FOLEY

FOLEY & LARDNER LLP

CYMANII the cybersecurity manufacturing innovation institute

SECURE TOGETHER

Recommendations for Managing Cybersecurity Threats in the Manufacturing Sector

SEPTEMBER 2023

FOLEY.COM

CYMANII.ORG

In the hyper-connected era of smart manufacturing, accelerated by "Industry 4.0," the manufacturing sector is undergoing a digital revolution. By leveraging technologies such as advanced automation, artificial intelligence, the Internet of Things (IoT), blockchain, and the like, manufacturers continue to optimize production, increase efficiency, and drive innovation. However, this digital revolution brings with it complex cybersecurity risks and threats, creating significant implications for manufacturers.

For the second year in a row, manufacturing has been the most targeted sector by cyberattacks, accounting for nearly one in four incidents.[1] Throughout 2022 alone, ransomware attacks on the manufacturing industry nearly doubled, accounting for 72% of all ransomware attacks and implicating 104 unique manufacturing subsectors.[2]

As manufacturers increasingly integrate digital information technology (IT) with physical operational technology (OT), the vulnerabilities that cybercriminals can exploit continue to multiply exponentially. Accordingly, while cybersecurity has always been an essential aspect of manufacturing, the increasing reliance on technology now makes it one of the industry's most critical concerns. Below we describe various types of cybersecurity risks and attacks faced by manufacturers and outline some of the legal implications and considerations that entities in the manufacturing sector should consider.

1 *See* "X-Force Threat Intelligence Index 2023," IBM Security. (February 2023). Retrieved from https://www.ibm.com/downloads/cas/DB4GL8YM; last visited June 1, 2023.

2 *See* "ICS/OT Cybersecurity Year in Review 2022 - Executive Summary," Dragos. (n.d.). Retrieved from https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Exec-Summary-2022.pdf?hsLang=en; last visited June 1, 2023.

AUTHORS

Howard Grimes
Chief Executive Officer,
Cybersecurity Manufacturing Innovation Institute

Aaron Tantleff
Partner,
Foley & Lardner LLP

Alex Misakian
Associate,
Foley & Lardner LLP

Cybercriminals continue to target the manufacturing sector due to its integral role in the economy, potential critical industry and supply chain impacts, and vast amounts of sensitive data held by organizations within the sector. Cyberattacks may disrupt businesses and supply chains, undermining the benefits of digitalization and resulting in financial and productivity losses causing reputational damages.

It is also important to understand the international landscape and its direct impact on U.S. manufacturers. State-sponsored cyber actors are enlarging their threat vectors in both capabilities and active intentional use in supply chains.[3] China's laws and policies support the active use of human intelligence to gather information regarding supply chains.[4] Recently, Chinese advanced persistent threat (APT) supply chain attacks were used to steal data from companies.[5] These attacks were initiated by APT41[6] (also known as Barium, Winnti, Wicked Panda, and Wicked Spider).

Russian state-sponsored cyber actors also have demonstrated capabilities to compromise IT, OT, and industrial control systems (ICS) networks by using mechanisms that maintain long-term, persistent access.[7] This access allows exfiltration of sensitive data from IT/OT networks by deploying destructive malware to disrupt critical industrial control systems and operational technology functions.[8] The intent is to disrupt U.S. manufacturing capabilities and productivity.[9]

3 *See* https://www.fbi.gov/investigate/counterintelligence/the-china-threat; last visited September 13, 2023.

4 *See* https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-071223; last visited September 13, 2023 and https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf; last visited September 13, 2023.

