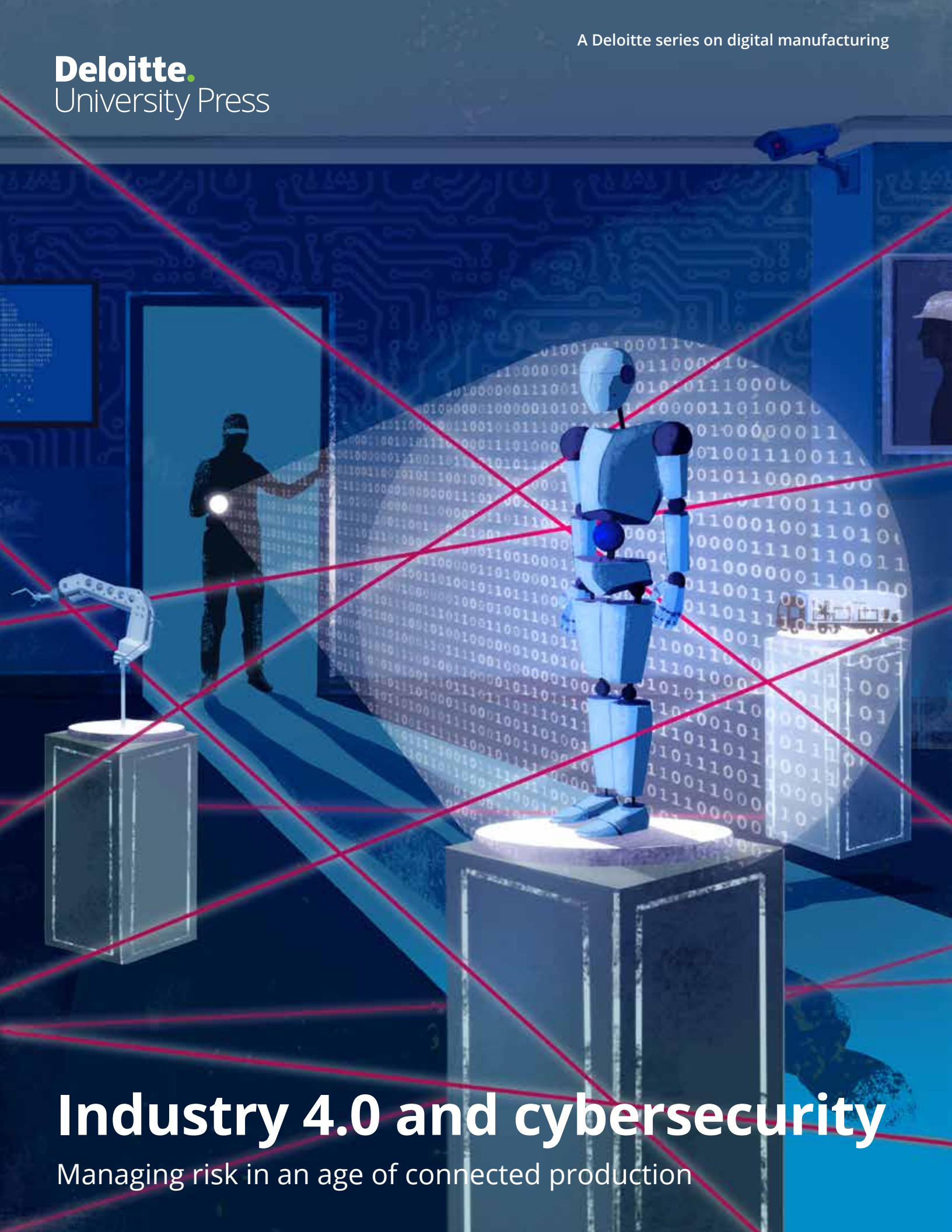
A Deloitte series on digital manufacturing

Deloitte.
University Press



Industry 4.0 and cybersecurity

Managing risk in an age of connected production

Deloitte Consulting LLP's Supply Chain and Manufacturing Operations practice helps companies understand and address opportunities to apply Industry 4.0 technologies in pursuit of their business objectives. Our insights into additive manufacturing, IoT, and analytics enable us to help organizations reassess their people, processes, and technologies in light of advanced manufacturing practices that are evolving every day.

COVER IMAGE BY EVA VAZQUEZ

Contents

Introduction

The fourth industrial revolution brings with it a new operational risk for connected, smart manufacturers and digital supply networks: cyber. The interconnected nature of Industry 4.0–driven operations and the pace of digital transformation mean that cyberattacks can have far more extensive effects than ever before, and manufacturers and their supply networks may not be prepared for the risks. For cyber risk to be adequately addressed in the age of Industry 4.0, cybersecurity strategies should be secure, vigilant, and resilient, as well as fully integrated into organizational and information technology strategy from the start.

In 2009, malware manipulated the speed of centrifuges in a nuclear enrichment plant, causing them to spin out of control. This malware, now known as Stuxnet, was introduced into stand-alone networks via flash drives, and it autonomously spread across production networks. Stuxnet's sophistication serves as a powerful example of cyberattacks' potential as weapons in the world of connected physical factories.[1] And the battle is decidedly unbalanced: Organizations must protect a wide swath of technology, while attackers need only pinpoint the weakest link.

It is important, however, that we balance our focus between the external threat landscape and the very real—and typically overlooked—cyber risks created by businesses who are increasingly using smart, connected technologies to innovate, transform, modernize, and otherwise make tactical or strategic business decisions that could result in such risk. These new and emerging risks should be managed and mitigated.

The increased connectivity of smart machinery, a shift known as *Industry 4.0*, raises the stakes. Industry 4.0 heralds a new age of connected, smart manufacturing, responsive supply networks, and tailored products and services. Through its use of smart, autonomous technologies, Industry 4.0 strives to marry the digital world with physical action to drive smart factories and enable advanced manufacturing.[2] But while it plans to enhance digital capabilities throughout the manufacturing and supply chain processes and drive revolutionary changes to connected devices, it also brings with it new cyber risks for which the industry is unprepared. Developing a fully integrated strategic approach to cyber risk is fundamental to manufacturing value chains as they marry operational technology (OT) and information technology (IT)—the very force driving Industry 4.0.

As threat vectors radically expand with the advent of Industry 4.0, new risks should be considered and addressed. Put simply, the challenge of implementing a *secure*, *vigilant*, and *resilient* cyber risk strategy is different in the age of Industry 4.0. When supply chains, factories, customers, and operations are connected, the risks posed by cyberthreats become all the greater and potentially farther reaching.

Thinking about how to address cyber risk at the end of the strategic process is simply likely too late. Cybersecurity should become an integral part of the strategy, design, and operations, considered from the beginning of any new connected, Industry 4.0–driven initiative.

