WHITE PAPER

The Importance of Manufacturing Security in the Industrial Enterprise

Managing Risk in Industry 4.0

Connection®
we solve IT®

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.connection.com

What's Your Industry 4.0 Risk Strategy?

Industry 4.0's merger of what were once two distinct technology areas—operational technology (OT) and Informational Technology (IT)—promises great benefits. Unfortunately, a rushed integration of OT and IT technology stacks can easily create new security risks that malicious actors can exploit. Fortunately, with careful planning, it is possible to mitigate cybersecurity risks that stem from Industry 4.0 implementations.

Manufacturing Is Under Attack

In 2020, manufacturing became the second-most attacked industry, after finance.

Manufacturing is experiencing increasing interest from malicious actors. In 2019, one study found that 74% of OT professionals had experienced a breach in the past 12 months. In 2020, manufacturing became the second-most attacked industry, after finance. Worryingly, manufacturing was only the eighth-most attacked industry in 2019.

Additionally, 33% of all data theft incidents in 2020 were inflicted on manufacturers. There are clues to cyberattackers' intent: 21% of attacks on manufacturers in 2020 came from ransomware—more than in any other sector. A 2020 Verizon study found that 73% of manufacturing incidents are financially motivated. Malicious actors recognize that manufacturers have an extremely low tolerance for downtime, and coordinate profitable ransomware attacks accordingly.

Case Study: Steelcase

In October 2020, furniture manufacturer Steelcase suffered a Ryuk ransomware attack. Ryuk actors most likely used access provided by BazarLoader or TrickBot to deploy ransomware on Steelcase's network.

Steelcase reported that it temporarily shut down parts of its network to contain the attack's spread. Ultimately, Steelcase reported that no information was stolen, but it was forced to shut down global operations for two weeks. As a result, some Steelcase shipments were delayed, and the company incurred additional costs while its systems were repaired, restored, and strengthened.

Considering Steelcase is the largest office furniture manufacturer in the world, with 13,000 employees and $3.7 billion in annual revenue, the Ryuk ransomware attack would have been extremely costly.

Attacks Cause Significant Losses

The costs of intrusions are significant. Large manufacturers can lose millions of dollars in a cyberattack: aluminum producer Norsk Hydro lost $75 million in the aftermath of its 2019 breach. With downtime costing as much as $260,000 per hour, even minor breaches can prove costly.

But the damage doesn't stop with money. Of manufacturers who experienced an intrusion, 40% reported a degradation in brand awareness, and 35% reported operational outages that put physical safety at risk. With that much at stake, manufacturing security is critical to get right.

65% of manufacturing environments run on outdated operating systems.

Industry 4.0 Presents Major Security Challenges

Managed devices, lifecycle management, and other standard security protocols have enabled IT departments to limit an organization's risk profile for some time.

However, conventional IT practices don't transfer neatly to the manufacturing floor. On top of the regular business demands for more timely data, insight, and reporting, IT professionals in manufacturing face a myriad of additional complexities as they try to merge OT and IT tech stacks. As a result, they may feel frustrated, challenged, and under pressure to deliver results.

Diverse and Aging Technology Stacks

Manufacturing teams are skeptical of any security solution that might impact uptime. Consequently, both IT professionals and manufacturing teams must come to a mutual understanding of how endpoint protection or other security implementations will affect a machine's performance, how enterprise security policies affect unmanaged machines, and more.

In addition, manufacturing frequently relies on old, outdated, or aging machines. In fact, 65% of manufacturing environments run on outdated operating systems. These machines may be critical components of legacy processes, or may simply be in operation to maximize return on investment. Either way, machines have long lifecycles, and it is unlikely that the security solution is to just buy a new machine or upgrade. In this scenario, it is imperative for IT professionals to support end-of-life products with a comprehensive security strategy.

Finally, manufacturing teams often rely on a diverse range of equipment for their operations. Even if these diverse machines are up to date, they likely utilize different operating systems. Here, IT professionals must recognize that the type of operating system standardization found in an office suite might not make sense for the factory floor.

The Endpoint Puzzle

The Industrial Internet of Things (IIoT) and remote machine control systems are significant drivers of Industry 4.0. Unfortunately, these technologies also have considerable security risks.

An integrated monitoring environment across both IT and OT will provide the best chance of success in defending against attacks.

