Cyber Risks in the Manufacturing Industry

The cyber risk landscape is constantly evolving. There are thousands of incidents every year. Knowledge of the latest risks and threats is one of the most important tools in your cyber defense arsenal to mitigate risk. Chubb not only provides cyber coverage, but also access to risk management professionals who can provide real-time protection once a data breach, network security, or phishing event occurs. So you can focus on what matters most—staying productive.

Cyber claims reported to Chubb from manufacturing clients increased by 10 percent from 2017–2018.

In 2018, 86% of incidents reported to Chubb in the manufacturing industry were caused by someone outside the organization who had no ties to the organization.

During the past three years, the median cyber incident costs (i.e., call center, notification, crisis response, etc.) reported to Chubb by manufacturing clients climbed to nearly $400,000.

These external actions compromised servers 55% of the time and impacted individuals 33% of the time.

Why?

Cyber criminals may target manufacturers because there could be a high incentive to pay a ransom - if the factory floor shuts down, the entire operation shuts down. With the advent of robotics, artificial intelligence, and advanced manufacturing techniques, manufacturers are challenged to securely integrate older legacy systems. Complex manufacturing systems can also be hard to restore – making them appealing to the criminals who can use the length of the outage to demand higher ransoms.

Cyber risk for manufacturers continues to evolve with a higher risk for social attacks such as phishing.
Claims Scenario

A manufacturing company experienced a ransomware attack that resulted in the encryption of several of their files. After the Insured contacted our 24/7 incident response hotline, they were offered a consultation with an incident response coach and forensic experts from Chubb’s cyber panel. As a result of these discussions, the Insured chose not to pay the ransom. However, once the forensic firm began working on remediating the ransomware attack, they discovered that the Insured was also the victim of crypto-mining. Crypto-mining occurs when an unsuspecting party has coin mining (Bitcoin or other cryptocurrency) software installed into its system.

As a result of crypto-mining, the bad actor was able to secretly mine cryptocurrency at the expense of the Insured’s system. This type of surreptitious mining operation often leads to a drain on the processing power which extends to a degradation in service. In addition to the forensics firm and incident response coach, the Insured also incurred credit monitoring and notification fees, as Personally Identifiable Information (PII) was compromised in the attack.

Having a Cyber Insurance policy from Chubb enabled our client to understand the cyber damage to the fullest extent quickly and cost effectively rectifying the damage.

For the latest information on current cyber threats, including instant access to our proprietary cyber incident data on the Chubb Cyber IndexSM, visit www.chubb.com/cyber.