In this paper, we examine the modern connected digital supply networks, smart factories, and connected device themselves, focusing on the unique cyber risks faced by each.[3] Moving through the production life cycle (figure 1)—from the digital supply network, to the smart factory, and finally to the connected object—we explore the actions operations and information security executives can take to anticipate and effectively address cyber risks as well as proactively integrate cybersecurity into their strategy in the age of Industry 4.0.

Figure 1. Smart production life cycle and cyber risk

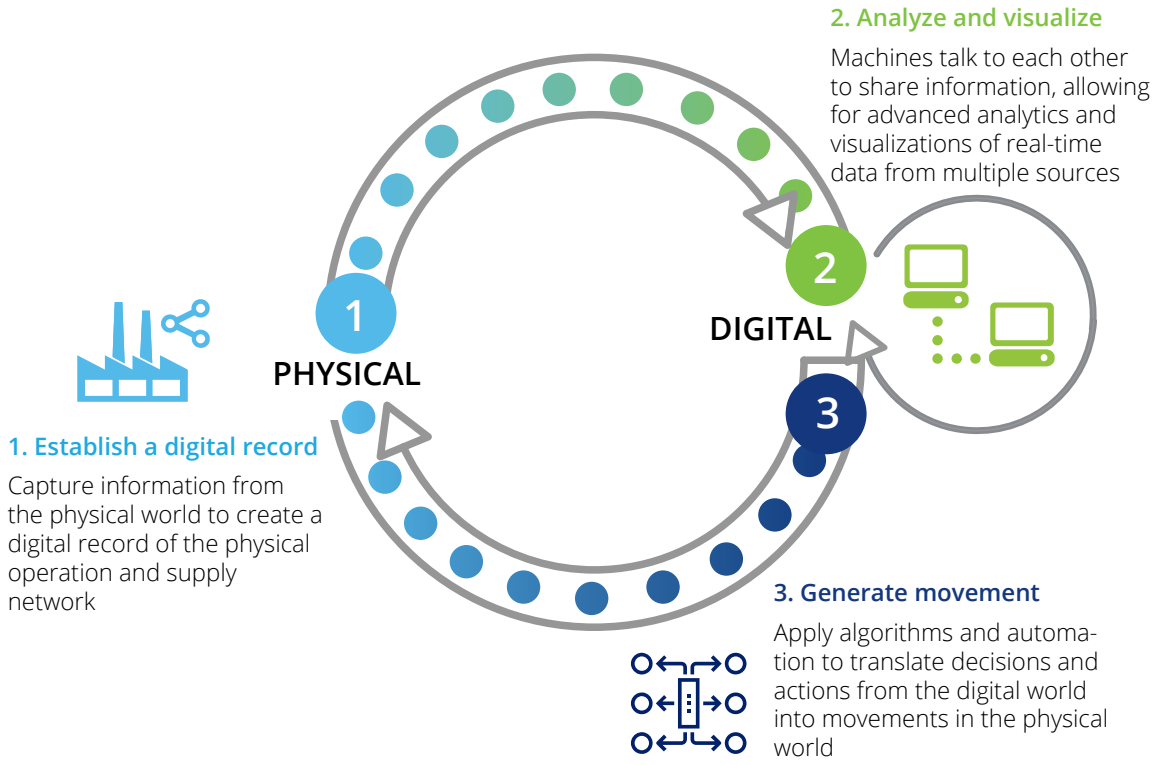
Production life cycle stage	Secure, vigilant, resilient categorization	Cyber imperative	Objective
Digital supply network 	Secure, vigilant, resilient	Data sharing	Ensure integrity of systems so private, proprietary data cannot be accessed
	Secure, vigilant, resilient	Vendor processing	Maintain trust when processes cannot be validated
Smart factory 	Vigilant	Health and safety	Ensure safety for both employees and the environment
	Vigilant, resilient	Production and process resilience/efficiency	Ensure continuous production and recovery of critical systems
	Vigilant, resilient	Instrumentation and proactive problem resolution	Protect the brand and reputation of the organization
	Secure, resilient	Systems operability, reliability, and integrity	Support the use of multiple vendors and software versions
	Vigilant, resilient	Efficiency and cost avoidance	Reduce operating costs and increase flexibility with remote site diagnostics and engineering
	Secure	Regulatory and due diligence	Ensure process reliability
Connected object 	Secure	Product design	Employ secure software development life cycle to produce a functional and secure device
	Vigilant	Data protection	Maintain the safety of sensitive data throughout the data life cycle
	Resilient	Remediation of attack effects	Minimize the effects of an incident while quickly restoring operations and security

DIGITAL MANUFACTURING ENTERPRISES AND INDUSTRY 4.0

The Industry 4.0 technologies that enable digital manufacturing enterprises and digital supply networks involve the integration of digital information from many different sources and locations to drive the physical act of manufacturing and distribution. This integration of information technology and operations technology is marked by a shift toward a physical-to-digital-to-physical connection. Industry 4.0 combines the Internet of Things (IoT) and relevant physical and digital technologies, including analytics, additive manufacturing, robotics, high-performance computing, artificial intelligence and cognitive technologies, advanced materials, and augmented reality, to complete that cycle and digitize business operations.

The concept of Industry 4.0 incorporates and extends the IoT within the context of the physical world—the physical-to-digital and digital-to-physical leaps that are somewhat unique to manufacturing and supply chain/supply network processes (figure 1). It is the leap from digital back to physical—from connected, digital technologies to the creation of a physical object—that constitutes the essence of Industry 4.0, which underpins the digital manufacturing enterprise and digital supply network.

Figure 2. The physical-to-digital-to-physical leap of Industry 4.0



Source: Center for Integrated Research.

Even as we explore the ways in which information creates value, it is important to understand value creation from the perspective of the manufacturing value chain. Throughout the manufacturing and distribution value network, business outcomes may emerge from the integration of information and operations technologies via Industry 4.0 applications.

For further information, visit *Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises*.[3]

The digital supply network

Changing supply chain, evolving cyber risks

THE supply chain—how materials enter into the production process, and semi- or fully finished goods are distributed outside—is fundamental to any manufacturing organization. It is also tightly connected to consumer demand. Many global organizations use demand forecasts to determine the quantity of materials necessary, manufacturing line requirements, and distribution channel loads. Analytics have also become more sophisticated, so that today's organizations are able to utilize data and analytics to understand and predict customer buying patterns.

Industry 4.0 technologies are expected to prompt a further evolution in the traditional linear supply chain structure by introducing intelligent, connected platforms and devices across the ecosystem, resulting in a digital supply network (DSN) capable of capturing data from points across the value chain to inform each other. The result may be better management and flow of materials and goods, more efficient use of resources, and supplies that more appropriately meet customer needs.[4]

For all its benefits, however, the increasing interconnectedness of the DSN also brings with it cyber weaknesses that should be properly planned and accounted for in every stage, from design through operation, to prevent significant risks.

