emazzanti technologies
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

Boost Manufacturing Cyber-security with IT/OT Convergence Best Practices

Information technology (IT) and operational technology (OT) alignment improves security and reduces downtime.

Industry 4.0 continues to transform manufacturing. From collaborative robots to powerful data analytics, connected systems offer a host of exciting possibilities. However, those opportunities come with a cost in terms of security. To combat the rising threat of cyber-attacks, manufacturing companies must turn their focus to IT/OT convergence.

Critical Differences Between IT and OT

Before Industry 4.0, information technology (IT) and operational technology (OT) typically operated in separate silos with competing priorities. Even now, IT processes focus on data confidentiality and security. OT, on the other hand, prioritizes availability and safety.

However, with advanced analytics, machine learning and artificial intelligence, the boundaries between the IT and OT have blurred. They can no longer inhabit parallel universes. But with differing priorities, minimal cross-over knowledge and a sometimes-adversarial history, developing a productive working relationship between the two areas can prove challenging.

For example, the IT realm emphasizes patch management to mitigate risk. After all, security experts stress the importance of applying security patches quickly. But on the factory floor, downtime means revenue loss, and a change in one system can cause ripple effects elsewhere. Halting production to apply a patch may have unintended negative repercussions.

Benefits of IT/OT Convergence

While the process of IT/OT convergence may feel cumbersome, aligning the two departments yields tangible benefits. Removing the silos paves the way for more informed business decisions, as well as increased efficiency and greater productivity. In fact, greater alignment can actually improve the security so important to IT while also reducing downtime.

IT/OT Convergence Best Practices

When IT and OT operate in siloes, the separation leaves security gaps that hackers can exploit at will. But when manufacturing companies work to develop an integrated IT/OT security strategy, they can eliminate those gaps and minimize risk. The following IT/OT convergence best practices will start you on the road to greater security.

1. **Security ownership at executive level** – For a security strategy to prove effective, the oversight must come from an executive with organization-wide authority to implement security objectives.

2. **Cross-functional teams** – Effective IT/OT convergence requires communication and shared understanding. Drive the convergence process with cross-functional teams at both the executive level and the working team level. The security team should include specialists trained to operate within the parameters of both IT and OT.

3. **Inventory of technologies and vulnerabilities** – With input from all key stakeholders, develop a detailed list of devices and software. You may be surprised at the number of assets you discover. Identify current policies, priorities and workflows. Also look for security gaps and clarify responsibilities.

4. **Adapt IT best practices to OT environment** – Some IT best practices can actually produce negative effects in the OT environment. For example, encryption can introduce unacceptable

delays unless applied carefully. Consequently, a cross-trained security team will need to adjust best practices to accommodate the OT environment.

5. **Segment IT/OT networks** – Segment the OT from other IT networks. Using separate virtual networks, administrators can more effectively manage OT traffic and reduce exposure to the internet.
6. **Patch management** – Implement a patch management strategy that takes both IT and OT priorities into account. For instance, test patches first on low priority lines to assess potential impacts. Then, coordinate deployment of patches according to downtime schedules.
7. **Ongoing risk monitoring** – Implement regular security audits and ongoing monitoring of all systems. Using artificial intelligence and machine learning, the system can automatically alert security staff to anomalous activity.

Proactive Approach to IT/OT Security

Manufacturers no longer have the luxury of deciding whether or not to integrate IT and OT. Industry 4.0 necessitates a combined approach. And while converging two historically separate operations can introduce challenges, partnering with the right manufacturing cyber-security expert can ease the pain.

The consultants at eMazzanti combine deep knowledge of both manufacturing and cyber-security. We can help your organization implement a comprehensive security strategy to keep data and operational technologies safe from cyber-attack.