Managing Access & Risk in the Connected OT Environment:

4 Key Findings for the Manufacturing Industry

Based on research by

Ponemon INSTITUTE

BearingPoint®

Cyolo

TABLE OF CONTENTS

INTRODUCTION

The manufacturing industry is undergoing a period of intense transformation as organizations adopt increased connectivity and industrial automation. The integration of Internet of Things (IoT) devices, advanced robotics, and real-time data analytics into manufacturing processes significantly enhances the efficiency of Industry 4.0-enabled organizations, but simultaneously broadens the cyber risk landscape and expands the potential attack surface for nefarious actors.

More specifically, many manufacturing systems now interlink networks that traditionally operated in isolation, exposing critical infrastructure to new and evolving cyber threats. The convergence of operational technology (OT) and information technology (IT) systems demands specialized security and access management solutions tailored to protect not only data confidentiality and integrity but also to ensure the availability and safety of manufacturing operations and processes. As organizations strive to mitigate risks and ensure secure access to sensitive OT environments, they face a range of **unique and complex challenges**.

High on the list of challenges is the predominance of legacy systems and infrastructure that are relied upon to keep many industrial processes running. These systems are vital to the functioning of the factory, but they are also old (often years or even decades past their end-of-life date) and cannot easily integrate with modern identity and cybersecurity protection, leaving them vulnerable to cyberthreats and unauthorized access attempts. Bringing these systems up to date with the latest security best practices typically requires extensive upgrades that themselves can cause highly problematic operational disruptions.

Another major challenge relates to the dependence of many manufacturing organizations on third-party vendors, technicians, and other contractors. These external specialists help keep operations running smoothly, but the organization vastly increases its attack surface when it opens its OT environments to third parties who are not bound by internal security policies and often work on unmanaged, uncontrolled devices. In the worst case scenario, third-party relationships can lead to disastrous supply chain attacks, as interconnected dependencies mean **a single breach can have cascading effects** across global manufacturing operations.

So, where do manufacturing organizations actually stand when it comes to combatting cyberthreats and protecting their OT environments? A comprehensive research report, conducted by the Ponemon Institute and sponsored by Cyolo, sheds light on this important topic. To create the report, the Ponemon Insitute surveyed 1,056 security professionals across the US and EMEA, 12% of whom reported that they work in manufacturing.

In this paper, we will explore several key data points specific to the manufacturing industry and make recommendations to help organizations in the industry ensure the security and safety of their OT environments and critical processes.

*To gain a more complete understanding of trends in OT security and cross-industry challenges related to OT systems access, **read the complete report**.*

KEY FINDINGS

1

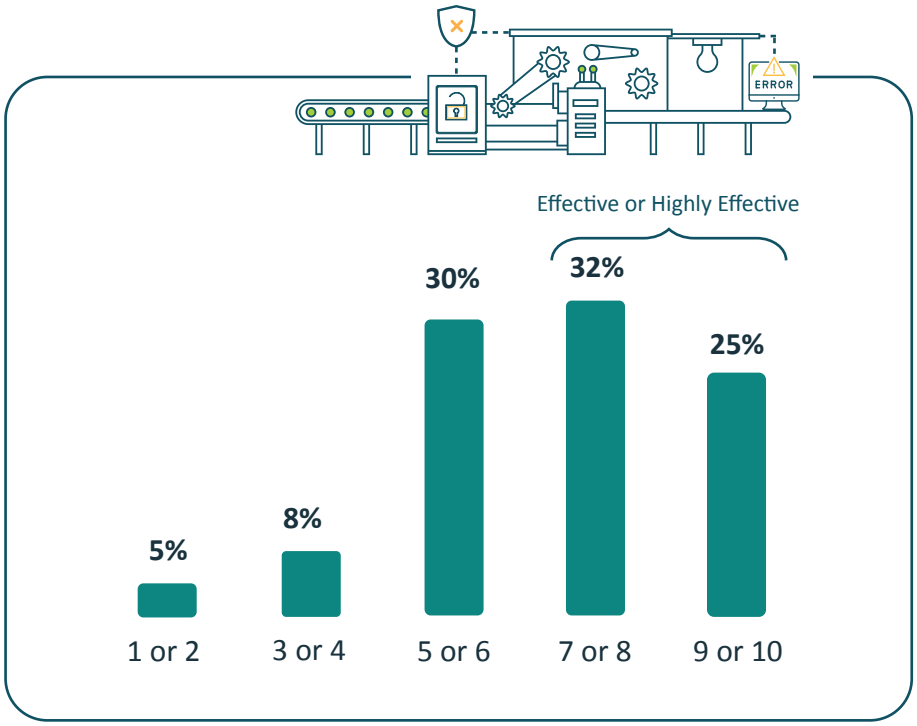
Too many manufacturing organizations are not effectively protecting their OT environments.