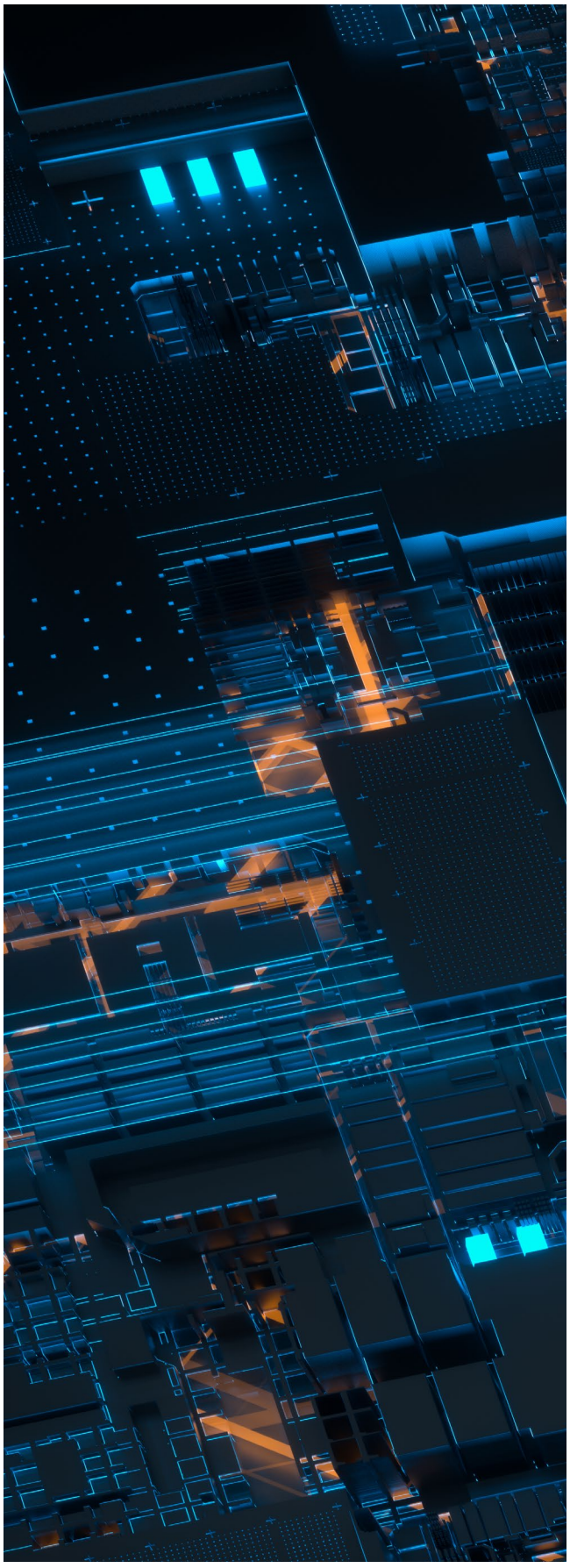
5 *See* https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china; last visited September 13, 2023 and https://www.fbi.gov/investigate/counterintelligence/the-china-threat; last visited September 13, 2023.

6 *See* https://krebsonsecurity.com/2020/09/chinese-antivirus-firm-was-part-of-apt41-supply-chain-attack/; last visited September 13, 2023.

7 *See* https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-071223; last visited September 13, 2023.

8 *See* https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china; last visited September 13, 2023.

9 *See* https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china; last visited September 13, 2023.



Additionally, the volume of cyber vulnerabilities in U.S. systems continues to increase dramatically.[10] Adversaries now have greater freedom and political support within their home countries, and financial support from adversarial governments to deliberately introduce vulnerabilities into critical infrastructure in the United States and other countries.[11] The "Triton," "Dragonfly," and "Havex" operations sponsored by Russia against multiple energy infrastructures demonstrate this approach.[12] These cyberattacks resulted in malware being installed on more than 17,000 devices in the United States and abroad, including ICS/supervisory control and data acquisition controllers used by power and energy companies.[13] Importantly, Robert M. Lee, CEO of Dragos, described Triton's infiltration into the safety system of a large petrochemical refinery as "the only reason to sabotage [cyber safety systems] is to kill people."[14]

These vulnerabilities, whether native or inserted, are typically operationalized in legacy systems that were not designed to be secure, further increasing the vulnerability of critical infrastructure supply chains.[15]

These cybersecurity risks can be broadly categorized into malware attacks, social engineering attacks, and APTs, in addition to other risks unique to the manufacturing sector.

