INNOVATION, TECHNOLOGY & SECURITY

TOP 5 CYBER SECURITY THREATS THE MANUFACTURING INDUSTRY SHOULD WATCH IN 2022

SmithAmundsen

Cyberattacks remain persistent in headlines; and yet, many companies continue to believe these will never happen to them. This mindset may be borne from believing you are too small to be of notice to threat actors or thinking you don't have the kind of data that would be attractive. Manufacturing companies may, in particular, believe they are fortified from such an attack because of the historically insular nature of the manufacturing industry and a lack of computerized connection with the outside world.

It's critical that this mindset evolve with the technology and the interconnectedness with other companies and consumers. Data a manufacturing company houses can include confidential data with business partners, sensitive data about employees and independent contractors, proprietary schematics regarding day-to-day operations and/or Operational Technology (OT) and Industrial IoT (Internet of Things). Vulnerability to cyber-attacks can also be seen in all industries in how they transfer money to their business partners.

The level of sophistication for bad actors only continues to grow and their cyberattacks have only increased in volume and intensity in the last two years. In 2019, the manufacturing sector was the 8th most targeted industry by cyberattacks. Such attacks mushroomed in 2020 due to the pandemic; and, in that same year, the manufacturing industry moved from the 8th most targeted industry by cyber attackers to second most targeted, falling below only finance and insurance. The 2021 Global Threat Intelligence Report (GTIR) indicated that this represents a 300% increase.

2022 is the perfect time to strengthen your cybersecurity practices and prevention. Here are the top 5 cyber security threats those in the manufacturing industry should know:

1. Ransomware Attacks.

This is the tried and true mode of cyberattack—one that threat actors continue to hone and one that continues to inflict a whole host of headaches for companies. Although there are many different ways for a data event to occur, ransomware continues to be the number one method of attack used by threat actors. Think of this as data "kidnapping," where your company's data will be held for ransom. Manufacturers are attractive targets because a loss of equipment usage equates to big monetary losses and potentially significant business interruption – not just for the manufacturer, but for their business and industry partners that are part of the supply chain. As a result, manufacturers are more likely to pay the ransom to be back in operation more quickly. However, in 2022, these types of attacks will likely present an additional problem: paying the attacker may be the prudent, ready-and-available solution but it may open a company up to re-extortion or a second attack. This not only leaves you vulnerable, but your reputation as well.

2. Insider Threats.

Cybersecurity threats are not only found in bad actors in foreign lands – sometimes these threats are found within the company's walls. Internal threat actors are someone within the company, or a former employee, that threatens the business based on data security infor-

About the Author: Molly Arranz is the chair of SmithAmundsen's Data Privacy & Security Practice Group. She is a certified privacy professional (CIPP-US) and a recognized Privacy Law Specialist by the American Bar Association. She can be reached at marranz@salawus.com, or (312) 894-3307. Sofia Valdivia is an associate in SmithAmundsen's Data Privacy & Security Practice Group. She can be reached at svaldivia@salawus.com, or (312) 455-3047.

mation the employee possesses. What is dangerous about insider threats is that anyone with access to the company's critical passwords can later become a threat actor. Companies that were not prepared for the new work from home shift – such as some manufacturers – were forced to make quick transitions in order to keep employees safe during the pandemic. But as a result, passwords were frequently shared, secure networks were not used, and personal devices became a potential technology solution. Ensuring that proper access and control structures are in place, for all employees, is critical. It is also vital that passwords are updated frequently and that your company keeps track of who is in possession of what information.

3. Unauthorized Access to Operational Technology.

The use of operation technology (OT) greatly benefits manufacturers' day-to-day operations. And while the use of this technology is not new, these devices have not always kept pace with the security measures needed to protect technology from outside bad actors. If a threat actor gained access to technology, it would not only halt a particular project, but it could be a potential safety concern depending on the criminal's intentions. Especially with the increased use of IoT technology – hackers would gain access to a whole host of processes related to manufacturing, including flow, light, pressure, temperature, and more. Exercising appropriate cyber-hygiene, including confirming appropriate upgrades and access controls, is important. The employment of technology, for more efficient production, will only increase, so now is the time to gain a deeper understanding of access points, security controls and incident response protocols.

4. Business Email Compromise.

There are two types of business email compromise attacks that are on the rise: social engineering, and invoice payment and fraud. In both instances, hackers pose as someone in the business in order to defraud employees, customers, partners, or vendors. Social engineering looks to impersonate internal employees and higher ups within the company, whereas invoice payment and fraud looks to redirect money straight into the hacker's bank account. With so many hands at play in the manufacturing industry, these types of attacks may find ready victims in your employee ranks. Not only can false payments be made, but intellectual property (IP) and other trade secrets that could devalue your company may fall into the wrong hands. Regular employee training and vigilance of suspicious activity in your network are critical.

5. Supply Chain Attacks.

You need to look no further than the May 2021 cyberattack on Colonial Pipeline to understand how a ransomware attack can affect those that operate in a supply chain. That attack alone shut down almost half the fuel supply chain in the Eastern United States. It was a scary example of how the impact on one link in the supply chain can cause a ripple effect on so many other organizations that are part of the process. Given that manufacturers are often integral links in the supply chain, now more than ever the industry should be vigilant.

Where do we go from here?

Lack of training and a lack of a plan can lead to panic. While threats in your industry may be imminent, preparation is key—as it can, if nothing else, lessen potential repercussions. Working with trusted advisors on creating an incident response plan and setting up appropriate and necessary safeguards can help create peace of mind and better ready your company for any level of cyber attack.