By Surya Kommareddy
and Swapan Ghosh

IS CYBER-SECURITY THE WEAKEST LINK IN YOUR SUPPLY CHAIN?

Increasingly interconnected supply chains empowered by Internet of Things technologies are producing vast new quantities of data, but also new vulnerabilities to cyber attack. In this new environment, manufacturing companies need to dramatically up their game on mitigating cyber risks.

MANUFACTURERS WILL NOT BE ABLE TO FULLY REALIZE the benefits of digital transformation without first addressing cybersecurity. The Industrial Internet of Things (IIoT) is redefining industrial manufacturing, enabling Industry 4.0 (I4R). Emerging technologies such as the IIoT, artificial intelligence (AI), machine learning (ML), and blockchain (all in the cloud) are redefining industrial supply chain management (SCM). However, with an increasing focus on IIoT-enabled supply chains, and the large repositories of sensitive data they provide, manufacturing assets and supply chains have now become a lucrative target for cyber attacks. While manufacturers can reap the many benefits of digital supply chains, it is imperative now more than ever that they pay attention to the growing concerns of cybersecurity.

Surya Kommareddy, *Director, Discrete Manufacturing, Oracle Corporation*

Swapan Ghosh, *Director, Discrete Manufacturing, Oracle Corporation*

However, according to Gartner, industrial managers are not paying enough attention to IIoT security, as they are not prioritizing these initiatives (Figure 1). This article will dive into the cybersecurity challenges and vulnerabilities in digital supply chains, review cybersecurity frameworks, and recommend holistic approaches to mitigate those risks.

Impact of Cyber Attacks

Typically, the motivation of a hacker is to sabotage operations, steal intellectual property, personal or financial data, or to extract ransom by unlocking encrypted data. When it comes to manufacturing supply chains, the implications are much broader. Cyberattacks from malicious hackers or software can paralyze entire connected manufacturing ecosystems, affecting production, product qualities, revenues, brand, and human lives.

Cybersecurity breaches can have costly effects that linger many years after an incident. The 2016 cyber risk in advanced manufacturing report from Deloitte said that, of the companies that experienced breaches, 38 percent lost between $1 million and $10 million. Apart from the better-known cyber incident costs of attorney and litigation fees, post-breach customer protection, technical investigation, and cybersecurity improvements, there are many additional hidden costs associated with an attack. The hidden costs may actually run much higher than the better-known, surface incident costs.

Cybersecurity Attack Vectors

Whatever the motivation, the hacker first finds a vulnerability and then exploits it to penetrate the digital enterprise to begin hacking. In a manufacturing company, critical infrastructure management functions are related to either operational technology (OT) systems, such as industrial control systems (ICS), or IT systems, such as Enterprise Resource Planning or SCM. With the expansion of I4R technologies, communications and interoperability between OT and IT systems have drastically increased, leading to potential vulnerability and risks to the manufacturing systems.

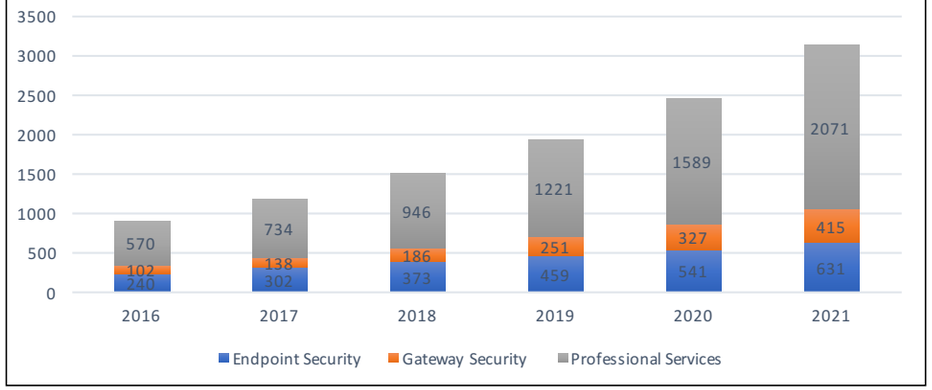
With increased numbers of touch-points all along the supply chain, cyberattacks can now be launched in a handful of pathways (vectors). The most obvious ones are the wireless and wired communication channels, which are LAN, WAN, Wi-Fi, Bluetooth connections, or point-to-point serial connections. Cyberattacks can also be launched locally if the attackers have direct access to a computer or device within the corporate network. Viruses can also be spread through seemingly innocuous networked devices such as thermostats, sensors, appliances, or even printers. While malware risks through email attachments are well known, a more recent risk is to embed software or hardware malware into genuine products delivered by legitimate vendors to penetrate and attack critical systems throughout the supply chain.

In the case of a Russian gas company cyberattack (1982)[1], the intruders knew the vulnerability and exploited the weakness in the "logic bomb" which caused significant damage to the Trans-Siberian pipeline. The largest such attack, named "WannaCry", happened in April 2017 and infected over 230,000 computers. Nissan Motor Manufacturing (UK) and Renault[2] had to halt production to stop the spread of the ransomware. Thus, one potential security risk could cause serious physical and economic losses to industrial manufacturing companies.

