtime? Cybersecurity breaches, reported 47% of respondents to Copia Automation's survey, followed by hardware malfunctions (45%), coding and software issues (41%), human errors (32%), and environmental disasters (25%).

"The cost of downtime minimizes or eliminates the margin between profitability and failure for manufacturers," said Copia's co-founder and CEO, Adam Gluck. "With coding errors and cybersecurity breaches shown as significant causes for downtime, manufacturers need to take every technological measure to protect their bottom line and ensure continuous operations with enhanced productivity."

In other findings from the Copia survey, respondents reported they spend an average of 10 times longer (45 hours per month) debugging code than reviewing it, with this figure

rising to 20 times (77 hours per month) in the retail and material handling sectors of industry.

The average percentage of downtime due to code changes is higher for those with more industrial sites (65% for 76-99 sites) compared to those with fewer sites (31% for 11-25 sites).

The Copia survey contains responses from 200 executives, including C-Suite (42%), SVPs/VPs/heads of departments/directors (38%), and managers (20%). Respondents primarily came from the high-tech, electronics, and semiconductor (21%), retail (19%), and automotive (18%) industries.

See also: [Industrial OT widely vulnerable to intrusion, survey finds](#)

The Copia survey, [joining one in June from Fortinet](#), also highlights significant vulnerabilities in operational technology, the software and hardware that control industrial equipment. A possible cause for these is ad-hoc fixes in industrial programming, with 79% of respondents saying they are commonplace, according to Copia Automation, which is in the business of creating

solutions that allow companies to manage their OT.


While these quick fixes can temporarily restore operations, they often leave organizations susceptible to breaches because the changes aren't tracked. This makes it difficult or impossible to reliably maintain security updates. Considering the thousands of devices managed by manufacturers, the cascading effect of unmonitored changes can be substantial.

KITEWORKS: TOO MANY CONTENT COMMS TOOLS, IP LEAKAGE RED ALERT

The Kiteworks report cites widespread findings in the areas of the proliferation of communications tools, data breaches, third-party risk management, sensitive content security, compliance, and data classification and risk assessment, including:

- Nearly one-third of organizations rely on six or more content communication tools, escalating risks and operational inefficiencies.
- Preventing leaks of intellectual property is a top priority for

56% of respondents. The legal sector (75%) and the oil and gas sector (67%) express heightened concerns over IP leakage.

- Respondents reported high cyber breach frequency, with 32% experiencing seven or more data breaches last year, with legal fees often exceeding \$5 million.
- The U.S. government and security and defense sectors reported the highest incidence of breaches, but the Asia-Pacific region had the highest percentage of organizations reporting seven or more breaches (43%).
- Tracking challenges are widespread, with 39% of organizations globally reporting to Kiteworks that they can't track and control access to sensitive content once it leaves their domain, with local governments and pharmaceutical companies facing the greatest challenges.
- Only 11% of organizations believe no improvement is needed in sensitive content security, down from 26% in 2023. Large organizations and professional services firms indicate a significant need for improvement. 

Cybersecurity report shows threats to OT skyrocketing

Newly released survey from Fortinet says that nearly one-third of OT organizations reported more than six intrusions over the last year, up from 11% in 2023.

By [Scott Achelpohl](#)

Organizations with remote sites come in many forms, including distribution centers, warehouses, and factories. As companies embrace digital transformation, these often-massive remote sites rely on always-on application connectivity for seamless communication, collaboration, operations, and productivity.

A release this week from networking and security provider Fortinet adds to the evidence from other reports this year that all show the threat to manufacturing OT from cyberattacks is rising sharply.

According to the 2024 State of Operational Technology and Cybersecurity Report by Fortinet, 49% of respondents in 2023 experienced an intrusion that impacted either their OT systems only or both their IT and OT systems, but this year nearly three-fourths (73%) of these organizations have been impacted. The survey data also shows a sizable year-over-year increase in intrusions that only affected OT systems (from 17% to 24%).

