Tackling Cyber Risks in the Manufacturing Industry

As the manufacturing industry increasingly relies on advanced technology such as the industrial internet of things, automation and big data, manufacturers are particularly susceptible to cyberattacks. Manufacturing operations of all sizes are a desirable target for threat actors and thieves hoping to gain access to vast repositories of sensitive information, intellectual property and customer financial records.

Many companies now leverage artificial intelligence ("AI") to streamline production and avoid supply chain disruptions. For example, global consumer goods company, Unilever, uses AI to search for alternative ingredients in an effort to strengthen its supply chain resilience. Additionally, Walmart has begun using AI to negotiate with its suppliers. This software uses a text-user interface to negotiate with potential suppliers.

According to the IBM X-Force Threat Intelligence Index 2024, the manufacturing industry was the most targeted industry in 2023 for the third year in a row. The report notes that malware accounted for 45% of attacks, with ransomware accounting for 17% of the attacks. As the manufacturing industry is expected to remain a top target for data thieves through 2024 and beyond, companies must emphasize responsible data use, sound internal cybersecurity policies and security safeguards.

Cybersecurity and Data Privacy Concerns

Cyberattacks introduce a host of different risks and negative consequences, which includes supply chain disruptions, lost profits, loss of intellectual property and reputational damage. Some of the major cybersecurity risks that manufacturers face include:

Ransomware

Ransomware is a type of malware that blocks a data owners' access to sensitive data unless a significant amount of money is paid to an attacker. When ransomware is deployed, organizations are often forced to remove the infected systems from their network which can be time-consuming, disruptive and costly.

Phishing

Phishing attacks leverage text messaging, emails and other forms of electronic communication to deceive individuals into clicking on malicious links or divulging sensitive information. Through these attacks, attackers can obtain login credentials for company accounts that are then used to perpetrate fraud—often in the form of fraudulent payment requests to the victim company's clients. Manufacturers are susceptible to phishing attacks due to their extensive client lists and heavy reliance on third-party vendors.

Supply Chain Attacks

The supply chain is one of the most vulnerable aspects of a manufacturer's business. The supply chain allows companies to create and deliver products and materials, utilizing databases and automation to coordinate with business partners and vendors. For example, a manufacturer might incorporate a product from another manufacturer into its final product. Thus, an attack on one manufacturer could have detrimental effects on other companies as well.

There are three types of supply chain disruptions:

1. **Software Supply Chain Attacks** – Attackers will compromise only one application or piece of software to disrupt an entire supply chain. These attacks target an application's source code and deliver malicious code to a trusted app or software system.
2. **Firmware Supply Chain Attacks** – Attackers will insert malware into a computer's boot record, which can then be activated in minutes. After the targeted computer boots up, the malware is executed and the threat actor gains entry to the network. These attacks are quick, damaging and sometimes undetectable.
3. **Hardware Supply Chain Attacks** – These types of attacks depend on physical devices. Specifically, attackers may target devices critical to the manufacturing process, leading to lengthy production delays and reputational harm.

Takeaways

To effectively mitigate the possibility of a data breach, manufacturers should implement a comprehensive data protection and security program. This program should include:

- Data security measures such as encryption, network firewalls, system audits, multifactor authentication, access controls and routine system patches and updates;
- Employee cybersecurity education and training programs;
- Risk assessments and penetration testing; and
- Policies and procedures such as an information security policy, record retention policy, incident response plan and business continuity plan.

Additionally, the National Institute of Standards and Technology ("NIST") published the Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, which provides manufacturers guidance on identifying, assessing and responding to cybersecurity risks throughout their supply chain. According to NIST, many supply chain risks are associated with the lack of visibility and understanding organizations have regarding the technology used and the procedures used to ensure the "the security, resilience, reliability, safety, integrity and quality of the products and services." NIST's guidance urges manufacturers to consider and manage cybersecurity risks throughout the entire supply chain process.

Lastly, manufacturers who have government contracts should take steps to comply with the Department of Defense's ("DoD") Cybersecurity Maturity Model Certification ("CMMC") 2.0

program. The CMMC is designed to ensure that sound cybersecurity practices are in place to protect sensitive unclassified information and federal contract information that is shared by the DoD with its contractors and subcontractors.

Bond attorneys regularly assist and advise clients on data privacy and cybersecurity matters. For more information regarding data privacy matters, please contact Jessica Copeland, CIPP/US, Mario Ayoub, Victoria Okraszewski CIPP/US or any attorney in Bond's cybersecurity and data privacy practice.