10 *See* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

11 *See* https://www.fbi.gov/investigate/counterintelligence/the-china-threat and https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

12 *See* https://www.securityweek.com/us-charges-russian-hackers-over-infamous-triton-havex-cyberattacks-energy-sector/.

13 *See* https://www.securityweek.com/us-charges-russian-hackers-over-infamous-triton-havex-cyberattacks-energy-sector; last visited September 13, 2023.

14 *See* https://www.washingtonpost.com/world/national-security/theyre-on-the-lookout-for-malware-that-can-kill/2018/04/27/33190738-32c1-11e8-8abc-22a366b72f2d_story.html.

15 *See* https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

Types of Cybersecurity Risks Facing the Manufacturing Sector

Malware attacks involve the deployment of malicious software, may come in many forms — including viruses, worms, ransomware, and spyware — and constitute a significant threat to manufacturers as they can cripple an entire manufacturing operation, causing significant financial, operational, and reputational damage. This category of software is designed to infiltrate, damage, or disrupt systems. The most common malware affecting manufacturing is ransomware, which may involve the encryption and/or exfiltration of a victim's data and a ransom payment demand. Ransomware is especially dangerous for a manufacturer as it can halt production lines, disrupt operations, cause considerable financial loss, and significantly impact the global supply chain.

Social engineering attacks exploit human vulnerabilities rather than technological flaws to gain unauthorized access to systems and data, potentially leading to ransomware attacks or sensitive data theft. While phishing is a well-known form, social engineering attacks may involve spear phishing (targeted at specific individuals or companies), baiting (enticing a user to perform an action with a false promise such as a free gift), and pretexting (creating a fabricated scenario to manipulate the victim into providing access or information).

Advanced persistent threats are sophisticated, coordinated attacks that often target high-value industries like manufacturing. These attacks are typically conducted by highly skilled groups with substantial resources, intent on stealing sensitive information or disrupting critical infrastructure. In the manufacturing sector, APTs often target valuable intellectual property (IP) such as proprietary production techniques, research and development data, or business strategy documents. In addition to IP theft, APTs can cause significant operational disruption as prolonged, unauthorized access to a manufacturer's network may allow attackers to manipulate industrial control systems, disrupt production processes, or even sabotage equipment. APTs can also compromise supply chains. A successful attack on a manufacturer could give the attacker access to connected networks such as suppliers, logistics partners, or customers. This potential for wide-ranging impact makes APTs a grave concern for the entire manufacturing ecosystem.

IP theft is one of the most coveted manufacturing targets for cybercriminals and is often the most prevalent target of APTs. Manufacturers often possess valuable proprietary information, including blueprints, manufacturing processes, and research and development data. Accordingly, sophisticated cybercriminal groups or state-sponsored entities may utilize APTs, among other cyberattack tools, to target and exfiltrate IP. IP theft, including encrypted files, is being retained by foreign governments for future decryption using new technologies.[16] Given the value of proprietary information such as unique manufacturing methods, product designs, and research data, the impact of such theft on a manufacturing company can be immense, leading to potential market share loss, decreased competitive advantage, and substantial financial repercussions.