See also: [Navigating red-alert security challenges in manufacturing](#)

Also, nearly one-third (31%) of respondents reported more than six intrusions in the last year, compared to only 11% in 2023. All intrusion types increased compared to the previous year, except for a decline in malware, according to a [release from Fortinet](#).

Phishing and compromised business email intrusions were the most common, while the most common techniques used were mobile security breaches and web compromise, according to the global Fortinet survey of more than 550 OT professionals, conducted by a third-party research company.

Given the rise in attacks, nearly half (46%) of respondents in the report indicate that they measure success based on the recovery time needed to resume normal operations.

The report “shows that while OT organizations are making progress in strengthening their security posture, teams still face significant challenges in securing converged IT/OT environments,”

said John Maddison, Fortinet’s chief marketing officer.

“Adopting essential tools and capabilities to enhance visibility and protections across the entire network will be vital for these organizations when it comes to reducing the mean time to detection and response and ultimately reduce the overall risk of these environments.”

DETECTION METHODS NOT KEEPING UP WITH THE THREATS

Though intrusions are surging, the report suggests that most organizations still have blindspots in their OT and IT environments. Respondents claiming that their organizations had complete visibility of OT systems within their central security operations, for example, have dipped since last year, dropping from 10% to 5% in 2024.

However, those reporting 75% visibility increased, which suggests that organizations are gaining a more realistic understanding of their security posture, according to Fortinet. Yet over half (56%) of respondents experienced

ransomware or wiper intrusions—an increase from 32% last year—indicating there's still room for improvement regarding network visibility and detection.

See also: [Industrial OT widely vulnerable to intrusion, survey finds](#)

Responsibility for OT cybersecurity is elevating within executive leadership ranks at some organizations, according to the Fortinet State of Operational Technology and Cybersecurity Report.

The percentage of organizations that are aligning OT security with the CISO continues to grow, increasing from 17% in 2023 to 27% this year. At the same time, there was an increase to move OT responsibility to other C-suite roles, including the CIO, CTO and COO, to upwards of 60% in the next 12 months, clearly showing concern for OT security and risk in 2024 and beyond, Fortinet added.

The findings also show that some organizations, where the CIO is not outright responsible, there is an upward shift of these responsibilities from the director of network engineering to the VP of operations role, which illustrates another escalation of responsibility.

This elevation into the executive ranks and below, regardless of the title of the individual overseeing OT security, may suggest that OT security is becoming a

higher-profile topic at the board level, according to Fortinet.

REPORT LAYS OUT CLEAR BEST PRACTICES FOR PROTECTING OT

The Fortinet report offers organizations actionable steps for improving their security posture. Manufacturers can address OT security challenges by adopting the following best practices:

- **Deploy segmentation.** Reducing intrusions requires a hardened OT environment with strong network policy controls at all points of access. This kind of OT architecture starts with creating network zones or segments.
- **Establish visibility and compensating controls for OT assets.** Organizations must be able to see and understand everything that's on the OT network. Once visibility is established, organizations must protect any devices that appear to be vulnerable, which requires protective compensating controls that are purpose-built for sensitive OT devices.
- **Integrate OT into security operations and incident response planning.** Organizations should be maturing towards IT-OT SecOps. To achieve this, teams must specifically consider OT with regard to SecOps and incident response plans.

- **Embrace OT-specific threat intelligence and security services.** OT security depends on timely awareness and precise analytical insights about imminent risks. Organizations should make sure their threat intelligence and content sources include robust, OT-specific information in their feeds and services.

Survey respondents were from Australia, New Zealand, Argentina, Brazil, Canada, mainland China, France, Germany, Hong Kong, India, Japan, Mexico, Norway, South Africa, South Korea, Spain, Taiwan, Thailand, United Kingdom, and the United States, among others.

