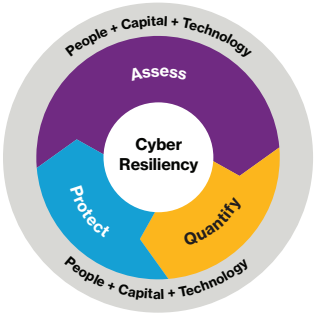

Decode industry.

Global cybersecurity risks in the manufacturing industry: Addressing systemic risk and capitalizing on the benefits of next generation technology

by Norma M. Krayem, Sr. Policy Advisor and Global Chair, Cybersecurity & Privacy Policy and Regulatory Team, Holland & Knight

Cybersecurity as a systemic risk

Manufacturing has long been a foundational part of the global economy and a leader in technological innovation. In a world dominated by a focus on the Fourth Industrial Revolution, and what has been called Industry 4.0, manufacturers have increasingly adopted robotics, artificial intelligence, machine learning and advanced analytics. As we consider the current and future view of Industry 4.0, attention is turning to what the future of "connected everything" means.

Recently, for example, the G20 Leaders met in Osaka, Japan on June 28-29, 2019 and focused on that next generation view: Society 5.0, which was defined as a "human centered society that achieves a high integration of cyberspace (virtual space) and physical space (real space), coming after the hunting society (Society 1.0), agricultural society (Society 2.0), industrial society (Society 3.0), and information society (Society 4.0). In such a society, new technologies have various transformative impacts on the way society works, such as the formulation of optimal value chains; the promotion of sustainable industrialization by automated manufacturing; increased production of crops by automating the agricultural work; and extending healthy life expectancy and reducing the social cost of ill health and aging through preventative examinations and nursing care robots; to name a few."[1]

As automation becomes more integrated in society, cybersecurity risk has become an increased imperative for manufacturing, one of 16 critical infrastructure (CI) sectors[2], which specifically underpin the U.S. economy and economies around the globe. While the term "smart" manufacturing is used constantly, "smart and secure" must become the new

> **"The future battlespace is constructed of not only ships, tanks, missiles, and satellites, but also algorithms, networks, and sensor grids. Like no other time in history, future wars will be fought on civilian and military infrastructures of satellite systems, electric power grids, communications networks, and transportation systems, and within human networks. Both of these battlefields – electronic and human – are susceptible to manipulation by adversary algorithms."** Cortney Weinbaum and Lt Gen John N.T. "Jack" Shanahan, "Intelligence in a Data-Driven Age," (Joint Force Quarterly 90, 2018)

moniker as cyber risk can no longer be ignored. The NotPeya and WannaCry global cybersecurity attacks demonstrated the debilitating, cross cutting nature of cyberattacks, as they hit every sector. Manufacturing was not spared.

The 2013 White House Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," help set the stage as a "call to arms" to rally the private sector, and specifically the manufacturing sector. Manufacturing sits at the constellation of a host of other CI sectors including energy, health, the defense industrial base (DIB), transportation, autonomous vehicles (cars, trucks, drones, planes), water/wastewater, satellites, communications, chemical and food/agriculture. Each is essential to the economic and national security of nations around the world — and can impact the health, safety and security of individuals.

Yet unlike the majority of other CI sectors, there are no cybersecurity mandates nor regulations for the manufacturing sector. An imperative exists to address the cybersecurity risks that stem from the Industrial Internet of Things (IIoT), cyber-physical security and even the data integrity of underlying systems. Furthermore, the sector has always been inherently global in nature, with supply chains spanning the world, and like other sectors, is increasingly subject to the challenges of cyber risk rising from the nature of geopolitical conflict. Increasingly, the U.S., the European Union (EU) and even individual states in the U.S. are passing laws that address IoT threats and raise the threshold of acceptable risk. The U.S. Departments of Homeland Security (DHS) and Commerce have published multiple reports making recommendations, ranging from how to consider the risk, as seen in the report "Strategic Principles for Securing the Internet of Things," [3] to the creation of a specific focus on the sector itself with the National Institute of Standards and Technology (NIST) release of the "Cybersecurity Framework Manufacturing Profile." [4] At the same time, there is a renewed focus by the DHS, the U.S. Department of Defense (DOD) and many others to help the sector better understand how cybersecurity risk can manifest itself in global supply chain security. This includes a focus on information communication technologies and services as well as broad-based global sourcing of component parts and country of origin identification.

