Published on *The National Law Review* https://natlawreview.com

So, You Think of Cybersecurity Only as a Cost Center? Think Again.

Article By:

Aaron K. Tantleff

Alexander Misakian

Introduction: Basis of the Current Risk Profile – "How Did We Get Here?"

U.S. manufacturers face a multitude of cybersecurity challenges that threaten their operations, reduce productivity, and jeopardize their intellectual property and data. For the past two years, the manufacturing sector has been the most targeted industry for ransomware attacks,[1] with manufacturers spending an average of US$1.82 million per attack in 2023, not including any ransom payments.[2]

These cybersecurity challenges and risks are exacerbated by the simple reality that manufacturing operations often rely on various intertwined systems not designed with cybersecurity in mind. Retrofitting those systems can be both costly and complex. But manufacturers with more modern systems do not escape the risks. Although the rapid integration of technology and connectivity in manufacturing operations has brought unprecedented levels of innovation and efficiency, it also exponentially expands the cyberattack surface area and creates new categories of vulnerabilities.

Equally problematic is the increased sophistication, frequency, and cost of responding to cyber attacks. According to a recent study by cybersecurity firm Sophos, 56% of manufacturing survey respondents experienced a ransomware attack between January and March of 2023.[3] Of those, only one in four companies thwarted the attacks before their data was fully encrypted, and over a third resorted to paying ransom in an effort to recover data.[4] Moreover, in 32% of these attacks, the cybercriminals not only encrypted the data but also stole it.[5]

To navigate the spectrum of cybersecurity challenges, U.S. manufacturers must adopt a holistic approach to safeguarding their operations and data and moving toward a system that protects the company and helps drive profitability. In this paper, we first outline five key cybersecurity challenges facing manufacturers, identify ways to manage those risks, and describe the legal and insurance considerations for manufacturers in addressing these issues. Next, we propose new approaches that have the potential to usher in a new era of smart, secure manufacturing that converts cybersecurity from a cost center to a value-driven profit center. In the final section, we describe the power of public-private partnerships in addressing cybersecurity challenges.

I. Navigating the Complex Terrain of Cybersecurity Challenges

Creating a holistic approach to safeguarding operations and protecting data requires considering numerous cybersecurity challenges inherent in manufacturing operations. Without minimizing the importance of others unique to a particular manufacturer, here are five key everyday challenges.

1. The Proliferation of Industrial Internet of Things (IIoT)

The first challenge stems from the growing adoption of the Industrial Internet of Things (IIoT). Although these IIoT devices and automation systems enhance productivity and efficiency, they are often inadequately secured and expand the attack surface for cybercriminals and nation-state adversaries. Vulnerabilities in a single device can trigger a cascading effect, resulting in infiltration of an entire manufacturing network, disrupting operations, data breaches, and even physical harm to human workers.

2. A Shortage of Skilled Cybersecurity Professionals

The shortage of skilled cybersecurity professionals in the manufacturing sector is a significant corporate concern that can escalate into a national security challenge. Manufacturers need experts who understand both the intricacies of industrial processes and how to secure these processes. Without these experts, companies can fall victim to various attack vectors, resulting in economic losses and productivity decreases. At a national level, nation-state adversaries actively seek cyber vulnerabilities that can be exploited to cripple critical U.S. manufacturing capabilities.

3. Supply Chain Vulnerabilities

Supply chain vulnerabilities pose a grave threat to U.S. manufacturers and the global economy. The interwoven global supply chain networks that sustain manufacturing operations enable cybercriminals the ability to target and exploit the weakest, least secured links in the supply chain. In 2023, we saw significant growth in cyberattacks targeting the supply chain, particularly attacks on third-party software, hardware, and services.[6]

By targeting smaller organizations with less robust cybersecurity infrastructure, cybercriminals can then leverage the compromised third party to gain access and compromise the systems of the manufacturers supplied by those entities. Any weak link in the supply chain can lead to the introduction of malicious code or backdoors into products or the compromise of entire network systems. As a result, manufacturers must exercise increased diligence when selecting external partners to work with, necessitating more stringent compliance verifications to vet the cyber tools used by these prospective partners.

4. Bridging the IT-OT Gap

Another vulnerability can result from the convergence of information technology (IT) and operations technology (OT) and the potential for miscommunications between differing security cultures. IT focuses on data integrity and confidentiality, while OT emphasizes safety and reliability. Merging these domains without proper alignment and communication can lead to confusion, misconfigurations, and vulnerabilities that cybercriminals can exploit.