See also: [Manufacturing leads in cyberattacks for a third straight year, so what are some defenses?](#)

Respondents represented a range of industries that are heavy users of OT, including: manufacturing, transportation/logistics, health care/pharma, oil, gas, and refining, energy/utilities, chemical/petrochemical, and water/wastewater.

Most of those surveyed, regardless of title, are involved in cybersecurity purchasing decisions. Many are responsible for OT at their organizations and/or have reporting responsibility for manufacturing or plant operations. ▣

Manufacturing leads in cyberattacks for a third straight year, so what are some defenses?

An overwhelming majority of intrusions could have been mitigated with patching, multifactor authentication or least-privilege principles, an IBM study has found.

By [Scott Achelpohl](#)

Manufacturing facilities are an important part of the U.S. economy, and they produce some of our most iconic brands. But an increasing amount of cybercrime is introducing more risk to the industrial sector, according to new research that IBM's [Michelle Alvarez](#) wrote about this week for *Smart Industry's* sister brand, [IndustryWeek](#).

See also: [Maximum security? How multifactor authentication is being defeated](#)

For the third year in a row, the [IBM X-Force Threat Intelligence](#)

[Report](#) ranked manufacturing as the most-attacked industry by cybercriminals. The sector's low tolerance for downtime has historically made it an attractive target for cybercriminals seeking to apply pressure for financial gains. Alvarez is on the [Strategic Threat Analysis team](#) at IBM that produced the report.

See also: [Protecting OT data under persistent threat from ransomware](#)

The IBM intelligence report found that last year, manufacturers

made up more than 25% of security incidents, with malware attacks—primarily ransomware—making up most of them. In the constantly shifting threat landscape, this trend calls for security fundamentals to remain an essential component of manufacturers' security strategy.

Fundamentals such as patching, multifactor authentication or least privilege principles can deter 85% of incidents, the report found.

See Alvarez's [full write-up on the IBM report](#) over at *IndustryWeek*. ■

Securing OT's future: Strategies to adapt in an evolving environment

These devices run very slim operating systems that often cannot accommodate onboard security measures. Moreover, many manufacturers have neglected security best practices.

By [Almog Apirion](#)

□ A [recent OT security report](#) revealed a concerning statistic: only 55% of industrial organizations are effectively mitigating risks and security threats. This lack of preparedness likely stems from the predominant historical approach to OT security—isolating systems to ensure their protection.

However, this isolation is no longer the norm for the industrial landscape. Increased connectivity is essential for modern industrial operations, although connectivity also introduces new challenges, particularly in controlling access and reducing risk from cyber incursion.

See also: [In reader survey, wide majority worries about OT vulnerabilities](#)

One of the most overlooked hurdles in implementing operational technology security solutions is the “cost of change.” Traditional security solutions often require significant infrastructure modifications, which can disrupt critical operations, lead to higher costs, and even jeopardize safety.

To optimize costs, worker safety, and efficiency during the implementation of new security strategies, organizations, like power plant operator [Rapac Energy](#), are looking for modernized access solutions that will enable them to keep cost of change as low as possible.

See also: [Fix your operations first, then technology can shine](#)

Rapac Energy exemplifies the challenges of modern industrial organizations. They needed to securely connect external suppliers, support teams, and customers to their OT and supervisory control and data acquisition (SCADA) systems.

However, their network remained isolated from the public internet for security and regulatory reasons. This disconnect generated significant cost and time-consuming processes while collaborating with essential partners such as service teams located across Europe.

The traditional approach of implementing a new security

solution meant potentially disrupting their entire network and requiring extensive overhaul of their mission-critical legacy systems—a risk Rapac wasn't willing to take. This is where the integration of adaptable and flexible security solutions becomes crucial.

MODERN STRATEGIES FOR ONGOING CHALLENGES

Modern secure remote access (SRA) solutions address these concerns. Designed to enhance the security of OT environments with zero change management required, these solutions provide secure access for internal and external users, in hybrid, on-premises and remote environments—online or offline—without requiring infrastructure changes. This minimizes disruption to operations, reduces costs and ensures continued safety.

