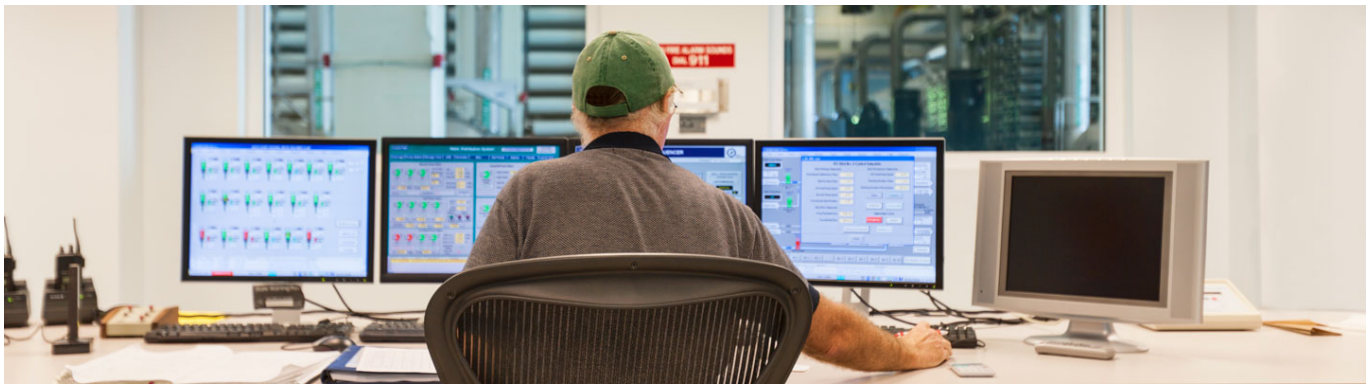

Technology

How Secure Is Your Shop Floor Network?

Don Sears | Jun 11, 2019

It may not be top of mind, but job shops and midsize manufacturers have to be thinking about IT/OT cybersecurity, especially in making military and defense parts. The regulations are here. Are you ready?

Is it enough to purchase the latest machinery and tooling technologies such as 5-axis machines, hire and mentor apprentices and new machinists, crank out parts, and stay on top of maintenance schedules? With smart sensors and more internet-based infrastructure in use now by employees on the shop floor, there is so much technology in and around machines and the control rooms of most shops.

Security management is now a real issue and it includes managing all systems and employee behavior. For those shops that make parts for the defense industry, security is a top compliance issue with a real consequence on business.

“The practicality today is that small to midsized manufacturers are running at capacity, orders are coming in, and the biggest issue is finding and retaining talent—the biggest constraint in getting product out the door. Considering all the decisions that manufacturers have to make every day, cybersecurity is not high on their radar,” says Elliot Forsyth, vice president of business operations at the Michigan Manufacturing Technology Center, in an ***article*** for Advanced Manufacturing.

We talk to industry insiders about the state of security in today’s manufacturing—and where it is heading.

Industrial Cyber Attacks: Data Breaches, Cyberespionage and More

The internet is a fantastic tool and boon for business. But it’s also a place of criminal activity where fraud, ransom, theft and ***system manipulation*** happen too often.

Manufacturing has not been spared from security issues. Industrial sectors, including oil and gas and critical infrastructure segments such as electrical and nuclear power plants, are also having to shore up their security. In 2018, petrochemical companies ***were hacked*** in Saudi Arabia with the intent to sabotage the operation and cause explosions.

This is an extreme case, of course, but it can happen. The majority of security incidents are targeting financial information and intellectual property.

"It's a very insecure space," says John Livingston, CEO of Verve Industrial Protection. "Most manufacturers are generally unaware of the problem or they do not have the resources in-house [to handle it]. … On one hand, many rely on cloud services and at the other end of the spectrum, they rely on old operating systems in their environments that are not patched."

How to Become an IT/OT Cybersecurity-Minded Manufacturer

To make any improvement in security is not all that different than any other major initiative a company undertakes: It starts with documenting and assessing today's reality. Know your risks.

The U.S. government advises companies to follow the guidelines in the ***NIST Cybersecurity Framework***:

"Manufacturers using the framework can measure and assign values to their risk along with the cost and benefits of steps taken to reduce risk. The better a manufacturer can measure its cybersecurity risk and costs, the more effective its cybersecurity solutions will be."

It sounds simple, but there is a lot to it. NIST breaks it down into five cyclical areas:

- Identify
- Protect
- Detect
- Respond
- Recover

Some of this can be outsourced to a third-party IT company or managed security services firm—but there are some very key important issues, such as employee training, that also need to be addressed. It will shift the culture and behavior of employees, but it takes a ton of reinforcement. Plant managers and company leaders play an important role.

