Why Manufacturing Companies Need to Up Their Cybersecurity Game

Cybercriminals now consider manufacturing companies a target-rich environment. Learn why and what can be done to get off that list.

In order to stay competitive, manufacturing companies are replacing analog processes with digital. Some examples are networking machinery along with computers, using CAD/CAM data files, integrating machine-learning software, and let's not forget introducing Industry 4.0 devices. With the move comes increased capability and convenience, but like most things convenient, there is a cost.

Dan Hanson, in his Marsh & McLennan Agency's post "Many Owners and Managers Assume They Have No Exposure. Wrong," cautions that manufacturing companies, in particular, small and mid-size organizations, are becoming more susceptible to cyberattacks including data breaches.

"The 2016 Marsh & McLennan Agency's Cyber Survey found that 50 percent of small/midsize companies have experienced a cyber-attack," writes Hanson. "And manufacturing along with other nonfinancial, non-retail, non-technology industries are now prone to data breaches."

Looking at why, Hanson suggests:

- Manufacturing companies are increasingly warehousing data of interest to cybercriminals; and
- Primary targets (for example, banks and tech companies) have beefed up security, making manufacturing companies the new low-hanging fruit.

What's a manufacturer to do?

What are manufacturing companies up against? Team Thomas of Thomasnet.com, a supplier-discovery and product-sourcing platform, enlisted the Hackett Group to identify major risks manufacturing companies are likely to face in the coming year. Team Thomas published their results in the report The Six Biggest Risks Facing Your Manufacturing Business Today. Here's what they found:

1. Cybersecurity breaches: Manufacturing companies were not known for storing sensitive information, but that has changed in a big way, and cybercriminals are noticing. "Generally, cybercrimes on manufacturing companies are designed to either steal intellectual property (IP) or cause some kind of physical disruption to a company's operations," mentions the report. "These disruptions can result in serious material damage, leading to high repair costs and significant downtime."

Team Thomas warns that Internet of Things (IoT) devices offer cybercriminals the chance to gain access to a normally secure network, affording the attackers a "foot in the door" so to speak.

2. IP theft and industrial espionage: Intellectual property (IP) runs the gamut from product proposals to digital prints, and trade secrets to proprietary manufacturing processes. "Although it is explicitly illegal, stolen IP may be very tempting to competitors," notes Team Thomas. "Using another company's trade secrets to improve their own products and processes, shady competitors can then manufacture comparable products for a lower price point while saving money on research and development."

Companies, including manufacturers, prefer not to consider the threat from employees,—current and former. The report adds that since the crime is committed within the company, it is difficult to prosecute. Team Thomas offers the following suggestions for combating internal threats:

- Develop a multi-step plan that prioritizes the value of data, determines the most critical and sensitive aspects of the business, and applies security measures accordingly;
- Implement segmented networks that section off the most valuable data, making it accessible to only a few trusted individuals;
- Perform regular insider threat detection and prevention audits;
- Inform employees about the risk of using personal devices within the facility and educating them on best cyber practices; and
- Communicate with vendors and suppliers to ensure all links in the company's supply chain are enforcing security initiatives.

3. Disruptive innovation: The phrase disruptive innovation, championed by Clayton M. Christensen in 1995, refers to where a business identifies and exploits a market overlooked by more mainstream businesses. While this is not a cybersecurity issue, stolen IP will help a dishonest company disrupt the market quicker and more easily.

A prime example offered by Team Thomas in the Hackett Group report is the collapse of the movie rental company Blockbuster by the then startup Netflix. The report adds, "The story of Blockbuster and Netflix serves as a cautionary tale for large companies, reminding them to pay attention to their smaller competitors."

4. Lack of access to critical talent and the skills gap: The cybersecurity profession is not the only industry facing a lack of skilled workers--manufacturing is as well. "Based on data collected from company executives, current employees were lacking in key competencies such as computer use, problem-solving, and math skills," explains the report. "Without these capabilities, companies may be limited in their ability to meet customer demand, adopt new technologies, increase productivity, expand into new markets, and develop new products."
Besides not meeting the manufacturing company's needs including understanding cybersecurity practices, the lack of the key competencies described above increase the risk of employees falling for targeted attacks like phishing.

5. Regulatory issues: Manufacturing companies, regardless of size, now have the ability to reach markets across the globe--this is a good thing; however, there is the matter of regulations. "Organizations must also adhere to a wide range of industry standards and check in regularly with a number of different agencies," suggests the report. An example is the General Data Protection Regulation (GDPR) that recently became enforceable.

6. Intensified global competition: Manufacturing companies in the US do not have a lock on international access; competing companies in other countries do, as well. As global competition heats up, manufacturers will need to make sure they have all their ducks in a row. This should be a huge wake-up call where cybersecurity is concerned; not all companies are honest, and stealing trade secrets or defaming a company is not out of the question.

Looking to a more secure future for manufacturers

Team Thomas offers a final warning:
"While sophisticated technologies such as cloud computing, Artificial Intelligence, and the IoT have presented manufacturing companies with countless opportunities for growth, these advancements have also created some unique challenges and risks."

But Team Thomas is willing to end the report on a positive note:
"Although these risks pose real dangers, knowing and understanding them allows companies to hunker down and create a solid plan of action. By moving forward with an analytic approach and developing actionable, flexible strategies, companies can furnish themselves with the necessary means to secure both their present-day and future success."

By Michael Kassner @ TechRepublic.com