See also: [How one manufacturer made all its digitized data easily searchable. Hint: It was AI](#)

With modern SRA solutions in place, enterprises like Rapac

are empowered with flexibility and adaptability amid evolving OT cyber threats and gain advanced capabilities including:

- **Secure access for third parties:** Controlled access for all external users, such as Siemens support teams and Rapac customers, without compromising the security of the network.
- **Enforcing identity-based access to both legacy and modern systems:** Continued support for both legacy and modern OT systems, eliminating the need for costly system upgrades.
- **Continuous authentication and authorization:** Ongoing authentication and authorization for all users,


ensuring only authorized individuals have access to specific systems and applications at any given time.

THE FUTURE OF OT SECURITY

The cost of change is a significant barrier for organizations looking to improve OT security. By adopting a solution that empowers scalability, without additional cost complexities, industrial organizations like Rapac Energy can achieve their security goals without compromising operational efficiency or safety.

Podcast: [Cybersecurity action steps and the dilemma of guarding private data](#)

Through the integration of modern SRA solutions, Rapac saved hundreds of thousands of dollars by avoiding unnecessary infrastructure changes and employee travel costs and improved their overall security posture while delivering a positive user experience.

In today's connected world, prioritizing OT security is no longer a choice—it's a necessity. However, enterprises don't need to fully overhaul their critical systems to enhance their security. With modern, adaptable solutions on the market, they have the option to strategically integrate key security solutions—ultimately creating a safer future for industrial environments. 

AI abuse by cyberattackers is a people—not technology—problem

Like any breakthrough, AI can be twisted for illegitimate purposes, but manufacturing IT and OT people can also turn the technology against cyber intruders. Here's how.

By [Ed Watal](#)

AI is here to change the world, whether we like it or not. While many have praised the breakthrough technology as the “revolution of work,” thanks to its potential to streamline operations and improve efficiency and productivity, others have expressed concern over the amount of influence AI already has exerted on our society. Ultimately, whether the AI revolution turns out to be a net positive or negative depends on who is using it—and for what purpose.

Although critics are correct in pointing out that artificial intelligence poses certain threats, we must recognize that these threats are not inherent to the technology but rather from people who abuse it. AI is just like any other innovation in history—if a way for people to exploit it for their own nefarious purposes can be found, rest assured that it will be.

See also: [Protecting OT data under persistent threat from ransomware](#)

Nevertheless, we cannot let this caveat prevent us from using AI in legitimate, beneficial ways. Instead,

we must mitigate and identify these harmful uses of the technology to create a landscape where AI technology can be used responsibly.

HOW GENERATIVE AI IS BEING ABUSED FOR THE BENEFIT OF SCAMMERS

Many of the most popular uses of AI today fall into the category of generative AI, or gen-AI. People have used gen-AI models, like ChatGPT, for uses that can improve their productivity and efficiency, from drafting emails to powering customer service chatbots or, in manufacturing operations, to make easier-to-understand technical manuals or anticipate equipment downtime. Unfortunately, the highly customizable nature of these models has allowed wrongdoers to find ways to intrude.

One of the most dangerous abuses of generative AI technology has been by scammers who have used it to improve their phishing schemes, which are designed to convince victims to reveal their personal information by

impersonating a trusted source—be it a boss, co-worker, friend, or loved one. In the past, it has been easier to spot this kind of scam because of simple, easy-to-spot mistakes such as grammatical errors or inconsistencies in voice.

See also: [Your competitors are using AI. Why risk falling behind them?](#)

However, today's scammers can train a model on a library of writing by the person they hope to imitate and create a convincing impersonation of them. The result is a message that is far more difficult to determine whether it was written by the person it claims to be or if it is a scam.