When asked to rate their organization's effectiveness in reducing risks and security threats to the OT environment on a scale from 1 = not effective to 10 = highly effective, just 57% of respondents from the manufacturing industry called their organization effective or highly effective (7-10 on the 10-point scale) in achieving these objectives. **As many as 13% admitted to being ineffective when it comes to mitigating risks and threats,** and the remaining 30% offered a rating that we could call "moderately effective."

Figure 1

How effective is your organization in mitigating risks and security threats to its OT environment?

Please use the scale from 1 = not effective to 10 = highly effective.



As stated in the full Ponemon report, "there are scenarios in which being 'moderately effective' is sufficient, but OT cybersecurity is not one of them." This is most certainly the case when it comes to securing heavy machinery and the other equipment, systems, and processes within manufacturing environments. Effective security defenses are absolutely essential, as a single cyber incident or instance of unauthorized access could cause potentially catastrophic results, not only in the financial realm but also in the physical.

Recommendation 1: For the sake of both security and safety, manufacturing organizations that lack confidence in their current cyberthreat and risk mitigation strategies must adopt new approaches and likely also new security and access management solutions.

First steps to take include beginning to treat all connections to critical systems as cases of privileged access, requiring multi-factor authentication (MFA) to all applications (including the legacy applications common within OT environments), and granting access exclusively to the application-level and never to the full network. These measures limit the amount of damage an attacker could cause if they succeeded to gain access to the factory floor.

2

Only 23% of manufacturing organizations have an accurate OT asset inventory.

Organizations cannot protect assets they do not know they have, and the research reveals an alarmingly large majority of organizations in fact do not know exactly what can be found inside their OT environment.

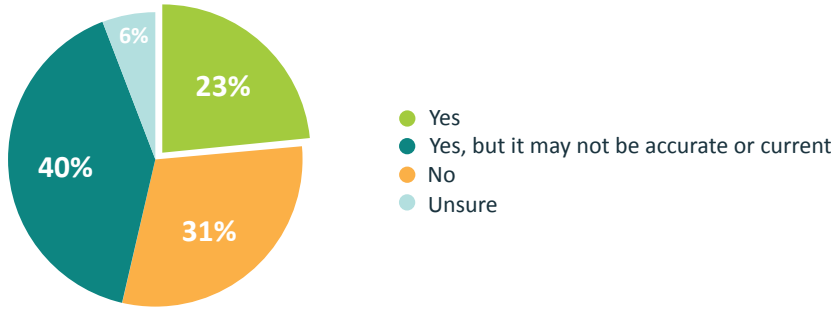
More than three-quarters (77%) of respondents from the manufacturing field report that their organizations do not maintain an accurate, up-to-date inventory of the industrial assets in their OT environments. With just 23% that do maintain a full and current OT asset inventory, manufacturing organizations lag slightly behind the cross-industry figure of 27%.

77%

of manufacturing organizations lack an authoritative OT asset inventory.

Figure 2

Does your organization maintain an inventory of the industrial assets in its OT environment?



Recommendation 2: Without a clear picture of the number and types of industrial assets they hold, organizations will have difficulty mounting a comprehensive defense. All who find themselves in this position should devote time to taking stock of their assets and then put processes in place to guarantee this inventory is maintained and regularly updated.

But, as crucial as it is to establish an OT asset inventory, it is equally crucial that organizations that aren't doing so already immediately begin enforcing policies to ensure secure access to the OT environment for both remote and on-prem users and devices. Creating an inventory will take time, particularly because some asset owners are likely to have moved to other roles and even other organizations. During this stock-taking period, critical systems and resources will remain vulnerable unless proper controls around secure access, connectivity, and oversight have been implemented.

For the fastest and most impactful results, organizations should prioritize instances of privileged access (this could include remote connections, third-party users, and other especially risky connections) and secure these first.

3

Manufacturing organizations open their OT environment to dozens of third-party vendors without fully addressing the risks this poses.