Currently, manufacturers connect an average of 4.7 IoT technologies to their organization's network. With IIoT connections on track to increase from 17.7 billion in 2020 to 36.8 billion in 2025, IT professionals must be prepared to secure a rapidly growing attack surface. IIoT devices, the networks they operate on, their data transfers to and from the cloud, and their interfaces with end users all need reinforcement to ensure network integrity.

Many manufacturers utilize industrial control systems (ICS) or supervisory control and data acquisition systems (SCADA). While ICS and SCADA enable significant productivity improvements within manufacturing organizations, they come with major security risks. In fact, just 11% of organizations utilizing SCADA/ICS report that they have never experienced a security breach. Additionally, threats are not limited to external actors: only 55% of SCADA/ICS operators use role-based access control, leaving openings for internal breaches.

Fortunately, most risks with SCADA/ICS can be mitigated. As manufacturers often give partner organizations high-level access to SCADA/ICS, IT professionals must take appropriate measures to protect their network from vulnerabilities. Implementing security measures such as role-based access control, secure shell (SSH) or transport layer security (TLS) encryption, and network security controls can minimize security risks to these vital pieces of equipment.

An Unmanaged Mess

Unmanaged networks are often unaddressed in manufacturing environments. Industrial environments commonly use a patchwork of network infrastructure, relying on nonuniform routers, nodes, protocols, and connectivity. These networks can bypass corporate infrastructure, leave machines and data vulnerable to attack, and provide limited options for IT teams to respond and remediate. Unfortunately, even though IT teams don't manage these networks, they are left to clean up the mess.

IT professionals need to restructure these unmanaged networks for effective monitoring through a single pane of glass. Hodgepodge networking solutions can be replaced with next-generation industrial networking technologies that support both traditional IT and industrial protocols. In addition to firewalls and intrusion protection, security threats can be mitigated with zero-trust policies, profiling of industrial devices, deep packet inspection, and comprehensive security monitoring from facility edge to the data center. In sum, an integrated monitoring environment across both IT and OT will provide the best chance of success in defending against attacks.

Data Storage and Recovery

Even the best laid plans can go awry. If a security event does occur, restoring critical data is vital to resuming operations and reducing losses from downtime.

Most business continuity and disaster recovery (BCDR) policies and solutions are designed for enterprise business systems and typical white-collar office environments. However, when planning a BCDR solution for manufacturing, IT professionals must consider the complex, heterogenous OT environment. Implementing a BCDR solution that meets needs for both IT and OT not only accelerates recovery after an event, but drives adoption and compliance within OT as well.

Culture and Resource Challenges

Perhaps the most difficult shifts required in the transition to Industry 4.0 are those of culture, resources, and skillsets. IT and OT have evolved to operate and deliver outcomes without depending heavily on the other. However, the convergence of IT and OT mandates a new, mutually beneficial way of working.

The rapid rate of industrial transformation has left many manufacturing teams struggling to adapt. Few are equipped with adequate resources to manage the wide range of specialty hardware, software, and processes in their facilities. And, while IT and OT appear to have conflicting goals, it is possible to find broad common ground. The success of the enterprise depends on mutual understanding of risks, business and operational demands, compliance requirements, and more. Only then can IT and OT work to implement achievable and sustainable security hygiene.

The Desk vs. The Line

Industry 4.0 requires organizations to build a bridge between the worlds of OT and IT. Since what works at the desk might not work on the production line, OT and IT must build partnerships based on new processes, technologies, and skills.

Importantly, failing to bridge this divide comes with enormous risk. No manufacturer wants to face unplanned downtime due to a security breach. Furthermore, while the initial costs from a breach are always significant, the road back to full recovery can cost more as it can take hours, weeks, or even months.

Connect with Excellence

At Connection, we understand the challenges IT professionals face with Industry 4.0. Our specialists come from the same real-world settings you work in, and we know the pressures and risks you face. Our extensive background in IT and manufacturing allows us to provide right-fit manufacturing security solutions for your organization, helping you mitigate risks and meet operational goals.

Whether you are looking for endpoint protection, industrial BCDR, threat scanning/response, managed security, industrial security, or you are merely unsure of your next step, we can help.

A Trusted Partner

As a leading National Technology Solutions Provider, we've been trusted for more than 38 years to connect people with technology that enhances growth, elevates productivity, and empowers innovation. Connection stands ready to deliver, install, and maintain technology nationwide by leveraging our internal professional services expertise and top-tier vendor partnerships.

Contact us today to learn how to get started.

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.connection.com

Connection
we solve IT