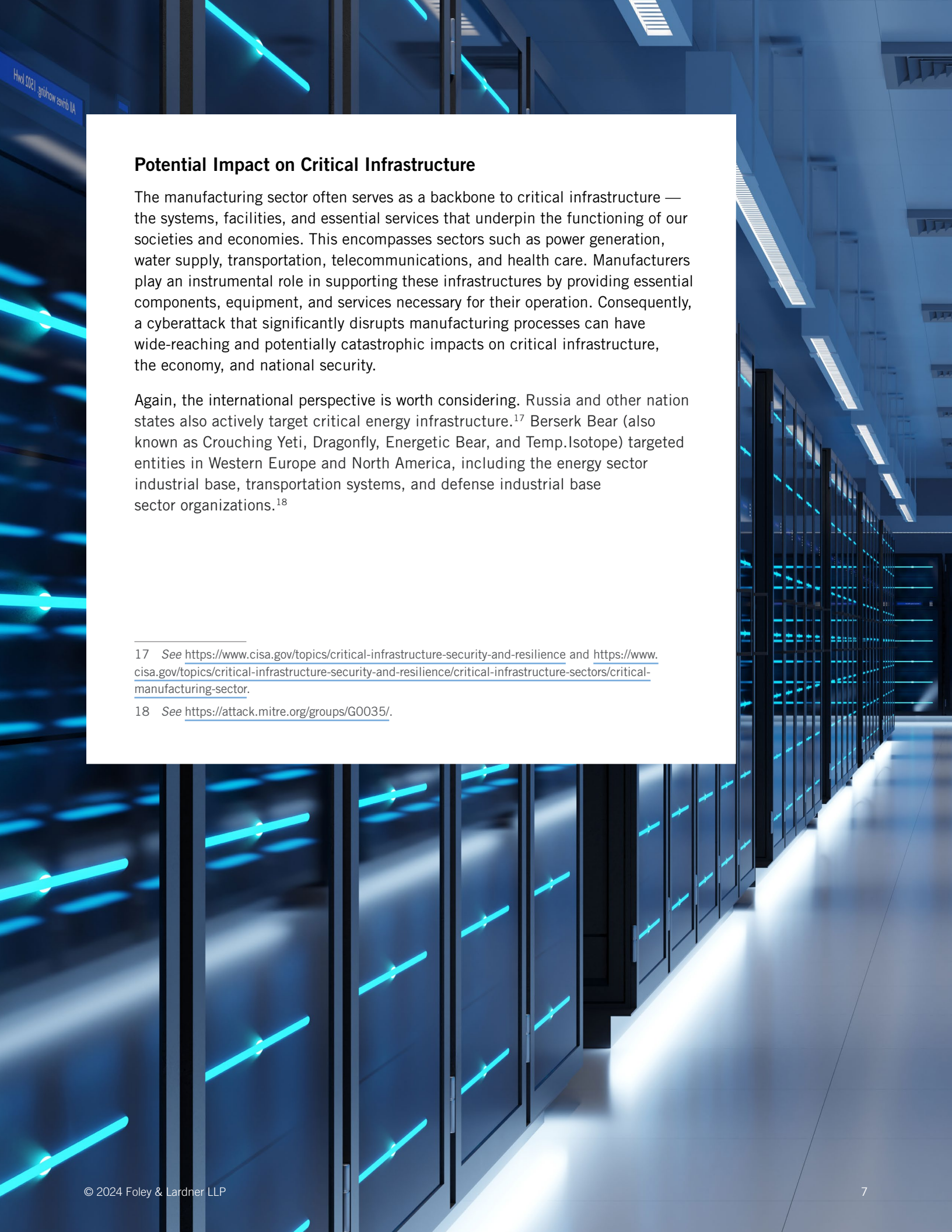
16 *See* https://www.fbi.gov/news/testimony/threats-to-the-homeland-111722 and https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

Supply chain attacks, often resulting from APTs, exploit the vulnerabilities in a company's supply chain network. Given the interconnected nature of the manufacturing industry, a single vulnerability can have far-reaching implications. Attackers can exploit weaker links, such as small suppliers with less robust security, to infiltrate larger, more secure networks. Notably, the 2020 SolarWinds hack, which affected government and corporate networks, was a supply chain attack. Avoiding this type of attack requires a design and build process that is both secure and defensible.

Industrial control system attacks, also often stemming from APTs, target ICSs crucial for modern manufacturing processes and can potentially give the attacker control over production processes. Such an attack can halt production, cause physical damage, or even result in safety incidents. Stuxnet, a malicious computer worm discovered in 2010, targeted ICSs in Iran's nuclear facilities, highlighting the potential real-world implications of such attacks.