Manufacturing Plant Vulnerability

Most manufacturing plants operate with staff who lack adequate networking, IT, and cybersecurity expertise. Even if a manufacturer has well-qualified IT staff, they may not be familiar with all of the capabilities,

FIGURE 1:
Worldwide IoT Security Spending Forecast
(Millions of Dollars)



(Gartner, 2018)

[1] Reed, T (2004). At the Abyss: An Insider's History of the Cold War. New York: Ballantine Books, page:102

[2] https://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5

Security breaches can have costly effects that linger many years after an incident, including many hidden costs.

the industrial protocols, and communication of smart devices used in the plants.

Most manufacturing capital equipment, if maintained well, could run for several decades. As a result, many plants have legacy equipment whose firmware, software, and ICS are no longer supported by their suppliers. For example, many ICS may still be running on legacy Windows 95 operating systems or another legacy OS that can no longer be upgraded or patched. Manufacturers would like to continue to use their capital investments as long as they produce good quality product, irrespective of the orphaned control or software systems which make them very vulnerable to cyberattacks when networked. These legacy machines were not built with security in mind as connectivity was not as widespread at the time. In spite of the layered architecture of modern ICS, security management processes are not seamlessly applied to ICS/SCADA systems as they are applied to IT systems.

Earlier, ICS environments were isolated from the outside world by a closed and trusted network. The ICS were operated securely by air-gapping concepts which ensured physical isolation of systems that were using legacy hardware, control protocols, and non-routable network addresses. However, due to the adoption of Industry 4.0 initiatives, more and more operational systems are connected to enterprise business systems, creating more potentially vulnerable entry points for both systems.

Digital Supply Chain Vulnerability

The complexity of globally distributed, physical supply chains was already high, and the addition of digital supply chains has brought a whole new level of complexity and risk. Digital supply chains have enabled deeper connectivity and communication among suppliers, manufacturers, distributors, and customers. Hyper-connectivity has increased the touchpoints and exposed the risk of IP and business data hacks across the whole digital supply chain.

The potential risk of cybersecurity has exacerbated given that most suppliers, manufacturers, and partners that participate in digital supply chains may not have well-coordinated technology development and adoption plans, which can lead to disparities and vulnerabilities. Even though a manufacturer may have a well-thought out cybersecurity plan, it may fail, as the hardware or software products from supplier's may have cybersecurity vulnerabilities that could be exploited. Not only that, a suppliers' network could be compromised to get a handle on sensitive business and IP data of the manufacturer.

With a higher risk of cyber attacks on modern digital supply chains, manufacturers should extend risk mitigation beyond their enterprise to the complete supply chain.

Many manufacturers take the if it ain't broke, don't fix it approach when it comes to adopting new technology. However, just as manufacturers undertake preventive measures around maintenance of equipment, cybersecurity should also be a proactive measure. Most manufacturers may not be aware of their existing vulnerabilities. It could be too late and too costly to patch a vulnerability after someone else has discovered and exploited it.

Manufacturers should be continually assessing existing policies, and applying the latest measures to strengthen the cybersecurity of their supply chain operations. Manufacturers should include cybersecurity as one of the key items in their supply chain risk mitigation plans. There are several resources that can be leveraged to accomplish the risk assessment.

To mitigate the security challenges in digital SCM, industry standards organizations such as the Industrial Internet Consortium (IIC) and the National Institute of Standards and Technology (NIST) have developed security maturity models and security-based best practices for IoT and industrial manufacturing. The IIC SMM guides a manufacturing company to understand its current security maturity and helps in developing a target maturity such that, based on a gap analysis, the company can develop security programs to meet business objectives. The NIST cybersecurity framework is based on a generic cybersecurity framework with special guidance for the manufacturing industry. However, the NIST framework gives detailed cybersecurity implementation guidelines for manufacturing companies specifically. The following sections briefly describe the model and framework.

FIGURE 2:
Security & Risk Assessment (Gap Analysis)

With a higher risk of cyber attacks on modern digital supply chains, manufacturers should extend risk mitigation beyond their enterprise to the complete supply chain.

Cybersecurity is more about people, policies, and processes than technology. C-suite executives should make cybersecurity a top company priority.

TABLE 1:
Cybersecurity Framework Functions and Categories

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

IIC IoT Security Maturity Model

The IIC IoT security maturity model[3] provides a guideline regarding the current maturity of an organization and how it should invest in security mechanisms to meet desired objectives. The security maturity level is a measure of the understanding of the current security level, its benefits, and costs. The maturity model is based on the Plan-Do-Check-Act (PDCA) cycle for a specific system. Initially, a target security maturity for a specific system is established, then the security improvement processes are started and, as security threats and processes change, the cycle is repeated again based on the requirements.