5. Constantly Evolving Cyber Threat Landscape

Cybercriminals are increasingly well-funded and resourced by nation-states interested in disrupting not just our manufacturers but the global economy. They also employ an evolving battery of threats that range from traditional malware to zero-day exploits and ransomware attacks. As cybercriminals continue to evolve and target the manufacturing sector, manufacturers should expect even more nuanced attacks that reduce manufacturing productivity and harm manufacturers' infrastructure and employees. Manufacturers must proactively stay ahead of this by adopting preventative measures and implementing next-generation Secure Defensible Architectures and other technologies discussed later in this article.

U.S. manufacturers face a complex and rapidly evolving cybersecurity landscape. The integration of IIoT, supply chain vulnerabilities, the shortage of trained professionals, IT-OT convergence, and a myriad of protocols (and vendors offering "solutions") all contribute to this challenge. While individual companies bear the risk and cost of cybersecurity, the aggregation of the collective risk to U.S. manufacturers can pose a significant threat to both the U.S. and global economies.

II. Managing Cyber Risks Today

Manufacturers need to adopt an integrated, multi-faceted approach to mitigate cybersecurity risks. This new approach must evolve more rapidly, be more agile than adversaries, and introduce innovations that provide verifiable security guarantees of physical processes. In the era where digital and physical worlds connect, securing manufacturing processes and data is of paramount importance to ensure the global competitiveness and resilience of the U.S. manufacturing sector.

Manufacturers should not allow themselves a false sense of security. For example, the term "Secure Architecture" can be misleading as it:

- Connotes a conjoining of perimeter defense + data security
- Often involves inadequate security controls that are applied only to a limited aspect of operations or a supply chain
- Provides little or no consideration for real-world physical consequences; and
- Is often aligned solely with compliance requirements.

Currently, many effective tools already exist. However, they primarily focus on preventing intruders from accessing the network – with the perimeter defense accomplished by implementing robust security measures. These measures include firewalls, intrusion detection and prevention systems, secure access control, and air gapping. By controlling access to the network, manufacturers can reduce the likelihood of a breach. In addition, investing in employee cybersecurity training and awareness further reduces risk, as the human element represents the single biggest cybersecurity risk. Employees are often the first line of defense against cyber threats, so training them on recognizing phishing emails, social engineering attempts, and the risks associated with portable devices such as thumb drives is crucial.

Regular software updates are crucial. These updates often secure against known vulnerabilities that have recently been exposed. Recently, the Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory confirming that threat actors generally target older software vulnerabilities because they are often low-cost and impactful ways to compromise a target.[7] Commonly, these vulnerabilities are old, with patches available for years. Manufacturers are acutely aware that outdated software harbors thousands of cyber vulnerabilities that cybercriminals can exploit. By maintaining up-to-date software across the entire system, manufacturers can close

potential entry points for the attackers. However, patching alone is not always enough; organizations need to apply suggested detection techniques for continuous monitoring. In some cases, attackers can reverse- engineer the updates and find ways to work around the released patches with new exploit variants,[8]emphasizing the need for organizations to continuously monitor their networks and systems.

As a result, collaboration with third-party vendors and suppliers can also mitigate risk. A recently launched Manufacturing Information Sharing and Analysis Center (ISAC) (https://www.mfgisac.org/) is a valuable source of public information on the latest cyber threats. ISAC provides critical information to assist manufacturers to secure and protect their own systems. Manufacturers also can use the ISAC information to hold their suppliers to higher cybersecurity standards, dramatically lowering the likelihood of supply chain attack risks. The United States has also funded organizations charged with securing U.S. manufacturers, including the Cybersecurity Manufacturing Innovation Institute (CyManII).

In addition, manufacturers must remain cyber-aware and familiarize themselves with the various tools and security frameworks, such as the National Institute of Standards and Technology (NIST), U.S. Department of Defense (DoD), U.S. Department of Energy (DOE), National Security Agency (NSA), and Federal Bureau of Investigation (FBI), and CISA documents. These organizations provide information on “hot” cyber threats and how to mitigate them proactively. Manufacturers should also establish an incident response plan and prepare how to respond, including how to report the incident and to whom.

