SKODA MINOTTI
CPAs, BUSINESS & FINANCIAL ADVISORS

Cybersecurity Risks in Smart Manufacturing Calls for Strategic Approach

By Joseph Compton, CISSP, CISA, QSA, CICP

The manufacturing industry has increasingly adopted data interconnectivity to achieve greater efficiencies and to better serve their customers' needs. As they integrate the Internet of Things (IoT) and other "smart" manufacturing technology into their daily operations, they also become vulnerable to greater security risks. Owners of industrial and manufacturing companies often do not see their operations as a potential target for cybercriminals. They should.

A Heightened Risk

A Kaspersky Labs report published in October 2017 revealed that in the first half of 2017, manufacturing companies were the most susceptible to cyber threats—their computers accounted for about one-third of all attacks. Hackers are stealing trade secrets, intellectual property and even business plans.

The IoT enables manufacturers to make things faster while data analytics helps them to spot potential problems and efficiently make corrections. The challenge is that the IoT also makes it easier for hackers to compromise systems through the use of malicious botnets, Botnets, a collection of infected Internet-connected devices by which hackers attack a website and all IoT devices connected to the manufacturing process, have become one of the biggest threats to security systems today, allowing cybercriminals to infiltrate almost any internet-connected device.

What's At Stake?

Along with an overall disruption of the manufacturing process, products can be defective, the manufacturer may lose valuable intellectual property and the company may face potential reputational damage. With the increasing number and cost of data breaches, IT security is no longer seen by business leaders as just a technology issue—it has become a business risk.

The Best Defense

Many manufacturers recognize there is a problem, but they often view cybersecurity protection measures as too expensive or cumbersome to take on. However, even with budget limitations, there are strategic steps every manufacturer can take to mitigate security breach risks for their business and their business' customers. These steps include:

1. Adopt an information security framework (PCI, NIST 800, ISO 27001, HITRUST). Implementing security frameworks usually includes conducting a gap assessment and a remediation cycle to implement missing controls.
2. Use data flow diagrams (DFD) to segment sensitive data and systems on the network.
3. Filter outbound network traffic to understand data that is leaving the network.
4. Hire a professional to conduct a risk assessment and penetration testing, which includes the analysis of network assets to identify potential vulnerabilities and threats.
5. Download software updates and patches as soon as they are released; by doing so, you make it more difficult for hackers to exploit vulnerabilities. Better yet, have software updates configured to automatically download.
6. Stay abreast of potential cyber threats and vulnerabilities of any new technology assets.
7. Provide cybersecurity training to all employees so they can recognize potential signs that there has been a breach.
8. Access third-party vendor cyber risks and determine measures that can help prevent any vulnerabilities.
9. Develop a response plan for the business to implement immediately upon a cybersecurity breach. It is not a matter of if your business will experience this in some form—it is a matter of when.

Hackers will use increasingly sophisticated means in their cyberattacks. Manufacturers must find ways to prevent these attempts to corrupt their data, steal their intellectual property and sabotage their operation. While cybersecurity is a serious challenge, it is not insurmountable. Going forward, you will need to tighten security measures as you embrace the very technology that will help you expand your operations. By implementing cybersecurity practices now, they may help prevent costly threats to your business.

Skoda Minotti can help you identify and implement the right security framework for your business. We can work with your manufacturing operation on a proactive approach to defend against a cybersecurity breach.

Questions about protecting your manufacturing operation against cyberattacks? Contact Joe Compton at 440-605-7252 or **email Joe**.