But it's not only written content that gen-AI has become dangerously and frighteningly good at creating. “Deepfakes”—images, video, and audio generated by AI—have become a viral threat. Scammers can use deepfakes for any number of nefarious purposes, ranging from blackmail and reputational damage to something as broadly impactful as manipulation of elections and stock markets.

HOW HACKERS ARE EXPLOITING AI TO AUTOMATE CYBERATTACKS

The other aspect of artificial intelligence that has been touted is its advanced data analytics capabilities. In several industries, AI has significantly improved efficiency and accuracy due to its ability to process extensive data sets far more quickly than a human, but this benefit could turn into something extremely dangerous should it fall into the wrong hands.

Podcast: [Generative AI on the plant floor](#)

Hackers have leveraged AI's data analysis prowess by training models to constantly probe networks for vulnerabilities. In doing so, they can increase not only the volume of their attacks but also their severity by making them much more difficult to identify and respond to.

However, these automated attacks become even more troubling when they target critical infrastructure and supply chains. Because so many industries and

institutions in our society now operate with or depend upon computers, hackers have several high-value targets to exploit.

Should a hacker find out how to exploit key vulnerabilities in networks running traffic lights, shipping routes, air traffic control, power grids, telecommunications systems, or financial institutions, the damage in money and loss of life could be tremendous.

HOW WE CAN STOP THESE ABUSES OF AI TECHNOLOGY

The silver lining here is that network operators can take a “fight-fire-with-fire” approach by applying the same tools that have been used against them to beef up their cybersecurity.

For example, the models that hackers use to probe networks for vulnerabilities can be used by network operators to identify weaknesses that need to be patched. In the case of fighting scams, AI models are being introduced that analyze writing and audiovisual materials to

determine whether they are authentic or AI-generated.

See also: [With AI, the time is now, say manufacturing technologists, futurist, ‘evangelist’](#)

Still, the best way to fight back against these negative use cases of AI is by keeping informed. Knowing how to spot suspicious emails and determine if they are fraudulent or legitimate can prevent people from falling victim to AI-powered phishing scams and implementing strong cybersecurity practices—including strong password use and access control measures—can make our networks less vulnerable to an automated attack.

AI is an incredibly powerful tool, and while it has the potential to help the world in many ways, wrongdoers can exploit its capabilities in ways that create new cyber threats. To address these cyber threats spurred by the misuse of AI technology, we must understand how it is being abused and what can be done to stop these abuses. ▣

Protecting OT data under persistent threat from ransomware

These attacks not only threaten the security of sensitive information but also disrupt critical industrial operations, leading to significant financial losses and the damaging of trust among consumers and partners.

By [Aron Brand](#)

■ A worrying statistic the [State of Ransomware in Manufacturing and Production 2023](#) confirms what IT and cybersecurity professionals already know: Manufacturing, with its wide use of operational technology, is a prime target for cybercriminals. The report reveals a staggering fact: More than half of manufacturing organizations—56%—were hit by ransomware from 2022 to 2023 alone.

Ransomware targeting industrial systems has evolved significantly in the last few years, with cybercriminals shifting from widespread, scattershot attacks to more focused, destructive campaigns against specific industries, with [manufacturing at the forefront](#).

See also: [Tailored cybersecurity solutions for U.S. manufacturing](#)

The interconnected nature of modern manufacturing operations, relying heavily on supervisory control and data acquisition (SCADA) and critical industrial control systems (ICS), and the prevalence of legacy systems that are difficult or costly

to upgrade make this sector particularly vulnerable.

These ransomware attacks not only threaten the security of sensitive data but also disrupt critical industrial operations, leading to significant financial losses and damaging trust among consumers and partners.

UNDERSTANDING THE THREAT RANSOMWARE POSES

The manufacturing sector's reliance on OT alongside information technology (IT) systems increases its exposure to ransomware attacks. Many OT systems weren't designed with cybersecurity in mind and often run on outdated software that's difficult to update. This creates an ideal breeding ground for ransomware to take root and spread across both IT and OT networks.

