10 CyLab, Web.

11 Office of the Press Secretary, the White House, *Fact Sheet: Cybersecurity National Action Plan* (White House, Feb. 9, 2016), Web.

12 FIRST: For Inspiration & Recognition of Science & Technology, FIRST Robotics Competition, FIRST Inspires, 2016, Web.



Ten

# Cybersecurity in the Manufacturing Sector

*Brian Raymond*, Director of Innovation Policy,
National Association of Manufacturers

## WHAT MAKES THE MANUFACTURING SECTOR UNIQUE

Connected devices are everywhere. They make homes comfortable and vehicles safer. They make offices more efficient and drive down energy costs. They increase crop yields and monitor pipelines. They track inventory and manage logistics. What was unimaginable just a decade ago is now a reality. This ubiquity of connected devices is known as the Internet of Things. And there is one industry behind all of this innovation: our nation's manufacturers.

Manufacturers are the creators, users, servicers, and installers of the Internet of Things. Billions of connected devices are pervasive throughout manufactured products and on the shop floors where they are made. This technology is creating enormous opportunity and driving transformative change. It has made all manufacturers into technology companies.

The days of interacting with the customer only during a single transaction are over. Connected technology enables manufacturers to provide real-time performance monitoring and usage patterns for their customers throughout the entire lifespan of a product. This will create a positive feedback loop resulting in better and more efficient products that will be sold

and bought for their promise of measurable results. A tire manufacturer won't just sell tires, but a package to reduce costs through sensors that collect data on fuel consumption and tire pressure.

The IoT will make services like predictive maintenance a standard offering, as well as enable efficiencies and flexibility across the entire manufacturing process and down the supply chain that feeds it. Productivity could go up by as much as 30 percent. McKinsey & Company estimates the economic impact of the Industrial IoT could reach $3.7 trillion by 2025.[1] Manufacturing will build the IoT and be transformed by it, simultaneously.

While connected technology drives innovation in the manufacturing sector, it also creates new challenges. Manufacturers are now the first line of defense in securing our nation's most critical online assets. They place cybersecurity at the highest priority level.

One of the primary targets for cyberattack inside the manufacturing ecosystem is industrial control systems. This is the class of computers that help manage the shop floor. ICS are configured in growing numbers to be reachable through the Internet, including systems retrofitted with modern networking capabilities.

Even when companies take measures to secure their Internet-addressable ICS, they often link their factory production and enterprise information technology networks. That connection results in benefits such as increased productivity, but a new class of malware is exploiting those links to target ICS, likely for espionage.[2] A recent survey of ICS cybersecurity specialists found that three-quarters of them believe their operation has undocumented external network links, a condition the IoT will exacerbate.[3]

In short, what's keeping the number of physically damaging ICS attacks so low isn't good security but probably a lack of motivation on the part of for-profit hackers and nation-states. The former hasn't yet learned how to monetize ICS attacks and probably sees no reason to start, given the bountiful opportunities present elsewhere. Nation-states are apparently content to limit themselves to surveillance. Neither condition is permanent.





## CHALLENGES FACING THE NEW ADMINISTRATION

### THE IOT IS GOING FASTER THAN SECURITY CAN KEEP UP

Although in its infancy, the Internet of Things is already a target of cyberattacks.[4] Symantec identified in 2013 a worm apparently engineered to attack devices such as television set-top boxes.[5] Although the report was later debunked, one cybersecurity firm made waves when it claimed to have uncovered a smart refrigerator used by attackers to send out spam.[6] The mere fact that a household appliance may be a target has elevated the level at which manufacturers must consider securing the IoT.

Many IoT devices will possess minimal processing power. That is the nature of the thing—ubiquitous and cheap devices everywhere whose power comes through networking. As a result, many devices may not have capability for basic cybersecurity best practices, such as encryption and operating system updates. Even where capacity exists, manufacturers might not find it economical to patch devices made on a slim margin in a market relentlessly focused on the next generation of products.[7]

Devices are only one part of the IoT universe. Databases holding telemetry generated by the devices are another substantial component, one that likely to become another target for hacking. Cybersecurity firm iPower Technologies already spotted in 2015 malware targeting newly purchased police body cameras, likely in order to access law-enforcement data.[8]

### CYBER ESPIONAGE

Only the government tops the manufacturing sector as a victim of cyber espionage.[9] Primarily perpetuated by nation-states or their proxies, cyber espionage doesn't seek to disrupt computing infrastructure but exploit it for the information locked away inside. That includes intellectual property as well as business intelligence. Nation-states have targeted information such as pricing, production numbers, and business strategies in addition to vacuuming out high-tech design information.[10]

The IoT will increase the attack surface for manufacturers. The more that shop floors become imbued with intelligent machines, the more those

machines will contain data worth stealing. They will contain intellectual property worthy of theft by itself, but also metrics on production that bad actors have already shown a gargantuan appetite for illicitly acquiring.