The cyber risks of sharing data across the DSN

As the DSN evolves, one expected outcome is the creation of a network that allows real-time, dynamic pricing of materials or goods based upon the demand of purchasers relative to the supply available.[5] But a responsive, agile network of this nature is made possible only by open data sharing from all participants in the supply network, which creates a significant hurdle; it will likely be difficult to strike a balance between allowing transparency for some data and maintaining security for other information.

Organizations may thus want to consider ways to secure that information to prevent unauthorized users from accessing it across the network. They would also likely need to remain disciplined about maintaining those safeguards across all supporting processes, such as vendor acceptance, information sharing, and system access. Not only may these processes be proprietary in their own right, they may also potentially serve as access points to other internal information.

This may also place more strain on third-party risk management. In analyzing the cyber risks of interconnected DSNs, we have identified two main areas impacted by increased supply chain connectivity: data sharing and vendor processing (figure 3).

We discuss each area as well as potential strategies for addressing increased cyber risks below.

DATA SHARING: INCREASED ACCESS TO DATA FOR MORE STAKEHOLDERS

Organizations will likely need to consider what data should be shared, and how to protect the systems and underlying data that may be proprietary or have privacy risks. For example, some suppliers in a particular DSN may be competitors in other areas, and may not wish to make certain types of data available, such as pricing or information about proprietary materials. Alternatively, the suppliers may be subject to regulations that limit the type of information that can be shared. Opening up just part of the data may make it possible for those with malicious intent to gain access to other information.

Figure 3. Smart imperatives and risks

Production life cycle stage	Secure, vigilant, resilient categorization	Cyber imperative	Objective
Digital supply network 	Secure, vigilant, resilient	Data sharing	Ensure integrity of systems so private, proprietary data cannot be accessed
	Secure, vigilant, resilient	Vendor processing	Maintain trust when processes cannot be validated

Deloitte University Press | dupress.deloitte.com

Organizations should utilize good hygiene techniques such as network segmentation and intermediary systems that serve as "middlemen" to gather, protect, and provide information. Additionally, technologies such as trusted platform modules or hardware security modules should be incorporated into future devices to provide robust cryptologic support, hardware authentication, and attestation (that is, detect when unauthorized changes are made to the device). By combining this approach with robust access controls, mission-critical operations technology is secured at the application points and endpoints to protect its data and processes.

Where data must be available in part, or the data sensitivity is high, other industries such as financial services provide examples of protecting information. Here, organizations are leveraging tools such as encryption and tokenization for data at rest and in transit to safeguard communications if they are intercepted or systems are compromised. While on its path to interconnectedness, the financial services industry realized that it is no longer typically adequate to focus solely on security to address data privacy and confidentiality risks, and that these techniques should be married with other techniques, such as data governance. Indeed, organizations should perform risk assessments across their environment, including enterprise, DSN, industrial control systems, and connected products, and use those assessments to determine or update their cyber risk strategies. Taken together, all of these approaches can help to identify where higher levels of prevention are warranted as connectivity increases.

VENDOR PROCESSING: VENDOR ACCEPTANCE AND PAYMENT IN A BROADER MARKET

Expansion of a core group of suppliers to a broader network will likely disjoint current vendor acceptance processes, as new partners could bring their own systems into the mix. Governance, risk, and compliance (GRC) software to track third-party acceptance and risk would thus need to react faster and even autonomously. Further, information security and risk management teams leveraging these applications would need to develop new policies and guidelines to adequately secure themselves against fraudulent vendors, internationally sanctioned suppliers, and subpar product distributors. These effects have been experienced in consumer open markets where counterfeit goods and fake storefronts create headaches for organizations such as eBay and Amazon.[6]

Blockchain has been suggested as a technology to help solve these woes and address potential payment process changes. The process of establishing a historical record for currency is best known in the example of bitcoin, but other organizations are exploring ways to use this new tool to determine the flow of goods from production line through layers of purchasers.[7] Creating a historical ledger that is shared by a community establishes trust and visibility, providing protection for buyers and sellers by certifying a good's authenticity, enabling the tracking of goods movements for logistical purposes, and categorizing products more specifically than by lots or batches when handling recalls or defects. In the

absence of this level of assurance of product authenticity, manufacturers may want to perform testing and certification of products to ensure adequate security before incorporating them into their environment or products.

The connecting element between these two areas, data sharing and vendor processing, is trust. Organizations may need to keep evolving their risk management to preserve integrity and remain secure when transacting information or goods, as well as strengthening their monitoring capabilities and cybersecurity operations to remain vigilant, protecting those processes when trust cannot be validated.

As they seek to do so, DSN members can learn from other sectors' approaches to managing cyber risk. The automated trading model used by financial and energy corporations, for example, is similar in many ways to the responsive, agile DSN. It contains competitive intellectual property and the keys to resources on which organizations depend to survive—all of which, as with a DSN, could be potentially vulnerable when deployed in cloud and integrated third-party relationships. This risk has been realized in the financial services arena where algorithms are being targeted internally and externally. This has led to increased security and vigilance for the software code and insider threat programs to combat internal risks, both overt (corporate espionage, sabotage, and so on) and unintended (complacency, ignorance, and so on). Indeed, vigilance could be particularly important with respect to monitoring: As manufacturers move beyond the DSN to apply Industry 4.0 technologies to production itself, cyber risks will likely only evolve and multiply.

The smart factory

Facing new cyber risks in the age of smart production

JUST as adding connectivity to the DSN introduces new risk vectors, so too does smart manufacturing. Those risks not only increase and diversify, but also possibly exponentially. Recent Department of Homeland Security publications *Strategic principles for securing the Internet of Things* and *Security tenets for life critical embedded systems* highlight the issues at hand by examining the risks associated with life-critical embedded systems manufacturers may deploy in production, both directly and indirectly.[10]