A manufacturer can stay a step ahead in the ongoing cybersecurity war by deploying advanced threat detection and response mechanisms. For example, intrusion detection systems continuously monitor network traffic for suspicious patterns while advanced analytics and machine learning help identify anomalies that often can indicate an ongoing cyber-attack. Such systems, coupled with comprehensive and well-trained rapid incident response plans, further minimize damage in the event of a suspected breach.

Unfortunately, these precautions alone may still be insufficient to protect manufacturers. It is crucial to remember the underlying problem: the systems used were not designed with security in mind. While the available “bolt-on” approaches discussed above can help strengthen security and protect against cyberattacks, they can only do so much. Manufacturers must evolve and implement new, innovative strategies to secure U.S. manufacturers, sustain and grow the economy, and remain globally competitive.

III Legal Implication, Obligations, and Liabilities

In addition to the cybersecurity risks outlined above, manufacturers should understand the various legal obligations and implications, including potentially significant financial and legal liabilities.

1. Current Legislation and Legal Obligations

In response to the increasing cybersecurity threats, the United States has introduced various legislation and executive actions to enhance the protection of critical infrastructure. At the federal level, these include, but are not limited to:

The Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018: This act established CISA as the lead federal agency responsible for securing critical infrastructure. CISA’s functions and

role encompass:

- **Rapid Deployment:** CISA's responsibility includes swiftly deploying resources and support to affected entities to mitigate ongoing cyber threats.
- **Incident Analysis:** CISA will analyze reported incidents to identify patterns and trends, enhancing the ability to respond effectively to emerging threats.
- **Threat Intelligence Sharing:** CISA will facilitate efficient threat intelligence sharing among entities, fostering a collective cybersecurity defense posture.

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA): Signed into law in March 2022, CIRCIA mandates that critical infrastructure companies, including those in the critical manufacturing sector, report material cybersecurity incidents and ransomware payments to CISA within 72 and 24 hours, respectively.

The U.S. Securities and Exchange Commission (SEC): In March 2022, the SEC proposed a rule requiring publicly listed companies to report cybersecurity incidents, their cybersecurity capabilities, and their board's cybersecurity expertise and oversight.

Defense Federal Acquisition Regulation Supplement (DFARS): Manufacturers contracting with the DoD must comply with DFARS, which imposes specific cybersecurity requirements on contractors. This includes safeguarding controlled unclassified information (CUI) and complying with the NIST Special Publication 800-171 standards. Failure to meet these requirements can result in contract termination and legal consequences.

Federal Energy Regulatory Commission (FERC): FERC establishes cybersecurity standards for the energy sector to protect the nation's critical energy infrastructure. Compliance with FERC regulations is essential for energy-related manufacturers and utilities. Failure to comply can result in penalties, loss of licenses, and damage to the reliability of the energy grid.

Compliance with reporting requirements imposed by legislation like CIRCIA and FERC is critical.

Failure to meet these requirements can result in substantial penalties and legal repercussions. While CISA has until March of 2024 to develop and finalize the regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA,[9] proactive information sharing during the rulemaking period is encouraged. Accordingly, entities in the 16 critical infrastructure sectors defined by CISA, including those in the critical manufacturing sector, and all registrants with the SEC must consider and prepare to report incidents to the appropriate authorities and comply with the applicable regulations.

Emerging State Legislation: Several states, including Colorado, Florida, Maryland, and New York, are actively working on legislation related to critical infrastructure cybersecurity. While these bills have not yet been passed, it is likely only a matter of time before they become law.[10]

These legislative measures aim to improve information sharing, develop cybersecurity standards, and enhance public-private partnerships to protect critical infrastructure. However, covered entities must begin to prepare for and ensure compliance in the event of a cyber incident.

2. Potential Legal Liabilities

Manufacturers face various legal liabilities in the event of a cybersecurity incident and should

consider these issues as part of their response to an incident.

Data Protection Laws: If a cybersecurity attack involves a personal data breach, manufacturers may face liability based on data protection laws. 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. Non-compliance with these laws can lead to significant regulatory fines and penalties, which can be as high as 4% of annual global turnover or €20 million under the GDPR. Additionally, manufacturers may face considerable liability arising from class actions filed by affected individuals. Similarly, non-compliance with federal requirements such as CIRCIA can result in sanctions, fines, or outright shutdown.

Director and Officer Liability: Directors and officers of manufacturing companies owe fiduciary duties to shareholders and could face legal claims for an alleged breach of fiduciary duties. For example, a director or officer's duty of care may be interpreted as an obligation to implement reasonable cybersecurity measures. If a cybersecurity attack results in significant financial loss, directors and officers 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 also may file lawsuits alleging that the negligence of the directors and officers in addressing cybersecurity risks resulted in financial loss.