The IIC SMM has three stages: Dimensions, Domains and Practices. The dimension is the high-level view of the security priorities of the organization, where domains are the specific means to obtain those priorities and practices are specific activities associated with domains. The IIC SMM has three dimensions: Governance, Enablement and Hardening. Each dimension has domains and each domain has associated security practices. For example, Security Governance Dimension (to facilitate legal, regulatory and contractual compliances) has Security Program Management and Compliance Management Practice.

There are five comprehensive levels (0: None, 1: Minimum, 2: Ad-hoc, 3: Consistent and 4: Formalized) and three scope levels (1: General, 2: Industry, and 3: System). Based on these levels, the current security maturity and target maturity (as desired by the organization) at dimension, domain, and practice levels are determined for a particular scope of the organization. After that, a gap analysis is performed and phased security action plans are generated for implementation. A sample gap analysis is presented in Table 2.

NIST's Cybersecurity Framework

NIST has developed a cybersecurity framework[4] for the manufacturing industry. The framework has five core functions: Identify, Protect, Detect, Respond and Recover. The core functions and categories are presented in Table 1.

The framework has defined a manufacturing profile to implement cybersecurity controls in manufacturing environments and systems. For each critical security category in a manufacturing profile, sub categories are defined and for each category/subcategory, three levels of security profiles (Low, Medium and High) are identified for the manufacturers. The security profiles are based on the impact of any cybersecurity event including injury, financial loss, environmental impact, production interruptions, and public image loss for the organization.

For example, in Table 2, for the Identity function in Asset Management (ID.AM) category, two subcategories -- manufacturing systems components (ID.AM1) and manufacturing system software (ID.AM2) -- are defined and guidance have been provided for low, medium and high security profiles. The framework provides a detailed guideline for each function including its categories and subcategories. Manufacturing organizations may adopt this framework for monitoring and managing cybersecurity risks proactively.

Tackling Supply Chain Cybersecurity

Supply chains today span the globe. With countries regulating cybersecurity and privacy differently, it is challenging for companies to manage a comprehensive cybersecurity policy within the company and across its supply chain.

TABLE 2:
Manufacturing Profile Subcategory Guidance

Function	Category	Subcategory	Manufacturing Profile
Identity	Asset Management (ID.AM)	ID.AM-1	Low
			Document an inventory of manufacturing system components that reflects the current system
			Moderate
			Identify individuals who are both responsible and accountable for administering manufacturing system components
			High
			Employ automated mechanism to detect the unauthorized hardware and firmware components within the system
		ID.AM2	Low
			Document an inventory of manufacturing system components that reflects the current system
			Moderate
			Update the inventory of manufacturing system software as an integral part of component installations, removals and systems update. Identify individuals who are both responsible and accountable for administering manufacturing system software
			High
			Employ automated mechanism where safe and feasible to detect the presence of unauthorized software within the system

[3] https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf

[4] https://doi.org/10.6028/NIST.IR.8183

Cybersecurity in supply chains should be tackled holistically. In this age of hyper-connected products, security doesn't end with enforcing internal IT and OT policies; it has to span the vendors of each and every physical asset and enterprise software product.

SANS Institute, a provider of cybersecurity training and certification, advises that companies establish a supplier/vendor risk management program and retain the right to audit and test the cybersecurity controls of vendors, suppliers, and other service providers. NIST proposes other best practices, such as including security requirements in every RFP and contract, ensuring security handshakes between software and hardware, and imposing "One strike and you are out" policies on vendor products that do not match specifications.

Cybersecurity technologies are constantly evolving just as other IT technologies are. Attackers are getting smarter and often find vulnerabilities before the threat prevention vendors and software do. The challenge is in finding the right set of products and solutions that will provide the adequate security across prevention, detection, and resolution. Seventy-five percent of security budgets are historically spent on prevention. Gartner[5] recommends that customers focus more on a "Continuous Response" model where more time, energy, and budget are spent on detection and response.

Implementing cybersecurity is akin to implementing Star Wars-like impenetrable barriers and robots. Recently, enterprise software companies have introduced AI-driven security and risk management solution tools. The new purpose-built AI and ML-based security and risk management tools offer constant protection from threats. The tools adaptively tackle security incidents and keep records of the different methods that are used to resolve threats.

Modern cloud-based enterprise software solutions also provide greater security measures in terms of multi-factor authentication and identity management, customer data isolation, instant upgrades and patches to software, and greater availability through redundancy, handing over most security management responsibility to a trusted service provider.

In many cases, cybersecurity is more about people, policies, and processes than technology. C-suite executives should make cybersecurity a top company priority. When a SCM organization is hit by a cyber-attack, customers, as well as an antiquated SCM process, could take the brunt, requiring years to recover.

Because of the evolving nature of threats, organizations cannot completely eliminate risks but they can have better insight into how their end-to-end SCM service may be affected by a cyber attack. By undertaking a sound cybersecurity policy, manufacturers can ensure that cybersecurity is no longer their weakest link. M

[5] https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/security-architecture-into-your-organization/

Engineering culture will feel awkward at first integrating a data-driven approach, but engineers respond well to results.