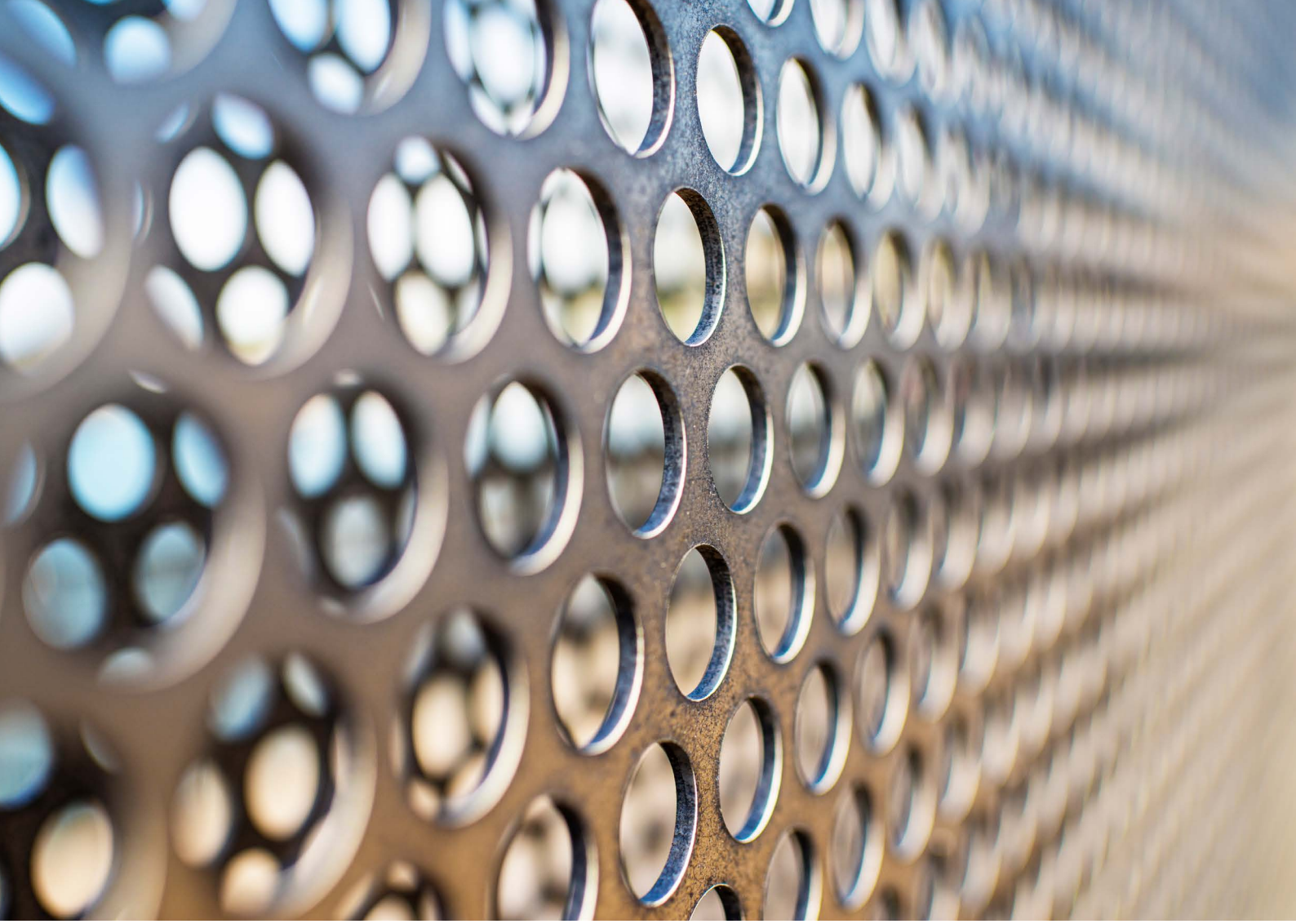


BRIDGING THE CYBER GAP IN MANUFACTURING

HOW TO NAVIGATE THE CYBER JUNGLE

Emmanuel Amiot, Eric Ciampi, Charles de Pommerol

OLIVER WYMAN

For Innovations brought on by technology are rapidly transforming the manufacturing and supply-chain sectors. Digitalization, a game changer, is bringing with it multiple benefits, such as mass customization, dynamic make-to-order products, real-time data-driven operations, and management of the extended supply chain. Increasingly, machinery, products, and delivery vehicles are becoming interlinked.