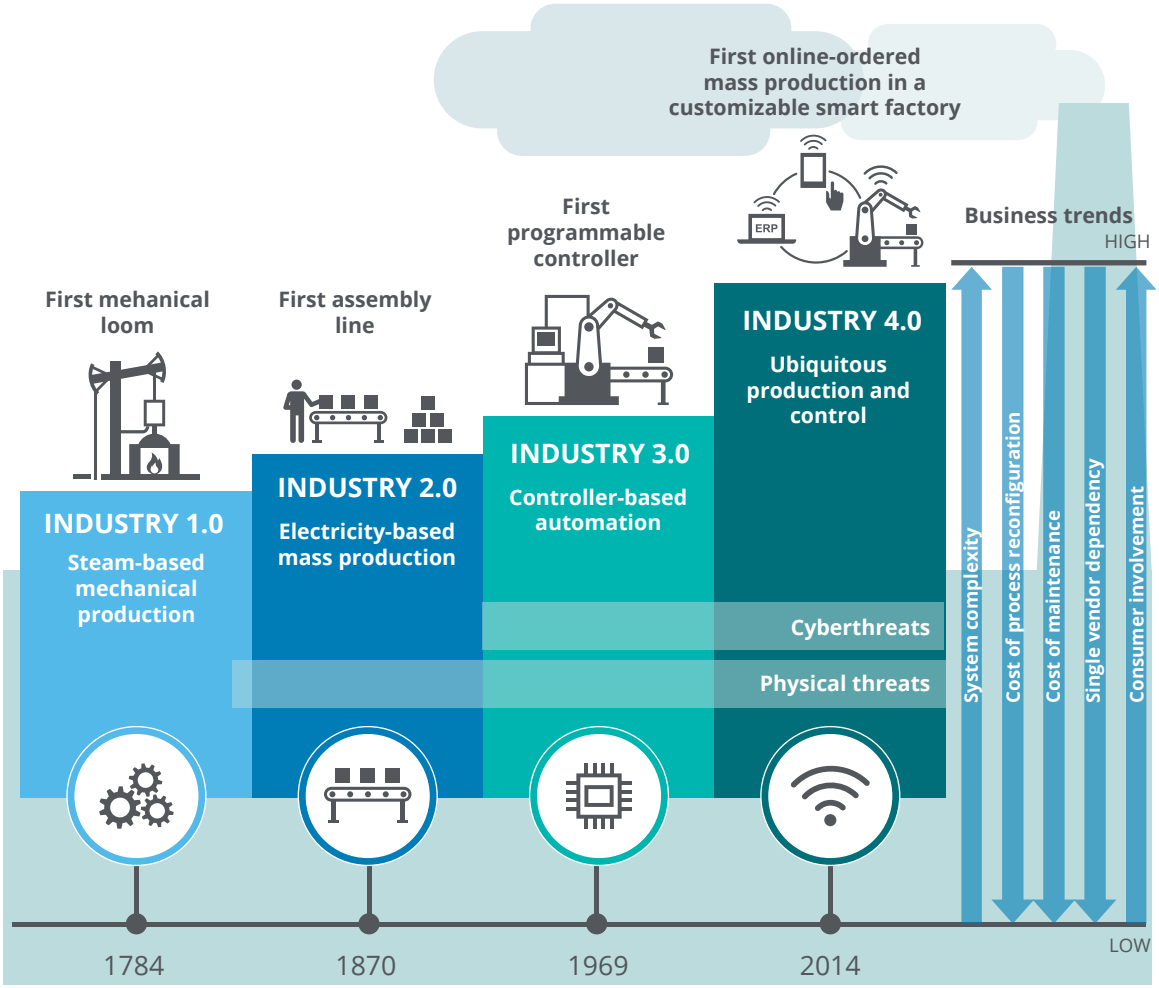
The broad definition of the term "life-critical embedded systems" means that almost any connected device, whether on the shop floor in an automated system or remotely located at a third-party contract manufacturer, should be considered a risk—even those that only peripherally or indirectly touch the production process.[11] This increased risk and dramatically expanded threat surface require a fundamental change in how security is viewed within Industry 4.0–driven manufacturing.

Connected production creates new cyber challenges

As production systems grow ever more connected, cyberthreats increase and broaden beyond those seen in the DSN. It is not hard, for example, to imagine that misused or manipulated requests for ad hoc production lines can result in financial loss, low product quality, and even safety concerns for workers. Further, connected factories may be vulnerable to shutdowns or other attacks. Moreover, evidence exists that manufacturers may not be prepared for the cyber risks their connected, smart systems present: A 2016 Deloitte-MAPI study found that one-third of manufacturers have not performed any cyber risk assessments of industrial control systems (ICS) operating on factory floors.[12]

To be sure, risks to manufacturers have existed as long as production has been mechanized, with cyberthreats augmenting and adding to physical threats as technology has progressed. But Industry 4.0 heralds the greatest leaps in cyber risk to date. The nature of these leaps is described in figure 4.

Figure 4. Progression of cyber and physical threats for each industrial revolution



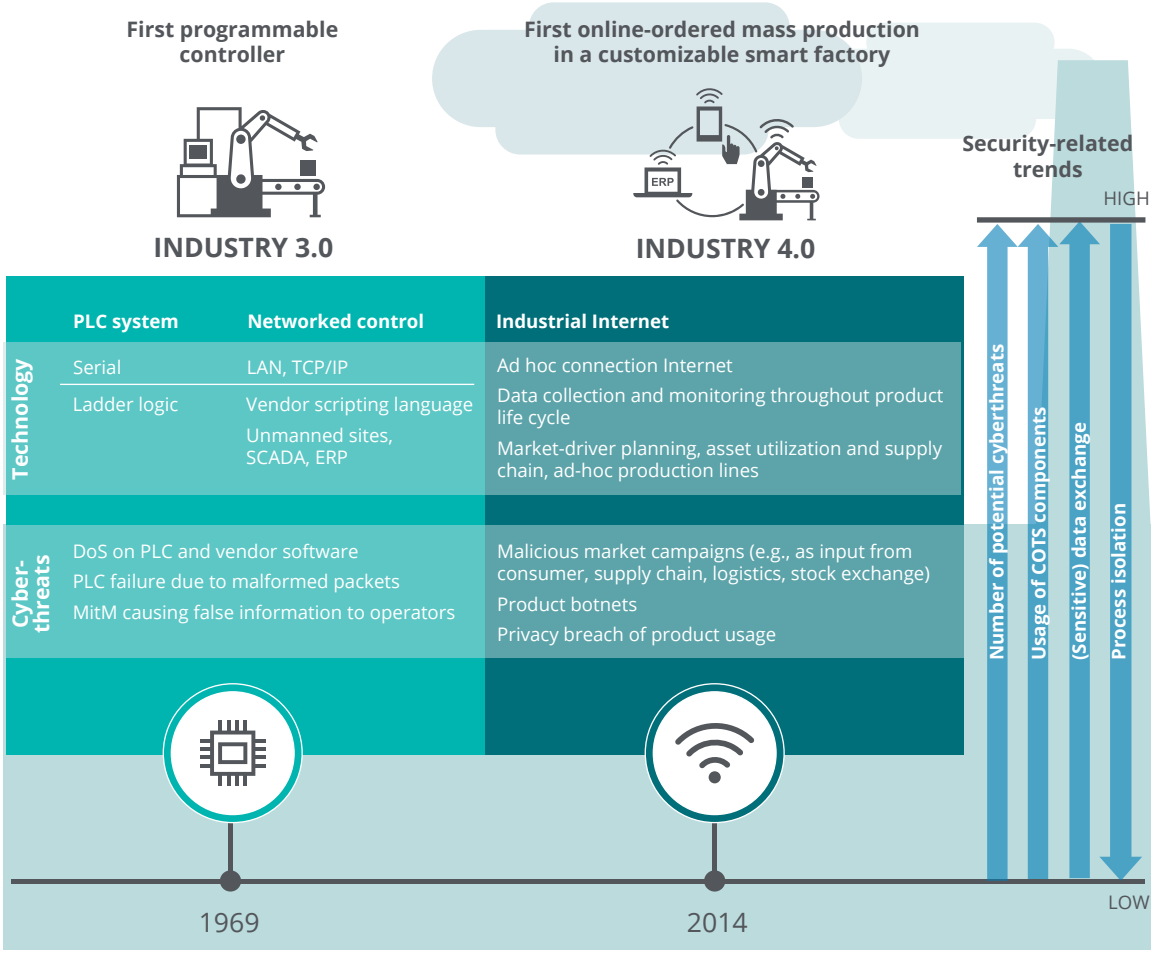
Source: Deloitte.