Third-party vendors, technicians, and other specialists play a vital role when it comes to keeping manufacturing operations up and running. In past content we have discussed in detail why industrial organizations rely so heavily on third-party support and how this dependence increases risk if access and connectivity are not tightly controlled and monitored.

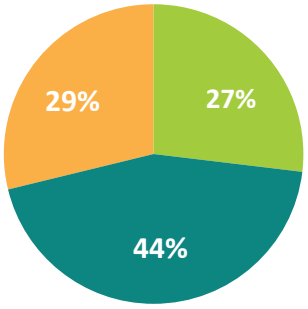
Data from the Ponemon survey confirms that manufacturing environments are in effect wide open to third-party vendors. According to the research, **71% of respondents reported that their organization authorizes OT environment access for third parties.** Diving deeper into this number, we discover that 44% allow remote as well as on-site access, while 27% permit third parties to connect to the OT environment only in-person. The COVID-19 pandemic marked a sea change in industrial organizations' willingness to enable remote connections into the OT environment, and recent trends indicate that the percentage that allow remote access for third-party vendors will only continue to rise.

So, just how many people are we talking about here? In the manufacturing industry, a full quarter (25%) of organizations who permit third-party access to OT systems limit such access to 10 or fewer vendors. This is a greater percentage than what was reported for oil and gas (20%), energy and utilities (19%), transportation and logistics (22%), or the cross-industry total of 21%.

But even while a sizable percentage of manufacturers permit OT environment access for only a small number of vendors, **a majority (57%) grant access to more than 50 different vendors – and 26% give OT access to more than 100 vendors.**

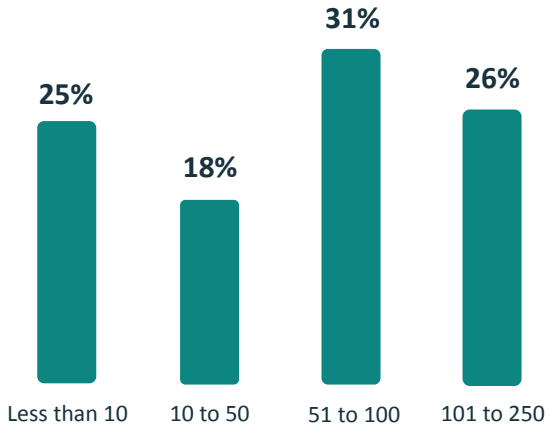
Figure 3

Does your organization permit third-party vendors to access its OT environment?



- Yes, but only on-site
- Yes, on-site and remote
- No

How many **vendors/third parties** are authorized to connect to your organization's OT environment?



Notably, even as most manufacturers are opening their OT environments to dozens of different third parties, just 16% of respondents from the industry reported that they are very concerned (9-10 on the 10-point scale) about the risks of this access. An equal 16% reported being very unconcerned (1-2 on the 10-point scale) about third-party access risk.

How concerned is your organization about risks created by vendors/third parties accessing its OT environment?

Whether or not organizations and their workers recognize it, opening the OT environment to third-party vendors without implementing the proper access controls is inherently risky. There are many well-documented reasons for this, including third parties' lack of familiarity with internal security policies, the fact that they typically work on unmanaged devices, and the difficulty of monitoring or controlling their activity after access has been granted.

Recommendation 3: Manufacturing organizations cannot afford to implicitly trust third-party vendors to employ best practices when connecting to the OT environment, nor can they blindly assume that vendors' security posture meets a high standard. To protect their critical assets, environments, and processes, manufacturers must implement **identity-based access for third-party users** and devices as well as connectivity and supervisory controls.

Additional recommended actions include augmenting or replacing legacy secure remote access (SRA) tools like VPNs with solutions that provide zero-trust access, enforcing MFA (including to the legacy systems typical to OT environments), setting access permissions for all third-party vendors according to the principle of least privilege, and adopting controls like session recording and supervised access to monitor what third-party users are doing while connected to critical systems.

4

Organizations lack a sense of urgency around OT security and compliance.