These changes imply the continued evolution of information systems towards greater modularity, openness, interoperability, and, especially, security. That said, industrial companies face a host of challenges in transforming their IT/OT capabilities: legacy hardware and software, insecure systems, networks with limited encryption proficiency, proprietary connectivity protocols, and a talent shortage.

Additionally, manufacturers are relatively late in addressing their cybersecurity needs. Making it a board-level priority in the industry has proven more difficult than in other sectors, such as financial services or defense.

Still, cybersecurity should be a key priority, as the cost of cybercrime is estimated in 2019 at $1,000 billion. The recent cyberattacks mounted on industrial companies – NotPetya, Triton, and Stuxnet – revealed the high degree of interconnectivity and vulnerability of industrial systems (such as SCADA, PLC, and Industrial Internet of Things (IIoT) devices) with the non-industrial world. The spread of IIoT has brought with it heightened concerns over what data is captured and how.

The case for change is clear: Cyberattacks in manufacturing industries are on the rise. But how do manufacturers close the cybersecurity gap in the most pragmatic and cost-efficient way?

Looking at what the financial-services sector has managed to do may provide an answer. The sector has been a leader in delivering cybersecurity in complex IT ecosystems. Seeing how key financial players defined, launched, and reoriented their cyber transformation offers powerful lessons. We'll focus on three lessons that are of critical importance.

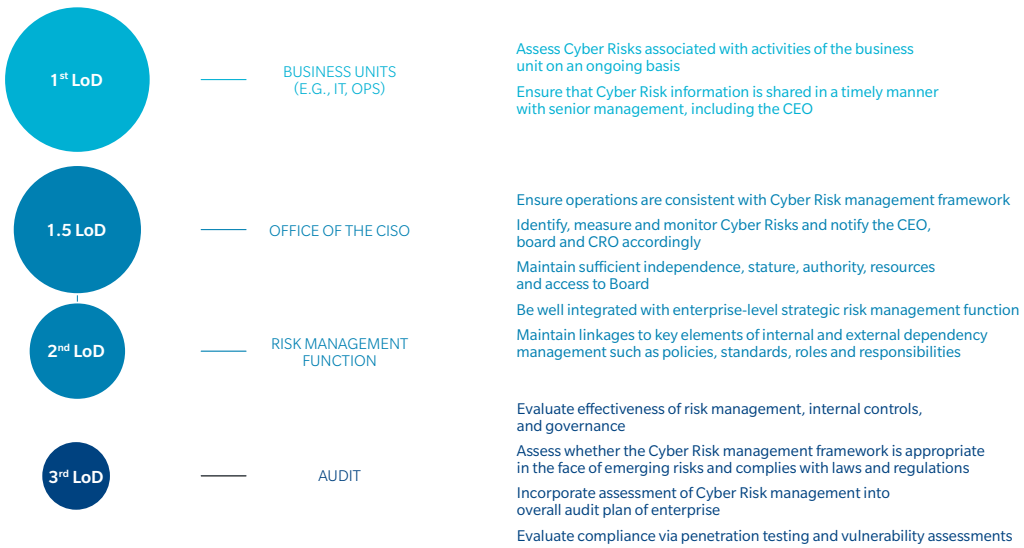
LESSON #1: THE CHIEF INFORMATION SECURITY OFFICER (CISO) AT MANUFACTURERS NEEDS TO BE A "SERIAL" TESTER

Companies need someone in the driving seat to steer cybersecurity initiatives at all its manufacturing sites.

Initially, the common reflex of any company has been to argue, "Cybersecurity is an IT matter." The CISO thus was conceived as the central owner of all security capabilities. In practice, however, the security setup turns out to be much more fragmented: the plant controls the industrial networks, infrastructure (such as IT production) maintains most of the corporate network security, operations oversee IT risk management controls and business continuity plans, and compliance owns security controls, including cyber fraud.

The positioning of the manufacturing CISO outside the IT function – and implementing a three lines of defense model – provides a solution to the roles-and-responsibilities puzzle. (See Exhibit 1.) In the model, the first line of defense are the controls on the activities of the business unit; the second line of defense is managed by the CISO and an enterprise-level strategic risk-management team; and the third and final line of defense consists of frequent audits.