What is at risk in the world of industry 4.0?

The European Union Networked Information Security Agency (ENISA) defines Industry 4.0 as a "paradigm shift towards digitalized, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT".[5]

Manufacturers, like all companies, must manage and address their own cybersecurity risk, and focus on how a potential cybersecurity attack could impact their end-users and customers. Global cyber incidents like WannaCry, LockerGaga and other ransomware attacks have hit manufacturers and crippled some manufacturing facilities. Attacks can force complete shutdowns of certain facilities, corrupt information technology (IT) systems and, at times, even force plant closures. Reputational risk is also a factor, as stock prices and brand value can be impacted. The manufacturing sector should also consider the following specific risks:

- Nation state attacks seeking to disrupt certain industries
- Intellectual property (IP) theft
- Data integrity issues/modification of customer specifications prior to manufacturing
- Cyber-physical damage to manufacturing facilities and end products
- Potential health and safety to employees
- Loss of productivity due to downtime
- Malware imbedded in supply chain that impacts integrity of the manufacturing process
- Loss of reliability and integrity of products

With cybersecurity presenting such a national and economic security risk: more regulations, not less, may be on the horizon.

Global agreement on cyber risk

The G20 held a ministerial meeting focusing on trade and the digital economy on June 8-9, 2019. The Ministerial Statement clearly articulated the benefits and risks that a digital world brings to sectors like manufacturing, stating: "Security in a digital economy is essential for strengthening public confidence in digital technologies and the entire digital economy." Concerns around cybersecurity risk to global supply chains and manufacturing and supply chain issues are also front and center for every major nation around the world. The G20 focused on and acknowledged the risk that also comes from the world of emerging technologies and the IoT. The Ministerial Statement also cited the benefits and the risks stating "Manufacturing, which is one of the most crucial industries in the global economy, is becoming more digitalized, networked and intelligent." [6]

U.S. approaches cybersecurity for manufacturing

Early in the Trump Administration, the White House released Cybersecurity EO 13800, which continued the focus on cyber risks to the manufacturing sector. EO 13800 specifically called for a review of "the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities."[7] While the manufacturing sector does not have any mandatory cybersecurity regulations, those entities that are publicly traded in the U.S. must also deal with the Securities and Exchange Commission (SEC). The SEC issued interpretive guidance in 2018 which laid out the expectations for corporate disclosures on cybersecurity risks. The guidance delineates where it believes existing SEC rules already encompass cybersecurity risks and associated disclosures. It reinforced an underlying concern that "cybersecurity risks pose grave threats to investors, our capital markets and our country." The SEC's guidance follows the requirement laid out in the EO and states: "As companies' exposure and reliance on networked systems and the internet have increased, the attendant risks and frequency of cybersecurity incidents have increased." Even EO 13777, one of the first EO's released on February 24, 2017 "Enforcing the Regulatory Reform Agenda" exempted national security issues, which includes cybersecurity, from the deregulation agenda.

Manufacturing is one of 55 national critical functions at highest risk for a cyberattack

As the U.S. and nations around the world continue to examine the best way to manage cybersecurity risk, the U.S. has chosen to focus on defining a new category of core functions that it considers to be at the heart of what must be protected. To achieve that, on April 30, 2019, DHS released a list of 'national critical functions' that the Department and the White House views as

> *"The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."* [8]

It includes a list of 55 functions that ultimately were drawn from the underlying list of 16 CI sectors. Manufacturing is one of the 55 functions and, as with the underlying CI sectors, it touches the majority of the other 54 functions in one way or another. Understandably, a cybersecurity attack on the manufacturing sector has wide-ranging impacts on all other sectors of the global economy as well.