From an operational perspective, modern ICS environments allow engineers to deploy unmanned sites while maintaining high efficiency and resource control. They do so by using connected systems such as enterprise resource planning, manufacturing execution, and supervisory control and data acquisition systems. These connected systems can often streamline processes and make things easier and more efficient, and they have continued to evolve as systems have become more automated and autonomous (figure 5).

From a security perspective, the increased networking and usage of commercial off-the-shelf (COTS) products in ICS introduces a variety of exposure points that could be abused by threat actors. In

The potential impacts of these attacks on production, customers, manufacturers, and the products themselves may grow broader and potentially more significant.

Figure 5. Evolution of technologies and related cyberthreats in industrial control systems (ICS)



Note:

Local area network (LAN)
Transmission Control Protocol/Internet Protocol (TCP/IP)
Supervisory control and data acquisition (SCADA)
Enterprise resource planning (ERP)
Denial of Service (DoS)
Programmable logic controller (PLC)
Man-in-the-middle attack (MitM)

Source: Deloitte.

contrast to generic IT where the focus is the information, ICS security focuses on the industrial process. Therefore, the targets in the smart factory primarily focus on the availability and integrity of the *physical* process rather than confidentiality of information, as with traditional cyber risk.

Notably, however, while the basics of cyberattacks remain the same, the methods of delivering the attack become more advanced (figure 5). Indeed, as Industry 4.0 connectivity continues to proliferate across not only the digital sphere but also the physical world, the potential impacts of these attacks on production, customers, manufacturers, and the products themselves may grow broader and potentially more significant (figure 6).

Figure 6. Smart factory imperatives and risks

Production life cycle stage	Secure, vigilant, resilient categorization	Cyber imperative	Objective
Smart factory 	Vigilant	Health and safety	Ensure safety for both employees and the environment
	Vigilant, resilient	Production and process resilience/efficiency	Ensure continuous production and recovery of critical systems
	Vigilant, resilient	Instrumentation and proactive problem resolution	Protect the brand and reputation of the organization
	Secure, resilient	Systems operability, reliability, and integrity	Support the use of multiple vendors and software versions
	Vigilant, resilient	Efficiency and cost avoidance	Reduce operating costs and increase flexibility with remote site diagnostics and engineering
	Secure	Regulatory and due diligence	Ensure process reliability

Combining IT and the OT: Digital meets physical

Implementing Industry 4.0 technologies likely necessitates that manufacturers consider both the digital processes and the machinery and objects that could be impacted. This can be commonly known as uniting the IT and OT. As we examine factors that drive operational and developmental priorities of companies running industrial or manufacturing processes that involve IT and OT, several strategic imperatives and operational values can be identified, along with corresponding cybersecurity actions (figure 7).

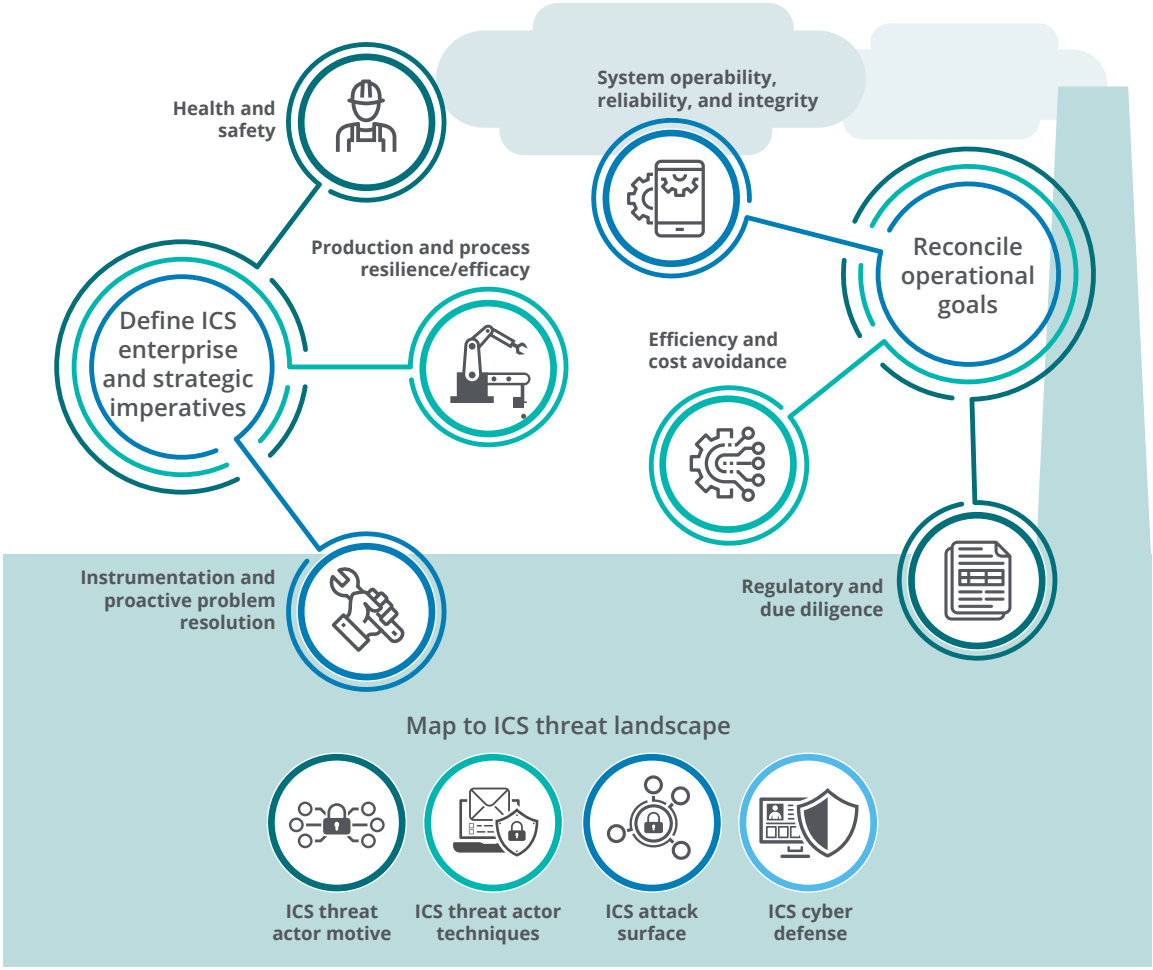
First, manufacturers are commonly driven by three strategic imperatives:

- **Health and safety**: Safety for both employees and the environment is typically paramount for every site. As technology develops, intelligent safety equipment could be upgraded in future environments.
- **Production and process resilience and efficiency**: It is often critical to ensure continuous production at all times. In practice, any production downtime reflects loss of money, but recovery of critical processes can result in greater losses, given the time to rebuild and restart.
- **Instrumentation and proactive problem resolution**: Corporate brand and reputation increasingly play a role in the global business market. In practice, malfunctions or production issues in plant sites can be critical to reputation, and changes in the environment should be acted upon to protect the brand and reputation of the organization.

Second, organizations need to respond to different operational values in their daily business:

- **Systems operability, reliability, and integrity**: To reduce the cost of ownership and ease component replacement, sites could invest in interoperable systems that support the use of multiple vendors and software versions.
- **Efficiency and cost avoidance**: Sites are continuously under pressure to reduce operating costs. In the future, businesses may invest more in COTS equipment and flexibility with remote site diagnostics and engineering.

Figure 7. Smart factory business drivers and threat landscape



Source: Deloitte.

- **Regulatory and due diligence**: Regulators require different requirements on safety and cybersecurity in ICS environments. In the future, businesses may have to invest even more in changes within the environment to ensure process reliability.

Cyber risks in the age of Industry 4.0 extend beyond the supply network and manufacturing, however, to the product itself. As products are increasingly connected—both to each other and, at times, even back to the manufacturer and supply network—organizations should realize that the cyber risk no longer ends once the product has been sold.[14]

Connected objects

Expanding risks to the physical object

By 2020, it is estimated that over 20 billion IoT devices will be deployed around the world.[15] Many of these devices may find their way into manufacturing facilities and production lines, but many others are expected to move out into the marketplace where customers, whether B2B or B2C, can purchase and use them.

The 2016 Deloitte-MAPI survey noted that close to half of manufacturers use mobile apps for connected products, while three-quarters use Wi-Fi networks to transmit data to and from connected products.[16] Use of these sorts of avenues for connectivity often open up considerable vulnerabilities. IoT device manufacturers should thus consider how to incorporate stronger, more secure software development practices into existing IoT development life cycles to address the significant cyber risk these devices often present.

This can prove challenging. Expecting consumers to update security settings, apply effective security countermeasures, update device firmware, or even change default device passwords has often proven unsuccessful. For example, an October 2016 IoT distributed denial of service (DDoS) attack via the Mirai malware showed how attackers could leverage these weaknesses to conduct a successful attack. In the attack, a virus infected consumer IoT devices such as connected cameras and televisions and turned them into botnets, bombarding servers with traffic until they collapsed and impeding access to multiple popular websites across the United States for the better part of a day.[17] Researchers identified that the compromised devices used to conduct the DDoS attack were secured with vendor default passwords and had not received required security patches or updates.[18] It should be noted that some vendor passwords were hard-coded into the device firmware, and the vendors offered users no mechanism to change those passwords. Existing industrial production facilities often lack the security sophistication and infrastructure to detect and counter such an attack once it breaks through the perimeter protection.[19]

Increasing production, increasing risk

As production facilities increase integration and deployment of IoT devices, it typically becomes even more important to consider the security risks these devices pose to manufacturing, production, and enterprise networks. Security implications of compromised IoT devices include production downtime, damage to equipment or facilities that could include catastrophic equipment failure, and, in extreme cases, loss of life. In addition, potential monetary losses are not limited to production downtime and incident remediation but can extend to fines, litigation expenses, and loss of revenue from brand damage that can persist for months or even years, well beyond an actual incident. Current approaches to safeguarding connected objects, some of which are listed below, may prove insufficient as both objects and attendant risks proliferate.

TRADITIONAL VULNERABILITY MANAGEMENT

Vulnerability management programs can effectively reduce identified vulnerabilities through scanning and patching cycles, but often multiple attack surfaces remain. An attack surface can be an open TCP/IP or UDP port or exposed technology that, while not vulnerable today, may have an unknown vulnerability waiting for an attacker to discover.

ATTACK SURFACE REDUCTION

Put simply, attack surface reduction (ASR) is the concept of reducing or eliminating these attack surfaces. ASR begins with IoT device manufacturers designing, building, and deploying hardened devices with only the most essential services exposed. The ownership of security should not lie solely with either the IoT device manufacturer or users; rather, it should be equally shared between them.

UPDATE PARADOX

Another challenge to production facilities is the so-called update paradox. Many industrial production networks are rarely updated, as it is costly for manufacturers to schedule the production downtime to do so. For some continuous-processing facilities, shutdowns and stoppages can result in the loss of expensive raw production materials.

To compound this update paradox, many of these connected devices are expected to remain in service for the next 10 to 20 years. It is typically unrealistic to assume that a device will remain secure throughout the device's lifespan without applying software patches.[20] For production and manufacturing facilities, it is important to maximize manufacturing asset utilization while, at the same time, minimizing downtime. IoT device manufacturers have a responsibility to produce IoT devices that are inherently more secure and hardened to a level where minimal attack surfaces exist, and configured to have the most secure settings using default "open" or insecure security configurations.

The same challenge that applies to connected devices within the manufacturing facility often applies to IoT-enabled consumer products as well. Smart systems grow antiquated quickly, and could potentially lead consumer objects to be more vulnerable to cyberthreats. The threat may seem small with just one object, but it widens significantly across a wide set of connected devices—witness the recent Mirai virus attack. To handle this threat, asset management and technology strategy could become more essential than ever before.