Insider threats from disgruntled employees, contractors, or other insiders with access to critical systems can prove just as dangerous cybersecurity risks as threats from outside the organization. As with other types of cyberthreats, insider threats pose a significant risk of IP theft. Notably, not all insider threats are intentional. While insiders might misuse their access intentionally, their credentials can also be co-opted through phishing or other methods, allowing an external attacker to infiltrate systems.

Third-party vulnerabilities involve cybersecurity risks that result from a manufacturer's relationships with vendors, suppliers, service providers, or any third parties that have access to their systems or data. In other words, a manufacturer's cybersecurity resilience is often only as strong as the weakest link in its supply chain. A third party lacking robust cybersecurity measures can become an initial vector for cybersecurity attacks.



Potential Impact on Critical Infrastructure

The manufacturing sector often serves as a backbone to critical infrastructure — the systems, facilities, and essential services that underpin the functioning of our societies and economies. This encompasses sectors such as power generation, water supply, transportation, telecommunications, and health care. Manufacturers play an instrumental role in supporting these infrastructures by providing essential components, equipment, and services necessary for their operation. Consequently, a cyberattack that significantly disrupts manufacturing processes can have wide-reaching and potentially catastrophic impacts on critical infrastructure, the economy, and national security.

Again, the international perspective is worth considering. Russia and other nation states also actively target critical energy infrastructure.[17] Berserk Bear (also known as Crouching Yeti, Dragonfly, Energetic Bear, and Temp.Isotope) targeted entities in Western Europe and North America, including the energy sector industrial base, transportation systems, and defense industrial base sector organizations.[18]

17 *See* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience and https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector.

18 *See* https://attack.mitre.org/groups/G0035/.

Energy. A cyberattack on manufacturers in the energy sector — including those that provide parts for power plants, oil refineries, and wind turbines — could result in widespread power outages, leaving homes, businesses, and public services without electricity. This could affect thousands, if not millions, of individuals and cause significant economic damage. At an extreme, it could even have national security implications as energy grids could be left vulnerable to additional attacks.

Transportation. Similarly, in the transportation sector, a successful cyberattack on manufacturers of automobile, aircraft, and train components could disrupt the availability of these parts and impact production. The cascading effect of such disruptions could lead to reduced transportation capabilities, major disruptions to the supply chain, and the availability of vehicles or goods, significantly impacting the mobility of goods and people and potentially even impacting military readiness if defense-related transportation is affected.

Telecommunications. In telecommunications, manufacturers produce everything from networking equipment to mobile devices. A disruption in manufacturing these products could have a ripple effect, causing communication blackouts that affect businesses, government agencies, and individuals. Such an event could severely disrupt daily operations across multiple sectors and hinder emergency response efforts.

Health care and pharmaceuticals. When it comes to health care and pharmaceuticals, cyberattacks can have particularly dire consequences. For example, an attack on medical device or pharmaceutical manufacturers could result in medication production shutdowns, compromised medical device functionality, or altering the formulation of life-saving drugs. In the worst-case scenario, this could have severe repercussions on patient safety and public health.

National security. Cybersecurity attacks on any of the critical infrastructure sectors noted above may have major national security implications, particularly if the targeted manufacturing company is involved in producing defense equipment or technology. A cyberattack on manufacturers supplying the defense sector could interrupt the production of essential military equipment, impairing a nation's defense capabilities, or result in a nation's enemies gaining access to the IP underlying critical defense technology. Similarly, disruptions in the energy or telecommunications sectors could compromise key national capabilities and intelligence operations.

Overall, the potential impact of cyberattacks on critical infrastructure underscores the urgent need for robust cybersecurity measures within the manufacturing sector. The interconnectedness of today's world means that a cyberattack on a single manufacturing company can ripple outward to affect a broad array of unrelated sectors. Moreover, these attacks can undermine the public's trust in critical services, causing societal instability. Given the potential scale of disruption and associated economic, health, safety, and national security risks, manufacturers must adopt a proactive approach to cybersecurity. Cybersecurity in the manufacturing sector is not merely an issue of business continuity; it is a matter of national and international security.

