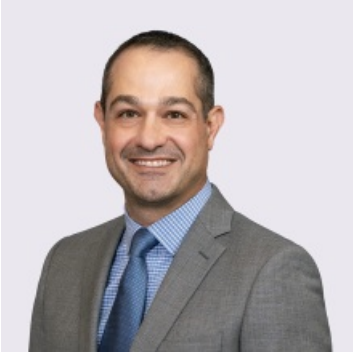
Legal Update Article

Dealing with the Growing Threat of Cyberattacks in Manufacturing Sector: What Employers Need to Know

By Jason C. Gavejian, Andrew D. Kinghorn & Nicholas B. McGrath

August 15, 2023

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Andrew D. Kinghorn
Principal
Andrew.Kinghorn@jacksonlewis.com

Nicholas B. McGrath

For the second year in a row, the manufacturing industry has fallen victim to more cyberattacks than any other major business sector.

Indeed, according to IBM Security's X-Force Threat Intelligence Index, nearly 25 percent of all cyberattacks in 2022 were carried out against manufacturers. While this figure of documented attacks is disturbing, there is reason to believe these incidents are underreported. Manufacturers are not subject to certain compliance reporting requirements governing other industries and often are not legally required to disclose data breaches. Whatever the actual number, cybercriminals are clearly targeting the manufacturing industry.

Ransomware attacks (the digital equivalent of kidnapping) represent the most prevalent cybersecurity threat in the manufacturing space. Ransomware is a malicious software designed to infiltrate an organization's systems and encrypt critical files and information. When the ransomware takes hold and the organization realizes it has been locked out of its own systems, the attacker demands a ransom in exchange for the decryption key. Again, IBM Security identified manufacturing as the sector most extorted through ransomware in 2022, accounting for more attacks than those in the energy, finance, healthcare, retail, education, and transportation industries.

The disproportionate number of ransomware attacks against manufacturers seems driven by the necessity and complexity of their operations. Given their integral role in the global supply chain and the prevalence of "just in time" inventory levels and delivery expectations, manufacturers typically have little-to-no tolerance for downtime. However, regaining access to systems and information following a cyberattack can be a costly and time-consuming undertaking. In some cases, the malware may permeate production systems and force manufacturers to take their physical systems off-line as a precautionary measure. For these reasons, extortion is a lucrative strategy for cybercriminals who understand that organizations may be more willing to pay ransom demands than to tolerate an extended operational disruption while they seek to reboot and regain access to their systems.

In addition to ransomware, infiltration of operational technology and the theft of data (even after the restart of systems after the attack), intellectual property, and confidential information can be extremely damaging from an operational, financial, and reputational perspective. As the manufacturing industry grows more dependent on the latest technological advancements (*e.g.,* advanced automation, artificial intelligence, and blockchain technologies), the potential consequences of a cyberattack become even more pronounced.

Associate
402-827-4249
Nicholas.McGrath@jacksonlewis.com

Related Services

Manufacturing
Privacy, Data and Cybersecurity

It is critical that businesses invest in strong cybersecurity and take steps to mitigate their vulnerability to cyberthreats. Manufacturers should develop secure backups and establish business continuity and disaster recovery plans to use in the event of an attack. Companies may also consider investing in cyber insurance to help cover the costs of investigating, remediating, and responding to cyberattacks. In addition to these contingency plans, employers should take preventive measures by conducting regular security audits, routinely updating and patching systems, and utilizing multi-factor authentication processes. Most importantly, it is crucial for companies to educate and train personnel on an ongoing basis regarding the nature of cyberthreats, the consequences of a breach, and employees' role in defending against these threats (*e.g.,* phishing recognition and best practices for housing sensitive data).

The legal landscape surrounding cybersecurity and data privacy laws is complicated and vary widely depending on the jurisdiction, industry, and the type of data at issue. Jackson Lewis attorneys in the Manufacturing Industry group, in conjunction with the Privacy, Data and Cybersecurity Practice group, regularly assist employers navigating these issues and can help identify and implement appropriate cybersecurity measures, as well as coordinate a response in the event of a cyberattack.

Please contact a Jackson Lewis attorney with any questions.

©2023 Jackson Lewis P.C. This material is provided for informational purposes only. It is not intended to constitute legal advice nor does it create a client-lawyer relationship between Jackson Lewis and any recipient. Recipients should consult with counsel before taking any actions based on the information contained within this material. This material may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome.

Focused on employment and labor law since 1958, Jackson Lewis P.C.'s 1,000+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged and stable, and share our clients' goals to emphasize belonging and respect for the contributions of every employee. For more information, visit https://www.jacksonlewis.com.