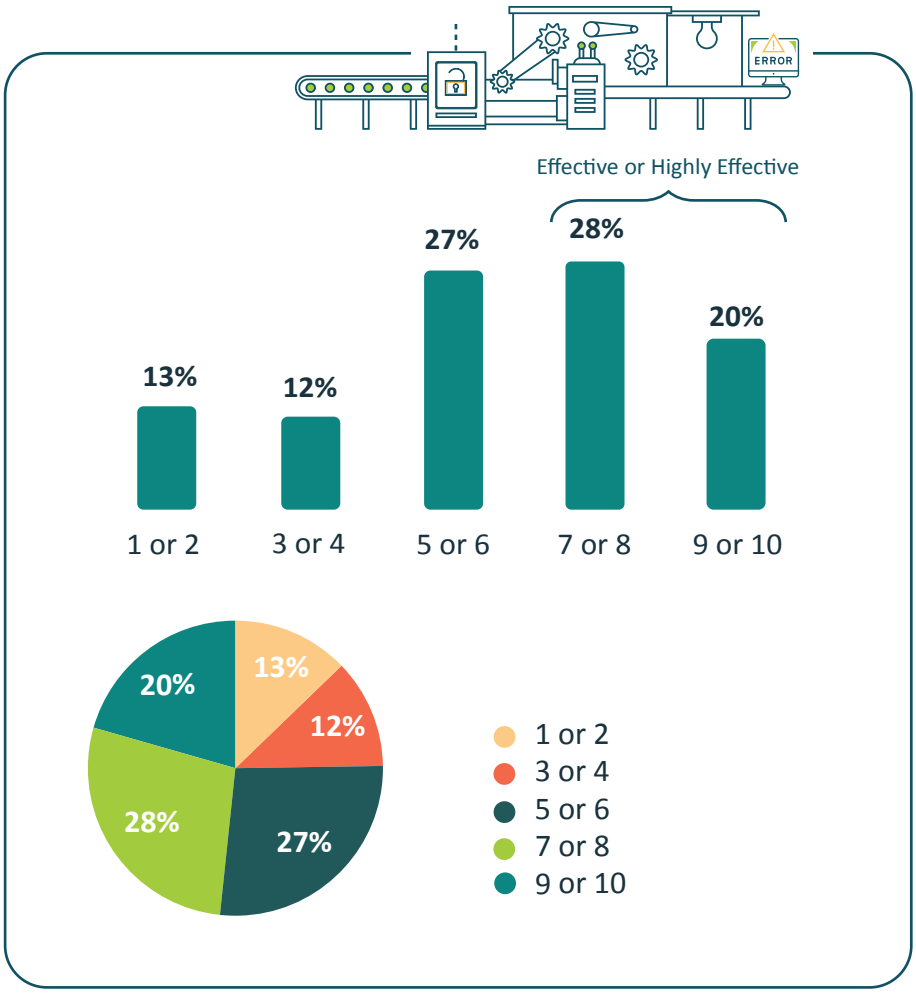
Perhaps due to the long history of OT isolation, many organizations across industries, but especially in manufacturing, do not seem to fully grasp the crucial and urgent need to secure these systems against unauthorized access and its potentially disastrous consequences.

When asked to rate the priority of securing access to OT environments on a scale from 1 = not a priority to 10 = a high priority, only 20% of respondents from the manufacturing industry answered that it is a high priority (9-10 on the 10-point scale). As a comparison, at least 26% (still, quite a low percentage!) of respondents from the oil and gas, energy and utilities, and transportation and logistics industries called securing OT access a very high priority.

Fortunately, when we combine those who rated security as either a priority or a high priority (7-10 on the 10-point scale) the total does reach 48% for manufacturing. This is certainly better than 20%, but it is still fewer than half of overall respondents who identify securing access to the OT environment as a key priority.

Figure 4

How much of a priority is securing access to your organization's OT/ICS environments?



There is no question that security teams have countless important tasks to fulfill (often with limited resources), and not every project can be given the attention it deserves. Still, in light of the potential consequences of a breach, it is surprising that more organizations are not making it a priority to secure access to their OT systems.

Besides the fact that security teams are overworked, what could be causing OT access security to be receiving short shrift, particularly in manufacturing? The Ponemon survey did not specifically address the growing skills gap, but numerous other studies have documented the severe shortage of workers entering the manufacturing industry. According to Deloitte, "talent shortages and skills gaps are challenging manufacturing operations. 77% of manufacturers say they will have ongoing difficulties in attracting and retaining workers." The Deloitte report specifies that both entry-level positions and roles for highly skilled individuals are going unfilled.