Cybersecurity risk in supply chains

One key area of concern to the manufacturing sector is its supply chain. To better address the risk, the manufacturing sector increasingly needs to review, measure and map cyber risk in its global supply chain. Sourcing of parts, identification of countries of origin and requiring suppliers to meet certain benchmarks for cybersecurity risk are all a new part of what doing business means in the 21st century economy. Trusted supplier programs, which have been used for many years for overall quality, safety and as a means to track even basic counterfeit parts, must also now include cybersecurity requirements and audits. In the U.S., DHS has created an Information and Communications Technology (ICT) Supply Chain Security Group comprised of representatives from the information technology and communications sector. The DOD, which has long mandated cybersecurity for its contractors in the DIB and respective supply chains is kicking off the "Cybersecurity Maturity Model Certification" (CMMC). The program will serve as a mechanism to help ensure that the major defense contracting firms are more accountable for their own supply chains and cybersecurity.

White House executive order on cyber risk in supply chains

On May 15, 2019, the White House released Executive Order 13873:"Securing the Information and Communications Technology and Services Supply Chain." The national and homeland security community is concerned about aggregated risk that comes from the use of common ICT and services. Manufacturing especially relies on and uses all of these technologies and services for everyday aspects of operations. The EO applies to all entities subject to the jurisdiction of the U.S.,[9] and it also focuses on banning companies that are "owned, controlled or subject to the jurisdiction or direction of a foreign adversary" in the ICT space. A foreign adversary is specifically defined and comes with a formal process of designation, to avoid capturing traditional "friendly" nations.

Industrial Internet of Things (IIoT) and advanced automation brings both efficiencies as well as increased cyber risk

The manufacturing sector was one of the first to integrate robotics into the assembly line and to include advanced automation into the very foundation of the sector. The additional use of artificial intelligence (AI) and machine learning has led to advancements in everything from medical devices to the future of autonomous vehicles. Networked robots, mobile robots and supervisory control and data acquisition (SCADA) systems, and the integration of AI bring great efficiencies, but if not imbedded with cybersecurity at the front end, could all increase advanced cyber risk to the manufacturing sector.

Concerns around IoT, IIoT and global cyber risks have the full attention of global regulators. In the U.S., a study on how to address the threat of botnets and IoT cyber risk was issued in a 2018 report, also mandated by EO 13800, entitled "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats." The report focuses on broad based IoT risk and includes some useful lessons learned for the manufacturing sector.[10] The EU has focused on IoT risk for consumer devices and in February 2019, the European Telecommunications Standards Institute (ETSI) Technical Committee on Cybersecurity (TC CYBER) released a new standard, ETSI TS 103 645, focusing on security beelines.[11]

The use of AI to power robotics as well as varying aspects of the manufacturing industry will revolutionize the industry. At the same time, cybersecurity risks to AI must also be addressed and managed. While AI will power increased protections, AI tools will also be used to propagate more sophisticated cybersecurity attacks. The Organization for Economic Cooperation and Development (OECD) recently issued the "Recommendation of the Council on Arterial Intelligence" in May 2019. The OECD endorsed the need to support a host of key factors including "transparency and explainability" as well as "robustness, security and safety." The U.S. is a key member of the OECD and has not issued AI standards, but did issue a White House Executive Order on AI which includes the need to "ensure that technical standards minimize vulnerability to attacks from malicious actors and reflect federal priorities for innovation, public trust, and public confidence in systems that use AI technologies." [12]

Looking ahead

Manufacturing remains a core part of almost every aspect of the global economy and is increasingly more important to all other sectors as technology, automation and connectivity in an IIoT world take over critical functions.

And notably, the manufacturing sector has been in the top five most attacked sectors for cybersecurity since 2015.[13] The global regulatory regime is starting to focus on and acknowledge this risk, and as a result, more regulations, mandates and standards could soon follow.

To best understand, prepare for and manage cybersecurity risk, the manufacturing sector should consider the business, legal, regulatory and financial damage that a cybersecurity attack can bring.

Here are the top 15 important considerations:

1. **Understand the risk:** Attackers are looking to steal, disrupt or destroy, and have a host of motivations that may have nothing to do with a particular company.
2. **Define the risk:** Cybersecurity encompasses both loss of data and operational risk in the manufacturing sector. A cyberattack could also result in physical damage and losses to the company.
3. **Enterprise risk:** Cybersecurity is a systemic risk and needs to be part of an enterprise risk management plan.
4. **Executive leadership has an important role:** The c-suite must engage in and be part of managing cyber risk on an ongoing basis. The board must also be an active participant in the process as well.
5. **Understand, identify and map the "crown jewels" of the company:** Think like an attacker and map out where cyber risk exists.
6. **Focus on the basics:** Preparedness, response, recovery and restart: All companies must have a written cyber incident response plan. It must continually be tested both through table-top and real-life drills. These must include both loss of data/IP, as well as operational attacks on the manufacturing systems themselves.
7. **Define key roles in the cyber incident plan:** Every aspect of the company has a role in managing cyber risk. Define roles in advance, detail them in the plan, test responses and ensure that you have a list of key vendors ready on a 24/7 basis to assist.
8. **Train all employees including the executive team and staff:** Some of the easiest attack vectors come through spear-phishing exercises.
9. **Conduct the basics:** Reset passwords for employees regularly, change default passwords on all SCADA and ICS equipment and ensure a system of "least privileged" access for all sensitive systems.
10. **Understand the role the government can play in advance:** In the U.S., the DHS has assets and programs to provide support and there are "safe harbor" programs that exist. Law enforcement and other agencies have a valuable role to play, but relationships need to be established before an incident.
11. **Supply chain security is a must:** Create and map out a supply chain security plan. Include all vendors, map countries of origin and incorporate security requirements in all contracts and add audit requirements. Just having a "trusted supplier" program is not enough.
12. **Automation and digital technology include cyber risk:** All new investments in digital technology must imbed cybersecurity protections at the front end. Protections need to be added to address legacy systems and legacy risk. Know and understand that speed-to-market may create more problems than the perceived upside.
13. **Manage your insurance coverage wisely:** Cyberattacks on the manufacturing sector can range from traditional data breach, to IP theft, to physical damages in plants that could shut down every aspect of global operations. Ensuring that you have the right policies in place and the company understands the impact of a cyberattack should drive the types of policies and coverages you seek.
14. **Think of cybersecurity as a market differentiator for the company:** Customers and consumers are presuming that companies know and protect against the risk. Consider ways to add cybersecurity protections to your products and services to demonstrate your commitment to protecting your customer.
15. **Remember the basics:** The latest technology is not always the most secure technology unless you mandate that cybersecurity be included at the front end. All vendors do not necessarily understand the risk and/or incorporate the level of security your company may want. Ultimately, make sure that your cyber incident response plans are active, up-to-date and tested and you have the resources in place for when a cybersecurity attack takes place.

Sources

[1] G20 Japan 2019 Themes: https://g20.org/en/summit/theme/
[2] The European Union (EU) uses the term "Essential Functions" which closely mirrors the U.S. CI sectors. The delineation of essential functions is part of the EU's Networked Information Security (NIS) Directive.
[3] See U.S. Department of Homeland Security (2016) "Strategic Principles for Securing the Internet of Things": https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things20 16-1115-FINAL.pdf
[4] See NIST (2017) "Cybersecurity Framework Manufacturing Profile": https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf
[5] ENISA "Industry 4.0 Cybersecurity Challenges and Recommendations:" https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations
[6] G20 Ministerial Statement on Trade and Digital Economy: Section 5.25: https://g20.org/en/summit/theme/
[7] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity- federal-networks-critical-infrastructure/
[8] DHS National Critical Functions List: https://www.dhs.gov/cisa/national-critical-functions-set
[9] EO 13873: The term "entities" is defined as "partnership, association, trust, joint venture, corporation, group, subgroup or other organizations. The term "foreign adversary" means any foreign government or foreign non- government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons. The term "information and communications technology or services" means any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display; https://www.govinfo.gov/content/pkg/FR-2019- 05-17/pdf/2019-10538.pdf
[10] U.S. Department of Commerce: https://www.commerce.gov/page/report-president-enhancing-resilience- against-botnets
[11] ETSI: https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security
[12] White House Executive Order: "Maintaining American Leadership in Artificial Intelligence:" https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial- intelligence/
[13] Top 5 Industries at Risk of Cyber-Attacks, Forbes, May 15, 2016

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

Contact

Norma Krayem
Sr Policy Advisor
Chair, Global Cybersecurity & Privacy Policy and Regulatory Team
Holland & Knight LLP
+1 202 469 5195
norma.krayem@hklaw.com

willistowerswatson.com/social-media

WTW-NA-2019-WTW284590

willistowerswatson.com

Willis Towers Watson