# Securing Smart Operations

## A Look at Connectivity, Vulnerability, and Five Steps to Mitigate Risk

by Maria Lowry and Michael Glessner

The power of smart operations stems from the development of new networks that connect people, sensors, and equipment. These new networks have the potential to create value that we are only beginning to understand and leverage. They are already yielding unprecedented insight into performance improvement opportunities to achieve manufacturing's primary goals; to keep people, equipment, and secrets safe, productive, valuable, and constantly improving.

The greater the connectivity between shop nodes, the greater the potential impact of a cyber-attack. Cyber-attacks targeted at integrated shop floors have the potential to not only negate gains from connectivity, but also destroy enterprise-wide networks, equipment, customer relationships, and may even place employees' lives at risk.

Cyber-attacks are no longer unusual—news reports of new and devastating attacks are increasingly regular. While most public reports focus on attacks targeting healthcare, infrastructure, and banking entities, manufacturing is the 2nd most frequently targeted industry for cyber-attacks[1]. Such attacks threaten to compromise manufacturers' ability to simply keep their lights on, let alone pursue their core objectives.

### The Potential Value of Network Connectivity...

According to Robert Metcalfe, the value of a network is proportional to the square of the number of connected users of the system.

$$Value^{system} = N^{users^2}$$

In a smart operation, sensors are connected to physical and electronic assets, customers are connected to products and services, suppliers are connected to enterprise and customer feedback, and products are connected back to the enterprise via a constantly communicating network of sensors, systems, and people.

Each node within the network generates data that can feed constantly evolving deep learning models that rapidly and automatically improve employee safety, increase quality, reduce waste, advance operation processes, enhance the roles of employees, and provide unprecedented value to customers. To learn more about the current and developing capabilities of smart operations, see *Manufacturing Innovation in a Digital World*.

## … And the Exponential Vulnerabilities

Just as the value of a network is the square of the number of its connections, a network's vulnerabilities are exponentially proportional to the network's number of connections. The difference between the value and vulnerability calculations is that the vulnerability exponent is constantly in flux.

$$N^{connections} = Vulnerabilities^{system^{x}}$$

Every connection in a smart operation is an access point that hackers can access at any time, and in countless ways—an insufficiently protected sensor, a customer's laptop operating on an insecure network, user error, or an employee's cellphone that hasn't undergone the latest manufacturer update. As the quantity, type, and complexity of a node increases or varies, the risk of compromise and consequences differ dramatically.

The reasons for this variability are simple:

1. **Hackers are constantly evolving their techniques:** hackers have historically set the pace for learning in cyber space, and mainstream cyber users are just now understanding how to keep up
2. **The incentives for hackers are diverse and growing:** while some infiltrate networks to test new techniques, others have carved their niche in the Espionage as a Service (EaaS) space and get hefty paychecks from competitors and governments alike

> "There are two types of companies: Those who know they've been hacked and those who don't." John Chambers, CEO of Cisco.

Many others have echoed this observation as a reality check of today's cyber security landscape and to highlight the necessity of safeguarding operational networks. Adequate preparation and vigilant monitoring must be taken to safeguard all data and networks to prevent an attack that could balloon into a physical threat to a facility, a privacy threat to a department, or a financial threat to your entire customer base.

## Five Important Steps to Mitigate Your Risk

The cost of cyber-attacks on the global economy is estimated to exceed $6 trillion by 2021[2], averaging $4 million per company per attack. With such a high price tag, the risks that accompany smart operations may seem to outweigh the benefits.

This could not be further from the truth.

Connectivity is the future of business, public and private life, and institutions. It's the path to discoveries and breakthroughs we are just beginning to imagine. The question needs to be, "How do I ensure that this initiative helps me achieve my goals without interference from outside forces?"

Simply said: Companies must create and execute a cyber and information defense strategy that includes the technological and personnel resources necessary to stay a step ahead of malicious activity. This is challenging to accomplish—cyber security for smart operations is in its infancy, so security professionals at every level, especially executive, are in high demand, and out-of-the-box technology solutions to ensure appropriate defenses do not yet exist.

These are five steps that you can take to begin to mitigate these circumstances and step out as a leader in secure smart operations:

1. Get a talent and research pool started on your terms and to your benefit: initiate relationships with university and certification programs that are pursuing cyber security research and excellence
2. Build upon existing access controls, Information Technology security, and Operations Technology security as part of your smart operations
3. Inform and educate employees about unexpected or mishandled security situations: treat breaches and near-misses as learning opportunities for everyone involved
4. Learn fast by building failsafe environments and using internal resources to find and remedy vulnerabilities
5. Partner with experts in your industry who have experience enabling secure smart operations and understand vulnerabilities

Make no mistake—as network opportunities evolve, so do hacker methods, incentives, and tenacity. These suggestions are a starting point, not a fool-proof (or hacker-proof) solution.

Whether your floor is preparing, implementing, or executing and reaping the benefits of a smart manufacturing strategy, you can be an integral part of your organization's success by making cyber security a cornerstone of your secure smart operation.

1. IBM X-Force Threat Intelligence Index 2017, IBM Security, Https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&, March 2017, accessed July 5, 2017, https://www.ibm.com/security/.

2. Steve Morgan, Hackerpocalypse: A Cybercrime Revelation, Herjavec Group, https://www.herjavecgroup.com/wp-content/uploads/2016/08/Hackerpocalypse.pdf, September 2016, accessed July 5, 2017, https://www.herjavecgroup.com/.

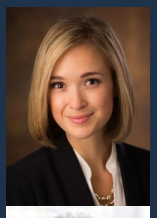
## Read more about smart connected operations:

*Getting Started with Smart Connected Operations*

*Practical Steps for Smart Connected Operations*

*Originally published on October 24th, 2017*

What's your view? Add your question or comment



### Maria Lowry

maria.lowry@kalypso.com

Maria is a senior consultant with Kalypso.

### Michael Glessner

michael.glessner@kalypso.com

Michael is a Director with Kalypso. His areas of expertise include new product development, business and innovation strategy, large-scale