NIST provides a self-assessment tool and a slew of ***resource information for manufacturers here***.

To find an MEP in your area with cybersecurity funding for NIST compliance, ***check here***.

In 2018, there were 352 security incidents in manufacturing and 87 of them had a confirmed data disclosure, according to Verizon's "***2019 Data Breach Investigations Report***," which is one of the most comprehensive studies published annually.

"For the second year in a row, financially motivated attacks outnumber cyberespionage as the main reason for breaches in manufacturing, and this year by a more significant percentage (40 percent difference)," the Verizon report's authors conclude. "If this were in most any other vertical, it would not be worth mentioning as money is the reason for the vast majority of attacks. However, manufacturing has experienced a higher level of espionage-related breaches than other verticals in the past few years."

If the goal is peak production and part making, there's little doubt that technology is playing a central role in helping companies achieve their goals. Gathering and monitoring precise machine information is becoming more critical to attaining peak performance.

Job shops are often connected to the internet, and the applications employees use, including email, websites and mobile apps, can all be the opening attackers need to get to employee and company information or intellectual property. This information could include libraries of parts specifications that an original equipment manufacturer would want out of the hands of competitors and a government would not want other nations to have.

"Manufacturers must undertake a risk assessment of their operations," says Koushik Subramanian, strategic advisor to the National Center for Cybersecurity in Manufacturing, in an ***article*** for Advanced Manufacturing. "Risk can be technical—found in machines, controls or software, and also found in personnel, practices and processes. Risk takes many different forms, but the most common is from cyberattacks where malicious individuals or groups try to break into systems by taking advantage of the weakest link: people. That's the reason phishing and ransomware are so popular and why attacks are trending higher."

For smaller shops, managing computers often means hiring outside information technology companies, aka "IT" companies, to help. For midsize and large manufacturers, it might mean some hybrid form of internal IT staffing and additional help from external companies for the more complex technology issues.

"Most of the industry is going through this awareness phase," says Livingston. "They are beginning to understand that there is a problem. But they are asking themselves: 'How do I get my arms around the world that has never really been managed as an internet-based infrastructure before?'"

Do you need a technical question answered? Ask the MSC Metalworking Tech Team in the forum.

Change Agents: Standards, State Funding and Third-Party Services

The National Institute of Standards and Technology is the body that regulates critical infrastructure and makes the rules for the aerospace and defense industries. In 2016, NIST ***published SP 800-171***, which contains the rules for "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

The standards have strict security controls included that can affect OEMs and defense subcontractors of all sizes. If a company is not in compliance, it likely won't be able to bid on the work.

"For most manufacturers who are not in critical infrastructure, losing a day of productivity because of a security issue is not a national emergency, but it hurts their bottom line," says Scott Sawyer, chief technology officer of ***Paperless Parts***. "Where this is really coming into play is intellectual property. The Department of Defense really cares about this area."

It's impacting manufacturers of all sizes.

"Even the 100-to-200-person companies are struggling with this," says Sawyer. "All of a sudden, they have to figure out how they're going to become compliant."

How are companies coping? Some that are trying to keep contracts or attract new ones with the defense industry are bringing in consultants—and they are implementing security programs. State and local economies can be adversely affected by these kinds of regulations. It can be costly. So organizations are offering funding to help companies become compliant with security standards

through manufacturing extension partnerships (MEP).

It's good news for those staying on top of the security issue, but most manufacturers are still in the dark. Especially smaller shops, explains Sawyer.

"Some have a false sense of security. They think they're not at risk because they're small and off the beaten path and their physical location is rural, they don't have a lot of employees and they keep a low marketing profile," says Sawyer. "But, you know, that's exactly in some sense what could make them a target. They are an easier target than a Lockheed Martin, Raytheon or Northrop Grumman because they don't have the security."

Those larger companies are targets, but they are also much more sophisticated about handling classified specifications and physical security, explains Sawyer. Sawyer would know—he worked in the defense industry for several years before moving into manufacturing.

Defense companies educate their employees on not talking about work when they leave the plant. Many are told to put their work badge out of sight once they leave. But even these efforts have not stopped motivated attackers from getting to important intellectual property.

"If you believe in American manufacturing, and you are patriotic, part of that should include caring about the information security piece of it," says Sawyer.

How is your shop handling security today? Are you gearing up or in "ignorance is bliss" mode? Talk about it in the forum. [registration required]