See also: [Maximum security? How multifactor authentication is being defeated](#)

Moreover, the adoption of Internet of Things (IoT) devices in manufacturing facilities, intended

to boost efficiency and automation, expands the attack surface. Each connected IoT device is a potential entry point for cybercriminals to gain initial access.

SCADA systems, crucial for industrial control systems in manufacturing operations, are often connected to the internet or other networks, making them vulnerable to the same cyber threats that can exploit IoT devices.

According to the [Dragos 2023 OT Cybersecurity Year in Review](#) report, several cyber adversary groups targeting industrial OT systems employ living off the land (LOTL) techniques as a means to achieve their objectives within these networks.

See also: [Navigating red-alert security challenges in manufacturing](#)

By using native tools already present in the OT environments and exploiting valid or default credentials, they can stay hidden for longer periods. The VOLTZITE threat group, for example, makes heavy use of LOTL techniques in

industrial OT networks, enabling them to remain persistent in these environments for considerable periods, impairing detection and incident response efforts.

ADOPT A LAYERED SECURITY APPROACH TO SHIELD DATA

A layered security approach, also known as defense-in-depth, can help protect data in manufacturing, particularly given the integration of IoT and SCADA systems. Beyond regular software updates where possible, and investing in employee training, this involves multiple security measures to protect the different aspects of the manufacturing network and its data including:

ZERO-TRUST ARCHITECTURE

Adopting a zero-trust architecture is crucial for securing ICS and OT environments, especially in the presence of legacy, out-of-support components that cannot be easily updated or patched.

This approach ensures that no entity, whether inside the industrial network or outside, is trusted by default. Continuous verification of all access requests to OT assets, such as programmable logic controllers (PLCs), SCADA systems, and human-machine interfaces (HMIs), is required.

By implementing zero-trust, manufacturers and critical infrastructure operators can dramatically enhance their

security posture, ensuring that each component of their industrial processes is secured against potential breaches, which could lead to severe operational disruptions or safety incidents.

See also: [In reader survey, wide majority worries about OT vulnerabilities](#)

This zero-trust approach becomes even more critical due to the presence of legacy systems that may have known vulnerabilities but cannot be easily updated, making them prime targets for cyber threats.

Network segmentation and the use of virtual local area networks (VLANs) play a crucial role in isolating different segments of the OT network, much like the subdivision of a submarine hull into watertight compartments for protection.

This isolation strategy helps limit the potential spread of threats and contain any potential breaches within a specific compartment or segment, mitigating the risk posed by both external threats and internally lurking threats, such as malicious insiders or compromised user accounts.

By segmenting the network into watertight compartments, a breach in one segment can be prevented from cascading and impacting other segments, thus minimizing the overall impact on industrial operations.

AIR-GAPPED BACKUPS FOR INDUSTRIAL DATA

Data backups serve as a critical safeguard for industrial environments, ensuring that essential operational data, configuration files, and regulatory data such as video surveillance footage can be restored quickly in the event of a cyberattack or system failure.

Regular backups, preferably continuous, should be performed, keeping copies of all important industrial data, system configurations, logs, and regulatory data both on-site and off-site. However, backups alone are not sufficient.

See also: [Air gapping OT assets may be the only sure way to shield critical infrastructure](#)

As ransomware attacks become more sophisticated, with [94% of victims reportedly having their backups targeted by attackers](#), according to Sophos, manufacturers and critical infrastructure operators must implement robust, air-gapped backup strategies.

Air-gapped backups are physically and logically isolated from the industrial control network to prevent ransomware malware from compromising the backup systems.

Immutable cloud storage is ideal, with solutions such as AWS Object Lock providing strong immutability guarantees and being in separate physical locations

with distinct administrative permissions and users.