Legal Implications and Potential Liabilities

The legal implications of these cybersecurity attacks are vast, including significant financial and legal liabilities from various sources.

First, manufacturers may face liability based on data protection laws if a cybersecurity attack involves a personal data breach. For example, if a manufacturing company controls large amounts of personal data, including customer or employee data, it would be subject to data protection laws such as the General Data Protection Regulation (GDPR) in the European Union, the California Privacy Rights Act (CPRA), and other comprehensive state data privacy laws in the United States, as well as cybersecurity requirements imposed by the federal government under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), the Defense Federal Acquisition Regulation Supplement (DFARS), and the Federal Energy Regulatory Commission (FERC), and other industry-specific regulations. A data breach that exposes or results from non-compliance with data protection laws could result in significant regulatory fines and penalties. For instance, the GDPR imposes significant financial penalties for non-compliance, up to 4% of annual global turnover or €20 million, whichever is higher. Additionally, manufacturers may face considerable liability arising from class actions filed by affected individuals. Similarly, noncompliance with federal requirements such as CIRCIA can result in sanctions, fines, or outright shutdown.

Second, directors and officers of manufacturing companies could face legal action from shareholders based on an alleged breach of fiduciary duties. Such duties include the duty of care, which could be interpreted as an obligation to implement reasonable cybersecurity measures in the context of cybersecurity. If a cybersecurity attack results in significant financial loss, and the shareholders can show that directors and officers failed to implement adequate cybersecurity measures, they could be held liable for breaching the duty of care. Similarly, if a cybersecurity attack results from a failure to properly vet and monitor a supplier or other third-party's cybersecurity policies and procedures, manufacturers may face potential claims alleging a breach of the required duty of care. Shareholders may also file lawsuits alleging that negligence of the directors and officers resulted in financial loss.

Third, if a cybersecurity attack involves the loss or disclosure of IP, especially in the case of industrial espionage, a company may be found to be in violation of trade secret laws or be subject to IP lawsuits if the cybersecurity attack results in the theft and subsequent disclosure and/or unauthorized use of proprietary information.

Finally, under contract law, manufacturers could be held liable for breach of contract if a cybersecurity attack disrupts their ability to fulfill contractual obligations. Additionally, contracts often contain clauses related to required data protection and cybersecurity. This could lead to various legal consequences, including termination of contracts and liability for any resulting damages.

Recommendations

Given the multitude of cybersecurity risks and significant legal implications, manufacturers must adopt *and comply with* robust cybersecurity measures and policies, including technical and legal measures.

Technical measures. These include implementing multi-factor authentication, utilizing modern endpoint detection solutions, ensuring comprehensive business continuity and backup procedures, regularly updating and patching systems, conducting regular security audits, and training employees on cybersecurity best practices. Technical measures are the first line of defense against cybersecurity risks. Manufacturers should review their cybersecurity policies and procedures and ensure proper technical security measures are implemented and followed. In addition, new approaches that cybersecure critical supply chains and manufacturing processes are in development.[19] Manufacturers should be aware of these innovations and work to deploy them as quickly as possible.

Employee training and awareness. Employees often represent the most significant, and most difficult to manage, vulnerability in an organization's cybersecurity defenses. As such, regular employee training and awareness campaigns are crucial. Training should educate employees about the nature of cyberthreats, the importance of cybersecurity measures, and their role in defending against them. Topics can include the importance of strong, unique passwords; the risks of phishing attacks; and the correct procedures for handling, storing, and sharing sensitive data. This training, especially focused on OT/ICS manufacturing systems is available through the Cybersecurity Manufacturing Innovation Institute (CyManII).