TALENT SHORTFALLS

A 2016 Deloitte-MAPI study found that 75 percent of executives surveyed believe they lacked the skilled talent resources needed to effectively implement and maintain a secure connected production ecosystem.[21] As the complexity and sophistication of attacks increase, it is becoming increasingly difficult to find the highly skilled cybersecurity talent needed to design and implement secure, vigilant, and resilient cybersecurity solutions.

The cyberthreat landscape continues to evolve, becoming more technically complex. Advanced malware, armed with zero-day exploits, that autonomously targets vulnerable devices and spreads with little human intervention is likely to overpower an already challenged IT/OT security staff. This disturbing trend highlights the need for IoT device manufacturers to produce security-hardened devices.

Taking an integrated approach to protecting devices

The IoT devices that perform some of the most critical and sensitive tasks in industry—including controlling the generation and distribution of power, water purification, chemical production and refinement, manufacturing, and automated assembly lines—are often the most vulnerable devices found on a network. As production facilities continue to reduce human intervention, the practice of protecting these devices at the gateway or network boundaries is no likely longer an effective solution (figure 8).

BUILDING CYBERSECURITY INTO THE DESIGN PROCESS FROM THE START

Manufacturers may be feeling a growing responsibility to deploy hardened, almost military-grade connected devices. Many have articulated a need for IoT device manufacturers to incorporate secure coding practices that include planning, designing, and incorporating cybersecurity leading practices from the beginning and throughout the hardware and software development life cycle.[22] This secure

Figure 8. Connected object imperatives and risks

Production life cycle stage	Secure, vigilant, resilient categorization	Cyber imperative	Objective
Connected object 	Secure	Product design	Employ secure software development life cycle to produce a functional and secure device
	Vigilant	Data protection	Maintain the safety of sensitive data throughout the data life cycle
	Resilient	Remediation of attack effects	Minimize the effects of an incident while quickly restoring operations and security

Deloitte University Press | dupress.deloitte.com

software development life cycle (S-SDLC) incorporates security gateways throughout the development process to assess whether security controls are effective, implements security leading practices, and uses secure software code and libraries to produce a functional and secure device. Many of the vulnerabilities identified by IoT product security assessments can be addressed early in the design process via S-SDLC security. It is often more costly and can be much more difficult, if not impossible, to apply security as a patch at the end of a traditional development life cycle.[23]

PROTECTING DATA FROM CONNECTED DEVICES

The vast amount of information created by IoT devices can be critical to an Industry 4.0 manufacturer. Industry 4.0–driven technologies such as advanced analytics and machine learning can then process and analyze this information and make critical real-time or near-real-time decisions based on that computational analysis. These sensitive data are not limited to sensor and process information; they may also include a manufacturer's intellectual property or even data related to privacy regulations. Indeed, close to 70 percent of manufacturers in the Deloitte-MAPI survey transmit personal information to and from connected products, while just 55 percent encrypt the information they send.[24]

The safety of sensitive data throughout the data life cycle will likely also need to be protected with the same sound security approach required to produce hardened devices. IoT device manufacturers would therefore need to develop approaches to maintain protection: not only securely store all device, local, and cloud-stored data but also quickly detect and report any conditions or activities that may jeopardize the security of those data.

Protecting cloud data storage and data in motion often necessitates the use of strong encryption, artificial intelligence (AI), and machine learning solutions to create robust and responsive threat intelligence, intrusion detection, and intrusion prevention solutions.

As more IoT devices are connected to networks, potential attack surfaces can increase, along with risk from compromised devices. These attack surfaces may not be exploitable or vulnerable today but may be easily exploited in months or years to come. Thus leaving devices unpatched and connected to the network is not likely feasible. The responsibility of securing these devices should not lie solely with the consumer or those who deploy the connected device; instead, the responsibility should be shared with the device manufacturers, who may be best positioned to implement the most effective security.

LEVERAGING AI FOR THREAT DETECTION

In August 2016, the Defense Advanced Research Projects Agency's (DARPA's) Cyber Grand Challenge (CGC) culminated with the top seven teams submitting their AI platforms in what was billed as the first "all machine" hacking competition. The CGC was announced in 2013 with the goal of identifying an AI cybersecurity platform or technology that can

scan networks, identify software vulnerabilities, and apply patches without human intervention. DARPA envisions AI platforms being utilized to dramatically reduce the lengthy time required by humans to identify vulnerabilities and develop software security patches to occur in real or near-real time, thus reducing cyberattack risk.

A truly vigilant threat detection capability may need to leverage the power of AI to identify the proverbial needle in a haystack. Existing signature-based threat detection technologies, inundated with the ever-increasing data produced by IoT devices, could be pushed to their limits while trying to reassemble data streams and perform stateful packet inspection. Even if these signature-based detection technologies can keep up with increasing traffic, they are still limited in their ability to detect activities within their signature database.

The combination of ASR, S-SDLC, data protection, secure and hardened device hardware and firmware, machine learning, and use of AI to power real-time responses to threats may be critical in moving forward with a secure, vigilant, and resilient approach to Industry 4.0–enabled devices. The failure to address security risks, such as those demonstrated by Stuxnet and Mirai malware exploits, and to manufacture hardened and secure IoT devices may result in a cyber landscape where attacks to critical infrastructure and attacks to manufacturing are crippling and commonplace.[25]

BEING RESILIENT WHEN ATTACKS INEVITABLY HIT HOME

The careful application of secure and vigilant capabilities can produce an extremely hardened target that can be an effective deterrent to most attackers. It is important to note, however, that while organizations can and should decrease their risk to cyberattack, no organization is ever fully immune. Being resilient to attack begins with accepting the fact that someday the organization could fall victim to an attack, and then carefully crafting the reaction.

There are three important phases to consider when addressing resilience: readiness, response, and recovery.

- **Readiness**. An organization should be well prepared to efficiently deal with all aspects of an incident. Clearly defined roles, responsibilities, and actions should be identified. Thoughtful preparation, using crisis simulations, incident walk-throughs, and Wargaming exercises, can help an organization identify gaps and apply effective remediation steps before a real incident occurs.
- **Response**. Management's response should be well planned and effectively communicated throughout an organization. A poorly executed response plan can escalate the impact of an incident and result in increased downtime, lost revenue, and damage to an organization's reputation. These effects can last well beyond the actual incident.
- **Recovery**. The steps needed to return to normal operations and limit the damage to an organization should be well planned and practiced. Post-event analysis should include incorporating lessons learned into subsequent incident response plans.

A resilient organization should minimize the effects of an incident while quickly restoring operations and security. Preparing for an attack, understanding what to do when you are attacked, and quickly remediating the effects of the attack should be completely addressed, thoughtfully planned, and fully exercised.