Never trust backups blindly; periodic restoration trials are also essential to confirm the completeness and functionality of the backups.

LEVERAGING AI FOR INDUSTRIAL CYBERSECURITY

As manufacturers and critical infrastructure operators strive to combat the rapid proliferation and mutations of cyber threats targeting industrial control systems, leveraging the power of artificial intelligence and machine learning has become essential.

The relevance of traditional signature-based defenses has diminished in the ransomware space, particularly against zero-day attacks. Modern cybersecurity platforms now employ AI and ML to monitor

behavior across both OT networks and IT infrastructure.

These technologies enable the detection of anomalies, identification of potential threats, and real-time responses, providing a proactive defense against ransomware, malware, and other cyberattacks.

See also: [Why IoT device manufacturers need to prioritize cyber resilience](#)

By leveraging hybrid-cloud solutions that apply AI to behavioral audit logs, manufacturers and critical infrastructure operators can enhance their cybersecurity posture and protect their industrial operations from potential disruptions or safety incidents.

Additionally, the implementation of behavioral anomaly detection further enhances the ability to identify subtle irregularities that

may indicate a threat. Given the imminent risk of AI-based threats, there is a compelling need for AI-based defensive capabilities to stay ahead of sophisticated cyber adversaries.

See also: [Effective cybersecurity depends on an effective IT/OT partnership](#)

As cyber threats evolve, the defensive strategies of manufacturing companies must mutate as well. The growing menace of ransomware demands more than data protection—it requires a commitment to maintaining operational continuity and safeguarding the integrity of supply chains.

Manufacturers need to adopt a proactive and layered approach to cybersecurity if they hope to keep their business in business in 2024 and beyond. ▣

Navigating red-alert security challenges in manufacturing

Cyber threats have evolved into a formidable adversary, targeting the factory floor with relentless precision.

By [Frank Balonis](#)

Manufacturing executives stand at the forefront of an industry driven by relentless innovation and technological advancement. Yet, amid the exhilarating pace of progress, a looming shadow threatens to undermine these efforts—cybersecurity threats.

The recent [Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report](#) paints a stark picture: Manufacturing is under siege from escalating cyber threats, requiring urgent action to fortify digital defenses and safeguard the very essence of innovation.

Cyber threats have evolved into a formidable adversary, targeting manufacturing companies with relentless precision. The Kiteworks report's findings reveal a sobering truth—the average cost of a data breach in manufacturing surged by 5.4% from 2021 to 2022, reaching a staggering \$4.47 million.

See also: [Maximum security? How multifactor authentication is being defeated](#)

This financial toll, coupled with the primary targets of cyberattacks being personally identifiable information (PII) in 60% of cases and the prevalence of denial of service (DoS) objectives in nearly two-thirds of incidents, underscores the urgent need for robust risk-management strategies.

One of the prominent challenges highlighted in the report is the proliferation of disparate tools used for sensitive content communications within manufacturing companies.

An astounding 85% of manufacturers rely on five or more tools, leading to a fragmented landscape that hampers compliance and security management. This complexity not only poses operational hurdles but also inflates expenses, with significant investments directed toward communication tools.

Manufacturers also face substantial risks associated with third-party content communication channels, with nearly two-thirds utilizing six or more systems for managing,

controlling, and securing content communications with external entities. File sharing and mobile application communication emerge as particularly risky channels, demanding immediate attention and robust mitigation strategies.

IMMEDIATE ACTION

AGENDA: BEST PRACTICES FOR CYBER RESILIENCE

In response to these pressing challenges, a proactive and comprehensive approach to cybersecurity is paramount. Here are five urgent action steps that manufacturing executives must prioritize:

1. Conduct cybersecurity

assessments: Initiate comprehensive audits and risk assessments to develop targeted cybersecurity strategies promptly. Identify vulnerabilities and prioritize mitigation efforts based on risk exposure.