Regarding the latter point, more than half (51%) of manufacturing respondents to the Ponemon survey did cite "lack of expertise" as a major barrier to ensuring secure OT environment access for third-party vendors. This noted "lack of expertise," together with the skills gap, likely contributes to the fact that security professionals in manufacturing are less aware of the risks of not properly securing OT access – leading professionals in the industry not to identify secure access as a significant priority.

If the risks of data and intellectual property loss, damaging operational disruptions, and possible safety hazards don't motivate manufacturers to place a greater emphasis on OT environment security, then perhaps the large and growing list of compliance mandates will. 52% of manufacturing respondents to the Ponemon survey reported that their organization is currently required to comply with industry regulations for ensuring secure access to OT environments. An additional 27% noted that no regulations apply today but relevant new mandates will likely demand compliance in the future.

Recommendation 4: Now more than ever, there is growing pressure and greater urgency to meet various regulatory and compliance standards. Manufacturers can help ensure their adherence to both current and future regulations by adopting an OT-specific cybersecurity framework. The IEC 62443 standards, as just one example, provide crucial guidance for addressing security needs throughout the lifecycle of OT systems and processes.

Developing and executing cybersecurity strategies are heavily influenced by regulatory demands and compliance frameworks. Companies need to navigate these requirements while keeping their operations efficient. Standards like IEC 62443, as well as ISO 27001 and NIST Cybersecurity Framework (CSF), offer strong protection against the ever-changing landscape of cyber threats and help organization to not just meet compliance demands but also (and perhaps ultimately more importantly) to ensure resilience and maintain operational integrity.

Key standards and regulations in the manufacturing industry include:

- **IEC 62443 Standards:** These are becoming the go-to for securing industrial control systems (ICS) in various industries, including manufacturing.
- **NIS2 Directive:** This updated EU critical infrastructure regulation expands its reach to include manufacturing and other critical sectors. NIS2 sets out requirements for cybersecurity incident reporting and mandates risk management measures.
- **Cyber Resilience Act (CRA):** Likely to have a compliance deadline of 2027, the CRA is set be the world's first regulation that defines security requirements for products as a market entry barrier. More simply put, once the CRA is in effect, 'products with digital elements' will no longer be offered in the EU unless certain security conditions are met.
- **Machinery Regulation (EU) 2023/1230:** While not focused exclusively on cybersecurity, this regulation includes health and safety requirements for machinery, considering cybersecurity and digital instructions.
- **Singapore's Cybersecurity Act's Codes of Practice:** Known as CCoP 2.0, this is a key standard for Critical Information Infrastructure (CII) owners in Singapore.
- **Australia's Security of Critical Infrastructure Act 2018 (SOCI Act 2018):** The Act is part of Australia's broader strategy to protect essential services like electricity, water, port facilities, and manufacturing which are crucial for the nation's well-being and security.
- **U.S. HHS FDA Cybersecurity Requirements:** These new requirements focus on cybersecurity for cyber devices in healthcare.
- The National Institute of Standards and Technology **(NIST)** released a summary and analysis of comments on **SP 800-171** Revision 3's initial public draft, impacting numerous businesses working with the federal government.

Conclusion: Now is the Perfect Time to Prioritize Securing OT Environment Access

Modern manufacturing organizations face real and persistent obstacles when it comes to securing critical systems against unauthorized access and other cyberthreats. The isolation that once largely protected OT systems from such threats has given way to a new era of connectivity that promises greater productivity and security even while creating serious potential risks. At the same time, organizations depend on the specialized skills and subject matter expertise of third-party vendors to help keep operations running, but connecting these users and their devices to OT environments without implementing the proper access controls also increases risk.

The data collected in the Ponemon study reveals major gaps in manufacturers' current efforts to manage OT systems access and risk. Significant progress can and must be made in a variety of areas, including but not limited to risk mitigation, industrial asset management, and oversight of third-party access and remote connections.

The good news is that there are security solutions available today that can drastically lower the risks of third-party access and OT connectivity. The Cyolo PRO secure access solution enables organizations to safely connect third parties, including OEMs, to OT environments for enhanced productivity. **Cyolo PRO (Privileged Remote Operations) is an advanced, infrastructure-agnostic solution that redefines Secure Remote Access by shifting the outcome from managing access to managing operations.**

Learn more about Cyolo PRO and read the complete Ponemon Institute research report for more insights into how organizations across industries are managing threats to the connected OT environment.