Espionage isn't just a matter of lost revenue. It's a threat to economic security with implications for national security. "Our economy depends on the ability to innovate. And if there's a dedicated nation-state who's using its intelligence apparatus to steal day in and day out what we're trying to develop, that poses a serious threat to our country," recently explained John Carlin, assistant attorney general for national security.[11]

A secondary threat to national security stems from the manufacturing sector's global supply chain. Larger companies have the resources and sophistication to be sensitive to cyber vulnerabilities and take steps to contain them, but smaller enterprises may not. This leaves the entire supply chain vulnerable—creating threats in every sector, including the defense industrial base.

### INDUSTRIAL CONTROL SYSTEM SECURITY IS UNDERRATED

Attackers seeking to disrupt industrial processes don't need to exploit an underlying software vulnerability, the way that sophisticated hackers do when attacking enterprise IT systems. They simply need to gain access to the ICS (perhaps through the corporate IT network) and use the exposed digital controls to manipulate the system into failure. No further hacking required.

Operational technology is a different beast and much of the hard-won knowledge about mainstream technology cyber defense isn't transferable. Although ICS more and more incorporate commercial-off-the-shelf parts and operating systems, the objectives and priorities of an automated shop floor are different than a data center. "The number-one goal of IT security is rooted in the concern about privacy—'Protect the Data'—whereas the number-one goal of ICS security is based on the concern for safety—'Protect the Process,'" notes a blog post from an ICS security provider.[12] As a result, company cybersecurity and operational personnel who are hands-on with the automated systems are working hard to coordinate their efforts and cybersecurity strategies.





The Department of Homeland Security stood up in 2009 the Industrial Control Systems Cyber Emergency Response Team in recognition of this challenge, but the years since have proved disappointing. As Dale Peterson notes, ICS-CERT should be "developing secure ICS protocols and standards, accurately informing government and industry, analyzing ICS attack code," but its main output is further transmitting alerts already widely available to industry.[13]

## RECOMMENDATIONS

### INCENTIVES FOR IMPROVING CYBERSECURITY

Small- and medium-sized manufacturers in particular face bad economics when it comes to achieving a level of cybersecurity robust enough to stand up to nation-states, manufacturing's main cyber threat. Market forces stymie private-sector businesses from standing up cybersecurity capacity beyond the threshold of normal commercial risk, forces particularly strong below the threshold of large businesses.

"It's not a fair fight. A private company can't compete against the resources of the second largest economy in the world," said John Carlin, assistant attorney general for national security, discussing attacks from China.[14]

This gap between commercially sustainable levels of cybersecurity and what's necessary to counteract foreign adversaries isn't just a market failure. It's the space that federal government was designed to fill by dint of its constitutional charge to provide for the common defense. If the notion of national security depending on strengthening the network defense of a tractor plant in the Midwest seems strange, that's only because cybersecurity has altered what used to be geographic borders into digital frontiers. On the Internet, the domestic and the foreign rub shoulders without having to cross oceans.

But filling the gap with better cybersecurity isn't something the government can do on its own; it doesn't own the Internet, nor the tractor plant's computers. What's necessary is a public-private partnership that uses economic tools to encourage investment beyond ordinary levels of commercial cybersecurity spending.

Specifically, the government should complete the task begun with creation of the National Institute of Standards and Technology Cybersecurity Framework in determining what the most cost-effective elements of cyber defense are. The executive order that resulted in the framework's creation never saw it as an end in of itself. The order charged the network with setting out a "prioritized, flexible, repeatable, performance-based, and *cost-effective approach*" to cybersecurity (emphasis added).[15]

For NIST to determine how to use the framework cost-effectively is, admittedly, no easy task. But the structure for setting up studies with private-sector cooperation already exists with the sixteen critical infrastructure sector coordinating councils and their sibling government coordinating councils. In a nutshell, the councils for each critical infrastructure sector should seek out representative companies and solicit their voluntary participation in studies to test practical application of the framework in their information technology infrastructure. The studies would measure costs and benefits and identify where the chasm between commercially sustainable cybersecurity protections and nation-state-level protections opens up.

## FUND IOT SECURITY RESEARCH

No amount of incentives can overcome a key characteristic of the Internet of Things: ubiquity of cheap computers with minimal computing power. The ability to seed the environment with cheap computers is what makes the IoT possible. Durable goods will likely possess sufficient capacity for cybersecurity measures such as firewalls. But they will be the exception. What makes the IoT possible is also what makes it vulnerable.

