3 Steps to Proactive Manufacturing Cyber-Security

Global insurance giant Chubb recently published a cyber risk report listing manufacturing as one of the top two industries targeted by ransomware attacks. With a large attack surface and a high incentive to quickly restore operations, factories make a particularly attractive target. Consequently, the spotlight has turned to increasing manufacturing cyber-security.

In fact, just last March, the Norwegian aluminum producer Norsk Hydro suffered a ransomware attack. The incident forced the company to temporarily close multiple plants, and losses totaled nearly $52 million. Smaller manufacturers, as well, face significant risk, heightened by historically lax cyber-security measures.

Industry 4.0 Blends Opportunity with Risk

With Industry 4.0 and the proliferation of smart factories, manufacturing has reached a critical crossroads. Connected devices and artificial intelligence transform the industry. At the same time, legacy systems with decades-old processes still perform critical roles in production.

This blending of cutting-edge technology and integral, but dated, machinery brings unique risks, and cyber-security for manufacturing struggles to keep pace. Complex supply chains offer greater efficiency but tend to focus on cost and function rather than security. Legacy systems prove difficult to patch with updated security.

Cyber-attacks in the industrial environment can compromise intellectual property as well as cause physical damage. For instance, a slight variance in a system control can slip under the radar and lead to defective products and even safety issues. To protect themselves, factories must address supply chain security, conduct risk assessments and develop recovery plans.

1. Mitigate Supply Chain Security Risks

From raw materials to the sophisticated software that controls industrial robots, factories depend on an increasingly complex supply chain. Each vendor adds potential vulnerability. In addition, in the race to develop cost-efficient, powerful systems, new technologies too often trade security for productivity.

Manufacturers must address security from the very beginning. For instance, when evaluating new equipment and software, look for vendors that provide built-in security as part of the design process. This can include embedded features like hardware security keys.

In addition, carefully assess each vendor in terms of cyber-security and regulatory compliance. Ensure that third party contracts include security policies and procedures. Review and update vendor contracts yearly to keep pace with the evolving threats to manufacturing cyber-security.

2. Conduct Regular Risk Assessments

Cyber criminals constantly develop their weapons and search for vulnerabilities in your system. To protect your organization, you must do the same. First, identify all of your assets connected to the internet. In an era dominated by the internet of things (IoT), this can prove challenging. But keep in mind that anything on the internet provides a potential attack surface.

Secondly, conduct regular comprehensive risk assessments, covering all systems, to detect any vulnerabilities that arise from changes to the environment. Risk assessments should include vendor connections. Follow up with ongoing, vigilant monitoring to detect any anomalies.

3. Develop Detailed Recovery Plans

Even organizations with solid cyber-security can expect an attack. Consequently, you cannot focus exclusively on attack prevention. In terms of cyber-attacks, you must think in terms of *when* an attack occurs, rather than *if*. When you have a detailed business continuity plan in place, you can reduce response time from days or weeks to hours.

When preparing a recovery plan, keep in mind the following:

1. Coordinated recovery strategy – Business continuity reaches far beyond the IT department. Coordinate with every department, as well as with vendors, clearly outlining responsibilities. Identify possible cyber-attack scenarios and detailed actions for each one.

2. Ransomware protocol – Because ransomware presents the most common cyber threat, be sure to develop a ransomware protocol. For example, first response should include immediately retaining system logs. In addition, temporarily shut down internet connections while you contain the breach to avoid further contamination.

3. Backups – Ensure regular system backups. Test for quality and store the backups offsite, where they will remain safe from any attack on the network.

4. Communication plan – Determine a plan for communicating with employees, vendors, customers and law enforcement that is consistent with state and federal law. For instance, most states have data breach notification statutes.

5. Manual overrides – Install manual overrides for critical machinery so that you can shut down a compromised machine before it causes damage.

Proactive Approach to Manufacturing Cyber-security

eMazzanti has worked with manufacturers of all sizes to develop comprehensive cyber-security strategies tailored to their unique industrial environment. We can help you safely incorporate new technology with comprehensive risk assessments and 24/7 network monitoring. We also assist with developing detailed recovery plans to enable a quick return to full operations.