Legal measures. Manufacturers can also protect themselves by incorporating appropriate and compliant cybersecurity clauses into their contracts. For example, to mitigate the risks associated with third-party vulnerabilities, these clauses should specify third parties' responsibilities regarding cybersecurity, including data protection obligations, required security measures, and the procedure for responding to cybersecurity incidents. Manufacturers should also ensure they conduct thorough cybersecurity audits of their third parties. These audits should assess the third parties' cybersecurity policies, procedures, infrastructure, and compliance with relevant regulations. These clauses and audits protect manufacturers legally and incentivize third parties to uphold high cybersecurity standards and limit liability in the event of a cybersecurity attack.

Cyber insurance. Manufacturers also should invest in cyber insurance to mitigate financial risks associated with cyberattacks, including the costs to investigate, remediate, and respond to such attacks, negotiations and ransom payments, and potential litigation that may arise. Additionally, manufacturers should strive to comply with applicable cybersecurity standards such as ISO 27001 and the National Institute of Standards and Technology Cybersecurity Framework as these standards provide guidelines and best practices for managing cybersecurity risks. Achieving and maintaining these certifications can demonstrate that the company has taken reasonable steps to protect against cyberthreats.

19 *See* https://cymanii.org/.

Consider collaborating with legal counsel. Manufacturers face not only a multitude of cybersecurity risks but must also navigate the complex patchwork of cybersecurity and data privacy laws at state, federal, international, and industry-specific levels. These often complicated laws can vary widely depending on the jurisdiction, industry, and the type of data a company handles. Legal counsel can identify the applicability and ensure compliance with international, federal, and state data privacy laws, cybersecurity requirements imposed by the federal government, and other industry-specific regulations.

Legal counsel also can help identify potential liabilities and legal risks related to cybersecurity. Such steps may include facilitating risk assessments, developing risk management strategies, drafting policies and procedures to mitigate cybersecurity risks, and preparing and executing an appropriate incident response plan following a cybersecurity incident to ensure compliance with applicable data breach privacy laws. Legal counsel can also assist in reviewing and revising contracts with suppliers, service providers, and customers to ensure the inclusion of appropriate cybersecurity requirements and protections such as indemnification clauses or limitations of liability in the event of a cybersecurity incident. Finally, legal counsel involved and well versed in a manufacturer's cybersecurity practices and procedures can more effectively assist in the event of litigation, whether from affected individuals, business partners, or regulators.

Managing cybersecurity risks requires a comprehensive, multi-faceted approach combining robust technical measures, strong legal protections, and a commitment to employee training and awareness. By implementing these measures, manufacturers can significantly reduce their cybersecurity risks and protect themselves from potential legal liabilities.

CONCLUSION

While offering significant advantages, the digital revolution in the manufacturing industry has exposed the sector to elevated cybersecurity risks. As cyberthreats grow more sophisticated, manufacturers must navigate a complex legal landscape, balancing technologically supported growth with compliance with data protection laws, potential liability for cyberbreaches, and the need for robust cybersecurity defenses.

In this rapidly evolving context, proactive risk management and adherence to cybersecurity standards are not merely best practices but strategic imperatives. Manufacturers should continually revisit their cybersecurity strategies, aligning them with the latest technological advancements and regulatory updates. Fostering a strong cybersecurity culture will not only mitigate legal liabilities but will also contribute to the long-term resilience and competitiveness of the manufacturing sector.

ABOUT US

Foley & Lardner LLP

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 26 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

Cybersecurity Manufacturing Innovation Institute (CyManII)

CyManII was launched in 2020 by the Department of Energy, as part of the greater Manufacturing USA Network, designated as a Clean Energy Manufacturing Institute to work across the manufacturing industry, research and academic institutions, and federal government agencies to develop technologies that enable the security and growth of the U.S. manufacturing sector. Simultaneously, CyManII is continuing its collaborative research to design and implement architectures of the next-generation that are cyber-inspired and secure by design. CyManII is housed at the University of Texas at San Antonio.

FOLEY

FOLEY & LARDNER LLP

CYMANII the cybersecurity manufacturing innovation institute

FOLEY.COM

CYMANII.ORG

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Advanced Manufacturing Office Award Number DE-EE0009046. The views expressed herein do not necessarily represent the views of the U.S. Department of Energy or the United States Government.