Legal Update Article

How Modern Manufacturing Plants Can Protect Against Ransomware, Cyberattacks

March 1, 2023

Related Services

Manufacturing
Privacy, Data and Cybersecurity

To help protect against criminal ransomware and cyberattacks, modern manufacturing plants should ensure they have reasonable physical, administrative, and technical safeguards in place.

Manufacturing plants in the 21st century utilize multiple computerized operating systems to help collect, analyze, and store data. These systems physically control much of the machinery and production in their facilities. The sophisticated interplay of these systems and components have helped drive productivity and profitability for manufacturers. But this integration has also made manufacturers more vulnerable to ransomware and cyberattacks.

According to a report by the National Association of Manufacturers, the manufacturing industry accounted for the majority of ransomware incidents in 2021. Other reports saw an increase in attacks targeting manufacturing in 2022, with up to 75 percent of attacks targeting the manufacturing sector. Another troubling statistic: more than half of affected manufacturers were not able to restore from data backups.

Anatomy of a Cyberattack Against Manufacturers

A manufacturing company, like most companies, probably would not know it has been hit by a ransomware attack until its systems, including the entire manufacturing floor, are shut down and inaccessible. In many instances, the company's entire operations grind to a halt. With modern just-in-time delivery systems the norm in manufacturing, even a shutdown of a few days can be devastating, especially where affected plants are the only source of a key part or product. The threat actors know the company will be losing significant sums of money, and risk losing customers, every day of a shutdown — and they will use this to force a ransom payment.

Even when a company pays the ransom, however, there is no guarantee the company will be able to quickly resume operations. Often, getting a manufacturer's systems up and running again can take days or weeks. Some systems may even be unrecoverable and would need to be replaced entirely.

Importance of Data Backups

Viable data backups are critical in allowing a manufacturer to quickly rebuild and resume operations following a cyberattack. Therefore, one of the first moves typically undertaken by a threat actor is to delete any on-site backups. For the best protection, manufacturers should consider offsite or cloud-based backup solutions as part of their overall data backup strategy. Offsite backups can help manufacturers quickly restore data in the event of a cyberattack.

Another important component to data backups is regular testing to ensure that backups are viable and restored systems function normally.

Legacy Systems

Some manufacturers still employ legacy systems that cannot be backed up. These might

include custom systems that were built by employees no longer with the company or by vendors that have gone out of business. These systems may run on older, unsupported operating systems or hardware. For manufacturers with such systems in place, a cyberattack can cause a complete business disruption until replacement systems can be found.

Legacy systems that cannot be backed up should be replaced or be protected with additional security measures.

Assessing Manufacturing Executive Systems

MES, or manufacturing executive systems, are the nerve center of modern manufacturing operations. The MES monitors, tracks, documents, and controls the process of manufacturing from raw materials to finished products. The data stored in the MES also may be integrated with other mission-critical systems, such as process control systems.

Important issues to consider:

- Whether all MES components are backed up as images or only certain configuration and database files
- How quickly can the MES be restored in the event of an incident
- If on-site backups are deleted or unavailable, is the MES backed up elsewhere
- Does the company have a recent disaster recovery policy, data backup policy, and incident response plan in place
- Do these policies and procedures address backup and restoration of the MES
- How often are these policies and procedures reviewed and tested

***

A company's policies and procedures can help protect against business interruption from cyberattacks. Redundant and regularly tested data backups, including offsite backups, are critical to surviving these attacks and getting up and running quickly. Threat actors know that manufacturers will be desperate to restore operations in the event of an attack — making them more likely to pay the exorbitant ransoms. Therefore, it is important to assess and identify any security gaps before experiencing a cybersecurity incident.

Jackson Lewis attorneys have in-depth knowledge of the unique issues facing manufacturers and extensive experience responding to cyberattacks and helping companies ensure they have adequate physical, administrative, and technical safeguards in place. Contact a Jackson Lewis attorney for more information.