Intellectual Property (IP) Implications: Cybersecurity incidents involving IP loss or disclosure, particularly in industrial espionage cases, can lead to costly legal liabilities.

Contractual Obligations: Manufacturers could be held liable for breach of contract if a cybersecurity attack disrupts their ability to fulfill contractual obligations. Contracts often contain clauses related to required data protection and cybersecurity, and failure to meet these contractual obligations can lead to various legal consequences.

3. Cyber Insurance Considerations

Combating the increase in cyber threats and compliance with the growing legal requirements can be costly. Cyber insurance plays a crucial role in mitigating financial risks associated with cyber threats. Manufacturers should carefully consider the various aspects of cyber insurance. These policies typically consist of two main components:

- First-Party Coverage: This aspect of the policy addresses the direct costs incurred by the manufacturer as a result of a cyber incident. It includes coverage for data breach response, business interruption, and data restoration expenses. For example, if a ransomware attack disrupts operations, the business interruption coverage may help compensate for lost revenue during the downtime.
- Third-Party Coverage: Third-party coverage deals with liability issues arising from a cyber incident. It encompasses protection against legal costs, such as those associated with defending against lawsuits due to data breaches, privacy violations, and intellectual property theft. Manufacturers may also be covered for regulatory fines and penalties.

Determining the appropriate level and scope of cyber insurance coverage begins with a comprehensive risk assessment. Manufacturers should assess potential financial losses, legal

liabilities, regulatory compliance costs, and reputation damage to tailor insurance coverage to specific needs and risk tolerance appropriately.

IV. Proactively Addressing Cyber Risks

True cyber secure status requires more than costly, never-ending “bolt-on” applications. Manufacturers must collaborate with cyber and legal experts to develop “Secure Defensible Architectures” with the following features:

- The implementation of Digital Engineering Lifecycle[11] across the entire supply chain;
- Consideration of every operation, machine, and person as a “node” in this digital design to seamlessly integrate the supply chain with operations;
- Capturing every node in a cyber-physical identity (passport) that provides:
    - Guarantees of physical functions;
    - Linkage of security to product quality and energy/emissions efficiency (embodied energy); and
- Verifiable security properties that are extensible to multiple domains.

As part of the Secure Defensible Architectures, manufacturers must develop a Cyber-Physical Passport that ensures all supply chains are “born qualified” and “rooted in trust.”

Thus, an integrated and bold approach that *converts cybersecurity from a cost center to a profit center*.

The profit from cybersecurity investments is returned via (a) verifying the integrity and quality of products as a sales advantage and (b) optimizing energy efficiency and emissions reduction at the facility and supply chain network levels. Cybersecurity moves from an endless investment with no verifiable outcomes to an investment strategy that leads to verifiable security guarantees of physical processes and products while increasing quality and integrity and decreasing energy usage and emissions.

An additional factor must be considered – cyber vulnerability detection and mitigation. In the rapidly evolving landscape of cyber threats, addressing cyber weaknesses, enumerations, and vulnerabilities is critical to mitigating cyber risks. A cyber weakness refers to a flaw or susceptibility in a system’s design or implementation. These weaknesses can emerge due to coding errors, misconfigurations, inadequate security controls, or human mistakes. Enumerations involve systematically probing a target system to gather information about its architecture, services, and potential entry points. Cyber vulnerabilities are gaps in a system’s security that can be exploited to gain unauthorized access, disrupt operations, or steal data. These vulnerabilities can arise from software bugs, outdated software, or weak authentication mechanisms.

Currently, manufacturers chase cyber vulnerabilities by “patching” these in software updates. However, given the vast, ever-growing number of vulnerabilities, many consider this approach too expensive and non-scalable. Instead, manufacturers must develop comprehensive lists of cyber weaknesses (where each weakness reflects thousands to millions of vulnerabilities), categorize, enumerate them, and then develop dedicated attack annexes to guide mitigation strategies. Organizations like MITRE, with input from CyManII and many companies, have developed a comprehensive list of cyber weaknesses (https://cwe.mitre.org/), and CyManII is developing manufacturing attack annexes to enable U.S. manufacturers to address weaknesses (and vulnerabilities) growing at an unprecedented scale.