This is an irreducible problem that requires a different approach to cybersecurity, one premised on building secure systems from insecure components. This isn't a new notion, but it's one that's needs urgent revitalization, forearmed as we are with the certain knowledge of a planet's worth of devices coming online in the near future. The National Science Foundation, the Defense Advanced Research Projects Agency and the research arm of the Department of Homeland Security should make funding research into this a priority.





## ICS-CERT SHOULD BE STRENGTHENED

The Industrial Controls Systems Cyber Emergency Response Team performance needs to enhance its focus on development of best practices and on research. The organization's outreach to the manufacturing sector should also be improved.

"We tend to count things—how many alerts, how many advisories, how many incidents do you respond to," said ICS-CERT director Marty Edwards in May 2016.[16] "I think we have to get to the point of measuring what impact did we make inside of a company, or how is a sector improving or degrading over time in the cybersecurity area," he added. The manufacturing sector concurs.

---

1 James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon, *Unlocking the Potential of the Internet of Things* (McKinsey Global Institute, June 2015), Web.

2 Robert M. Lee, "Fourth Sample of ICS Tailored Malware Uncovered and the Potential Impact," *SANS Industrial Control Systems Security Blog*, Apr. 25, 2016, Web.

3 Derek Harp and Bengt Gregory-Brown, *The State of Security in Control Systems Today* (InfoSec Reading Room, SANS Institute, SurfWatch Labs, and Tenable Network Security, June 2015), p. 18, Web.

4 Hewlett Packard Enterprise Security Research, *Internet of Things Research Study* (Hewlett Packard Enterprise Development LP, 2015), Web; *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack* (Hewlett Packard Development Company, LP, July 29, 2014), Web.

5 Kaoru Hayashi, "Linux Worm Targeting Hidden Devices," *Symantec Official Blog*, Nov. 27, 2013, Web.

6 Paul Thomas, "Despite the News, Your Refrigerator Is Not Yet Sending Spam," *Symantec Official Blog*, Jan. 23, 2014, Web.

7 Bruce Schneier, "Security Risks of Embedded Systems," *Schneier on Security* (blog), *Wired*, Jan. 9, 2014, Web.

8 Patrick Sweeney, "Insecurity of Things: The IoT Devices You Deploy May Be Trojan Horses," *Venture Beat*, Apr. 17, 2016, Web.

9 Akamai Technologies, Anti-Phishing Working Group (APWG), et al., *2016 Data Breach Investigations Report* (Verizon, 2016), p. 53, Web.
10 David Talbot, "Cyber-Espionage Nightmare," *MIT Technology Review*, June 10, 2015, Web.
11 "The Great Brain Robbery," interview by Lesley Stahl, *60 Minutes—Business*, CBS Interactive Inc., Jan. 17, 2016, television and transcript.
12 Heather Mackenzie, "SCADA Security Basics: Why Industrial Networks Are Different than IT Networks," *Tofino Security*, Oct. 31, 2012, Web.
13 Dale Peterson, "Lies, Damned Lies and Statistics—Part 2," *Digital Bond*, Apr. 3, 2015, Web.
14 "The Great Brain Robbery," interview by Lesley Stahl.
15 Exec. Order No. 13636, 3 C.F.R. (2013).
16 "S4x16 Video: Interview with Marty Edwards, Director of ICS-CERT," interview by Dale Peterson, *Digital Bond*, May 24, 2016, Web.



Eleven

# Cybersecurity in the Food and Agriculture Sector

*Dr. Robert Zandoli*, Global Chief Information Security Officer, Bunge Limited

## WHAT MAKES THE FOOD AND AGRICULTURE SECTOR UNIQUE

At a distance, grain silos and feedlots look the same as they ever did. Up close, the food and agriculture sector has seen huge changes wrought by digital connectivity. A combine isn't just a grain-harvesting machine; it's a data-gathering platform.

Be it wired-up off-road equipment and agricultural machinery, high-tech food and grain processing, radio frequency ID-tagged livestock, or global-positioning-system tracking, the sector has become dependent on information systems to sustain and improve operations, competiveness, and profitability.

Wringing out even more efficient yields is a global and domestic necessity. Demand for agricultural products will increase significantly in the future, owing to population growth and rising living standards in emerging markets. Breadbasket countries like the United States must find sustained growth in yields to meet such exploding demands. Not just as a matter for growth but also to prevent domestic food costs from spiraling upward. Domestically, that means finding yet more efficient ways to farm.[1] And without making use of remote sensing and computer science, significant