Exhibit 1: Three Lines of Defense concept as applied to cyber



Source: Oliver Wyman analysis

This approach ensures that the CISO effectively and firmly defines and owns all IT/OT cybersecurity-related controls. The mandate of the CISO is to:

- Independently define and own the group cyber-risk appetite statement in coordination with the board, creating the right level of adherence from IT, business lines, plants, and support functions

- Define and own cybersecurity policies, standards, and procedures
- Help define the roadmap to implement controls and reach target thresholds
- Continuously test the organization against the defined targets – via penetration testing and red team exercises

LESSON #2 – BUILDING A STRONG FOUNDATION IS MORE IMPORTANT THAN DEPLOYING SECURITY SOLUTIONS

Once a manufacturing CISO is positioned and empowered adequately, the next step is to figure out where to start the transformation. Even in cases in which companies go in this direction, starting with the deployment of security tools rather than setting the basics right is not the way to begin.

Effective cybersecurity is about knowing where the data lies and who should have access to it rather than deploying a solution per se (in fact, that should be the very last step). It is crucial to put the foundations in place so as to avoid unnecessary costs and poor risk mitigation. In practice, this means:

- Defining your cyber-risk appetite and thresholds for controls by type of risk
- Building and maintaining an enterprisewide list of business-critical services
- Instilling a heightened cybersecurity awareness in the different teams
- Stress-testing infrastructure by simulating attacks
- Defining and maintaining incident management processes, including business continuity/disaster recovery plans, for critical processes and systems
- Building dashboards/KPIs for on-going monitoring
- Having two distinct but interconnected networks (industrial and corporate)

LESSON #3 – MOVING TO THE CLOUD WILL REQUIRE A ROBUST AND INNOVATIVE CENTRALIZED APPROACH TO SECURITY

Now that the lines of defense are in place and a solid foundation has been laid, the manufacturing CISO turns to defining the company's three-year cybersecurity strategy in coordination with senior leadership. The manufacturer's public cloud strategy represents the proverbial elephant in the room, given the rise of IIoT and the connected supply chain.

Leading companies have developed best practices in this domain. First, they have established a central, overarching security approach to the cloud and legacy systems made up of three layers of protection:

- Identity and Access Management (IAM): Access rights are managed centrally to ensure that access to systems and data is assigned to administrators and users on a "need-to-have" basis
- Multifactor Authentication (MFA): MFA is used to ensure that administrators and users are authenticated before accessing the cloud or legacy environment

- Encryption and tokenization are employed in cases of particularly sensitive data

Second, leading companies leverage security offerings from cloud providers to prevent common threats, benefit from scale effects, and avoid having to reinvent the wheel.

A FUNDAMENTAL CULTURAL SHIFT IS NEEDED

- Bridging the cybersecurity gap entails a fundamental cultural shift that the head of manufacturing, the CIO, and the board need to demand, support, and nurture. Here's how to trigger the change:

Over the next six months

- Conduct advanced, independent penetration tests and red team exercises to identify vulnerabilities
- Define the business' cyber risk-appetite statement based on identified exposures – with the goal of putting a dollar figure on potential losses
- Translate the cyber risk-appetite statement to a dashboard that enables management to oversee and steer the transformation
- Appoint a manufacturing CISO and develop your target cybersecurity model

Over the next 12 months

- Bring the most critical manufacturing sites up to speed in terms of cyberthreat detection and response
- Implement a strict access control policy to sensitive systems, supported by best-in-class identity- and access-management tools and advanced encryption to prepare for the transition to the cloud
- Close the most critical findings identified through penetration tests and red team exercises
- Define a cybersecurity organization ramp-up program and talent management strategy

Manufacturing companies have a great deal of work ahead of them in securing their operations, given their vulnerability to cyberattack. However, there are strategies to mitigate risk and secure key assets. To be ready for the future, manufacturing companies must be prepared to act now.

Emmanuel Amiot
Emmanuel.Amiot@oliverwyman.com
+33 1 45 02 32 71

Eric Ciampi
Eric.Ciampi@oliverwyman.com
+33 1 45 02 32 34

Charles de Pommerol
Charles.Depommerol@oliverwyman.com
+33 1 45 02 36 38