An additional challenge is the lack of managed security service provider (MSSP) expertise in the current state of small to medium-sized manufacturers (SMM). Often, SMMs outsource their security, believing that their cyber needs are adequately addressed, only to discover this isn't the case when facing a ransomware note. Many MSSPs overstate their abilities and visibility into critical functions of an SMM while also understaffing their operations due to a lack of workforce and profit margins. CyManII recommends that SMMs attempt to self-heal through mutual aid solutions and proper tooling rather than simply rely upon a third party. CyManII is developing generative AI for this and the correct implementation of security controls associated with early proper response to an attempted intrusion. Combining this approach with attack annexes against entire categories of Common Weakness Enumerations (CWEs) is groundbreaking. We may be at the crossroads of taking cybersecurity from unwieldy adolescence into maturity.

We must also equip manufacturers with a cyber- aware workforce. To do that, we must develop and implement training at a massive scale. CyManII has developed an extensive manufacturing-focused OT-ICS curriculum delivered in-person, virtually, and online. Using this approach and working with several partners (SME ToolingU, Cyber Readiness Institute, etc.),

we are rapidly approaching 1 million workers being upskilled in cybersecurity. Adding this skill set to U.S. manufacturers leads to more cyber-secure operations while minimizing downtime and production issues arising from cyber-attacks.

V. The Power of Public-Private Partnerships in Addressing Cyber Threats in Manufacturing

The manufacturing industry stands at the crossroads of technological advancement and escalating cybersecurity risks. In this digital era, Public-Private Partnerships (PPPs) emerge as a formidable force in addressing and mitigating the cyber threats that U.S. manufacturers face (and are a critical portion of CIRCIA compliance). PPPs forge collaborations, cooperation, and contracts between government, private companies, and cybersecurity experts.

This synergy harnesses the strength of each sector to collectively bolster the defenses against cyber threats. By pooling resources, knowledge, and expertise, PPPs develop comprehensive and integrated strategies that introduce new innovations into the market.

Manufacturers benefit from PPPs through access to real-time threat information, guidance on best practices, and the implementation of industry-wide standards. Most critically, PPPs engage companies in researching, developing, and deploying new cyber innovations into their manufacturing operations and facilities, allowing manufacturers to better protect against evolving vulnerabilities.

Cybersecurity is a team sport, and PPPs enable the strongest teams to work together – or perhaps "Secure.TOGETHER." In an era where cyber threats can disrupt operations, compromise proprietary data, impact national security, and threaten our economy, PPPs offer a robust defense mechanism. Uniting the public and private sectors is vital, as these PPPs are the lynchpin in fortifying the manufacturing industry's cyber resilience and ensuring sustained growth in our digital world.

Howard Grimes, Chief Executive Officer, Cybersecurity Manufacturing Innovation Institute, also contributed to this article.

Footnotes:

1 “X-Force Threat Intelligence Index 2023,” IBM Security, February 2023.

2 “The State of Ransomware in Manufacturing and Production 2023,” Sophos, June 2023 (14-country survey of manufacturers with 100-5,000 employees).

3 Id.

4 Id.

5 Id.

6 “Q2 2023 Threat Landscape Report: All Roads Lead to Supply Chain Infiltrations,” Kroll, 2023.

7 “CISA, NSA, FBI and International Partners Issue Advisory on the Top Routinely Exploited Vulnerabilities in 2022,” National Security Agency/Central Security Service, August 03, 2023. Available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3481350/cisa-nsa-fbi-and-international- partners-issue-advisory-on-the-top-routinely-exp/.

8 “Finding Something New About CVE-2022-1388,” VulnCheck, April 13, 2023. Available at: https://vulncheck.com/blog/new-Cve-2022-1388

9 CISA is required to publish a Notice of Proposed Rulemaking (NPRM) within 24 months of CIRCIA’s enactment – making the NPRM deadline March 2024.

10 “Cybersecurity Legislation 2022,” National Conference of State Legislature, July 22, 2022. Available at: https://www.ncsl.org/ technology-and-communication/cybersecurity-legislation-2022

11 Digital Engineering Lifecycle refers to the end-to-end process of developing and managing digital products or systems. It encompasses various stages from conceptualization to retirement and includes activities such as design, simulation, prototyping, testing, deployment, and maintenance. Essentially, it’s a comprehensive framework that leverages digital technologies and tools to streamline and enhance traditional engineering processes.

National Law Review, Volume XIII, Number 320