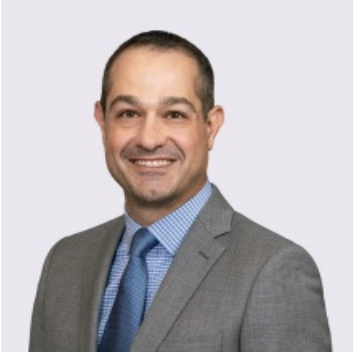
Legal Update Article

Modernization of Manufacturers: Safety and Cybersecurity Issues

By Jason C. Gavejian, Kymiya St. Pierre &

May 11, 2022

Meet the Authors



Jason C. Gavejian

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

Kymiya St. Pierre

(Kim-mee-UH • She/Her)
Principal
(949) 885-1360
Kymiya.St.Pierre@jacksonlewis.com

Related Services

Manufacturing
Privacy, Data and Cybersecurity
Workplace Safety and Health

Like many other industries, manufacturing has been hit hard with labor shortages. As of April 2022, U.S. factory activity reportedly is at its slowest pace in more than 18 months. Consequently, many factories seek more agility from artificial intelligence and other automated processes to better manage disruptions and uncertainty. With these modernizations comes the threat of potential safety and health hazards and cyber threats.

Occupational Safety and Health Administration

Increased automation may reduce some hazards and increase efficiencies, but technological advancements that employ computer-based controls of hazardous energy also may conflict with the Occupational Safety and Health Administration's (OSHA) existing standard for the Control of Hazardous Energy (Lockout/Tagout) (LOTO). The use of robotics also may introduce other hazards into the work environment. In 2019, OSHA issued a Request for Information (RFI) on the Control of Hazardous Energy (Lockout/Tagout) and overall use of robotics for more information from stakeholders about the increased efficiencies, and potential hazards, associated with robotics (84 Fed. Reg. 22756). OSHA's RFI demonstrates the recognition that robotic modernization can create new hazards that are not easily addressed through its current LOTO standard. OSHA's notice of proposed rulemaking to amend the LOTO standard is targeted for September 2022, but it could take years to complete. While manufacturers wait for updated guidance, service and maintenance of automated equipment should be performed in accordance with OSHA's existing LOTO standard until they are modernized.

It is important that manufacturers continue to assess the interaction between equipment and employees and stay informed on federal- and state-specific safety regulations by partnering with counsel on current health and safety regulations.

Cybersecurity

In addition to safety issues, modernization brings with it an increase in vulnerability to cyberattacks. According to Identity Theft Center's report on Q1 of 2022, manufacturing was a top-three targeted industry for cyberattacks. As manufacturers embrace modern technologies, this change opens these organizations to ransomware and data theft vulnerabilities in ways that were simply unavailable in the analog days. Part of this issue is likely due to organizations prioritizing innovations over the cybersecurity needed to protect the new technology. Reportedly, according to Cybersecurity Ventures, phishing attempts rose 200 percent in 2020, the amount held for ransom increased from $5,000 in 2018 to $200,000 in 2020, and experts estimated that an attempted ransomware attack occurred every 11 seconds in 2021. The Department of Homeland Security has warned organizations to be on high alert for a possible cyberattack as the war in Ukraine escalates. As recently as March 2022, the *Texas Tribune* reported that Russian hackers

had been probing Texas' energy infrastructure.

Manufacturers can prepare against cyber threats. Manufacturers should ensure they continuously invest in cybersecurity strategies to fit their needs, including partnering with counsel to develop strategies to address the interplay of business needs, data protection, and legal risks. As an initial step, organizations can develop and practice an incident response plan before a breach occurs. Steps include the following:

- Identify the internal response team (*e.g.,* leadership, IT, in-house counsel, and HR). These are the persons in the business who will direct the response to any data incident. They will make quick, informed, and prudent decisions that likely will be critical to the success of the response process and, possibly, the future of the business.

- Identify the external response team (*e.g.,* outside legal counsel, forensic investigators, notification vendors, and public relations). Having external members of the team identified ahead of time and negotiating/agreeing to any applicable contracts can be vital to the success of any preparedness plan. When a breach happens, valuable time can be lost trying to identify, evaluate, negotiate with, and engage third-party service providers necessary for the response.

- Anticipate critical business continuity and worksite safety issues that could be jeopardized by a compromise to information and control systems. To the extent possible, contingency plans should be laid out to enable continued operations while investigating the incident and mitigating harm.

- Consult with insurance brokers or cyber-insurance carriers to confirm applicable coverage or to discuss coverage options for cyberattacks. If coverage exists, notifying the insurance carrier should be one of the organization's first steps in response to an incident.

- Take into account all legal and contractual obligations that may affect the response process.

- Clarify the roles and responsibilities of the team members at key points in the response process: discovering the incident, investigation, coordination with law enforcement, remediation, notification, third-party inquiries, compliance, and reevaluation. This should include a well-defined decision-making process to facilitate good choices and avoid delays.

- Practice, practice, practice. It is likely that members added to the response team do not have first-hand experience with helping to coordinate a data incident investigation or response. Unfortunately, even a well-drafted plan does not give persons charged with implementing the plan proficiency in executing it. Once the organization creates its plan, it should gather its internal and external breach response team members to simulate an incident to help members gain valuable experience navigating investigation, mitigation, and overall response process, as well as working with each other. Just like a fire drill, practicing this process will help ensure any data incident is addressed in an efficient and orderly fashion.

It is also important that organizations create awareness of the risk of cyberattacks and of cybersecurity risks. This can include the following:

- Educate employees on how to recognize and avoid potential ransomware attacks and other forms of data breach.
- Instruct employees on what to do immediately if they believe an attack has occurred (*e.g.,* who to notify (generally, IT) and how to disconnect from the network). This may include coordinating with the organization's worksite safety team to ensure, for example, compromised systems and equipment do not cause physical harm to individuals or property damage.
- Instruct employees on what *not* to do (*e.g.,* delete system files and attempt to restore the system to an earlier date).

Preparedness can make all the difference in the success of an organization's ability to handle a cyberattack. An incident prevention and response plan is only as strong as employee awareness. Employees must understand the risks involved in maintaining complex data-driven systems and equipment and the basic steps they can take to prevent or mitigate a cyberattack and, if needed, respond to one.

***

As manufacturers modernize to adapt to the changing workplace, they should work with experienced attorneys in their jurisdiction to ensure they are poised to handle the challenges these technologies bring, from OSHA compliance concerns to cybersecurity. Contact a Jackson Lewis attorney if you have any questions about how to address these evolving issues.