2. Implement multifactor

authentication: Strengthen authentication processes with MFA for accessing sensitive

systems and data immediately. This additional layer of security significantly reduces the risk of unauthorized access.

3. **Establish incident response plans:** Develop and deploy incident response plans urgently to swiftly address and mitigate cyber threats. A well-defined response strategy minimizes the impact of breaches and ensures swift recovery.
4. **Educate and train employees:** Conduct regular and immediate cybersecurity training and awareness programs for all employees. Empower your workforce to recognize and respond effectively to cyber threats, particularly phishing scams and social engineering attacks.
5. **Enhance supply chain security:** Collaborate with supply chain partners urgently to implement robust cybersecurity measures. Strengthening the cybersecurity posture across the entire supply chain ecosystem is crucial for mitigating risks and ensuring resilience.

These action steps can strengthen your organization's resilience against data security threats, enhance your regulatory compliance posture, and unlock new levels of efficiency and innovation in your manufacturing processes.

ADDRESSING DATA PROTECTION, COMPLIANCE, AND EFFICIENCY CHALLENGES

The manufacturing industry confronts multifaceted challenges daily. To navigate the complex landscape of data protection, compliance issues, and efficiency dilemmas, here are three immediate actions manufacturers should consider implementing:

- Implement robust data security measures:** Manufacturers have embraced the concept of digital transformation, which has yielded advances in efficiency, accuracy, and profitability. But as this transformation continues, manufacturers also face greater dependency on sensitive data and its secure transmission. To ensure data security, manufacturers should:
 - Conduct a comprehensive assessment of current data security protocols to identify vulnerabilities and risks.
 - Invest in advanced cybersecurity technologies such as encryption, intrusion detection systems, and data loss prevention tools to fortify data protection.
 - Enforce strict access controls, authentication measures, and continuous employee training programs to prevent unauthorized access and data breaches.
 - Develop and update data security policies and procedures regularly

to align with industry standards and regulatory requirements.

Enhance regulatory compliance practices: The growth of the manufacturing industry has also been accompanied by a more complex regulatory environment, and in particular, as manufacturing technology becomes more sophisticated, so too are regulatory standards and compliance requirements for data security and data protection.

See also: [Inside the Rockwell, Church & Dwight OT cybersecurity team-up](#)

Compliance is especially intricate for manufacturers with a global footprint who may have to adhere to regulations across multiple jurisdictions. To ensure compliance, they will need to:

- Establish a dedicated compliance team or designate compliance officers within the organization to oversee regulatory requirements.
- Conduct regular audits and assessments to monitor compliance with international standards, data protection laws, and industry-specific regulations.
- Stay abreast of evolving regulatory frameworks and proactively implement necessary changes to ensure ongoing compliance.
- Foster collaboration with legal advisors, industry associations, and regulatory authorities to gain

insights into best practices and emerging compliance challenges.

Optimize data management

strategies: As manufacturers become more digitized and reliant on big data for everything from the shop floor to the global supply chain, management of that vast quantity of data may become a challenge as companies leverage increasingly sophisticated tools to glean insights and value from the information being collected.

Replay: [Taming data and no-nonsense ways to drive your digital transformation](#)

To optimize data management, companies must:

- Embrace advanced data analytics tools and platforms to process and analyze vast data generated by manufacturing processes effectively.
- Develop robust data governance frameworks to ensure data quality, integrity, and consistency across your organization.
- Leverage predictive analytics and machine learning algorithms to extract valuable insights that can enhance operational efficiency and decision-making.
- Collaborate with technology partners and data management experts to design tailored data

management solutions that align with your manufacturing operation's unique needs.

By taking these immediate actions, you can proactively address data protection risks, strengthen your regulatory compliance posture, and optimize efficiency in your manufacturing processes. This strategic approach will not only safeguard your organization's reputation and data integrity but also position it for sustainable growth and innovation in an increasingly complex and interconnected business environment. ▣