Being secure, vigilant, and resilient in the age of Industry 4.0

ZEROES and ones—the bits that drive connected companies today—are transforming manufacturing throughout the value chain, from the supply network to smart factory to connected object. As the adoption and breadth of use of connected technologies increase, cyber risks may grow and change, and will likely look different for each stage of the value chain and each organization. Each organization should adapt to the industrial ecosystem in the way that best fits their needs.

There is no simple fix or single product or patch that an organization can apply to address the cyber risks and threats presented by Industry 4.0. Connected technologies already support critical business processes today, and these processes will likely only grow more connected, integrated, and vulnerable in the future. Organizations may thus need to rethink their business continuity, disaster recovery, and response plans to accommodate the increasingly complex and ubiquitous cyber environment.

Regulation and industry standards are often reactive, and "compliance" often represents the minimum security posture. This does not usually achieve full security across the breadth of technologies in use—a particular challenge, given that disruptors need only find the single weakest point to gain successful entry into an organization's systems. This challenge may only continue to grow: Increasing connectivity and the need to gather and process real-time analytics may continue to introduce vast numbers of connected devices and huge amounts of data that require protection.

The breadth of risks requires a secure, vigilant, and resilient approach to understand the dangers and address the threats:

- **Be secure**. Take a measured, risk-based approach to what is secured and how to secure it. Is your intellectual property safe? Is your supply chain or ICS environment vulnerable?
- **Be vigilant**. Continually monitor systems, networks, devices, personnel, and the environment for possible threats. Real-time threat intelligence and AI are often required to understand harmful actions and quickly identify threats across the multitude of new connected devices that are being introduced.
- **Be resilient**. An incident could happen. How would your organization respond? How long would it take to recover? How quickly could you remediate the effects of an incident?

As industry moves to capture the business value that comes with Industry 4.0, the need to address the cyber risk landscape with a secure, vigilant, and resilient response has likely never been greater.

ENDNOTES

1. Kim Zetter, "An unprecedented look at Stuxnet, The world's first digital weapon," *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
2. For further information about Industry 4.0, see Brenna Sniderman, Monika Mahto, and Mark Cotteleer, *Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises*, Deloitte University Press, February 22, 2016, https://dupress.deloitte.com/content/dupress/dup-us-en/focus/industry-4-0/manufacturing-ecosystems-exploring-world-connected-enterprises.html.
3. For further information about digital supply networks, see Adam Mussomeli, Stephen Laaper, and Doug Gish, *The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains*, Deloitte University Press, December 1, 2016, https://dupress.deloitte.com/content/dupress/dup-us-en/focus/industry-4-0/digital-transformation-in-supply-chain.html.
4. Ibid.
5. Bridget McCrea, "The evolution of supply chain collaboration software," *Logistics Management*, September 2015.
6. Aron Hsiao, "Top ten risks eBay sellers face," *Balance*, January 8, 2016, https://www.thebalance.com/top-ten-risks-ebay-sellers-face-1140349.
7. Harriet Green, "Serving up a better burger: How IoT and blockchain will reinvent the global supply chain," *Venture Beat*, October 30, 2016, http://venturebeat.com/2016/10/30/serving-up-a-better-burger-how-iot-and-blockchain-will-reinvent-the-global-supply-chain/.
8. Stuart Trouton, Mark Vitale, and Jason Killmeyer, *3D opportunity for blockchain: Additive manufacturing links the digital thread*, Deloitte University Press, November 16, 2016, https://dupress.deloitte.com/content/dupress/dup-us-en/focus/3d-opportunity/3d-printing-blockchain-in-manufacturing.html.
9. Judith Evans, "Cyber criminals target trading algorithms," *Financial Times*, February 22, 2015, https://www.ft.com/content/f8556c92-b1d9-11e4-8396-00144feab7de.
10. US Department of Homeland Security, *Strategic principles for securing the Internet of Things*, November 15, 2016; and *Security tenets for life critical embedded systems*, November 20, 2015.
11. The term "life-critical embedded system" extends to any embedded system across all industries that need to protect human life, prevent loss or severe damage to equipment, and prevent environmental harm.
12. Trina Huelsman et al., *Cyber risk in advanced manufacturing*, Deloitte and MAPI, 2016, https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html.
13. Sniderman, Mahto, and Cotteleer, *Industry 4.0 and manufacturing ecosystems*.
14. Brenna Sniderman et al., *The design of things: Building in IoT connectivity: The Internet of Things in product design*, Deloitte University Press, September 12, 2016, https://dupress.deloitte.com/content/dupress/dup-us-en/focus/internet-of-things/connected-products-designing-for-internet-of-things.html.
15. Ron van der Meulen, "Gartner says 6.4 billion connected 'things' will be in use," *Gartner*, November 10, 2015, http://www.gartner.com/newsroom/id/3165317.
16. Huelsman et al., *Cyber risk in advanced manufacturing.*
17. Nicky Wolf, "DDoS attacks that disrupted Internet was largest of its kind in history, experts say," *Guardian*, October 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

18. Alex Hern, “Chinese webcam maker recalls devices after cyberattack link,” *Guardian*, October 24, 2016, https://www.theguardian.com/technology/2016/oct/24/chinese-webcam-maker-recalls-devices-cyberattack-ddos-internet-of-things-xiongmai.

19. Matthew E. Luallen and Barbara Filkins, *Results of SANS SCADA Security Survey*, SANS Institute, February 2013, https://www.sans.org/reading-room/whitepapers/analyst/results-scada-security-survey-35135.

20. Sniderman et al., *The design of things.*

21. Huelsman et al., *Cyber risk in advanced manufacturing*.

22. Broadband Internet Technical Advisory Group, *Internet of Things (IoT) security and privacy recommendations*, November 2016, http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

23. Sniderman et al., *The design of things*.

24. Huelsman et al., *Cyber risk in advanced manufacturing*.

25. Nicole Perlroth, “Hackers used new weapons to disrupt major websites across U.S.,” *New York Times*, October 22, 2016, http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

ABOUT THE AUTHORS

RENÉ WASLO

René Waslo is a cyber risk principal in the Advisory practice of Deloitte & Touche LLP, with a focus on cyber strategy development, threat intelligence, incident response, data loss prevention, application integrity, identity and access management, and data security. Her primary client focus is on Deloitte's multinational clients in the Chemicals and Specialty Materials, and Technology, Media, and Telecommunications practices.

TYLER LEWIS

Tyler Lewis is a cyber risk senior manager in the Advisory practice of Deloitte & Touche LLP, focused on leveraging technology in conjunction with business insight and cybersecurity expertise to improve operational capabilities, governance, and risk management within the consumer products marketplace.

RAMSEY HAJJ

Ramsey Hajj is a senior manager in the Cyber Risk Services practice specializing in security architecture around ICS and identity and access management implementation, and assessment services with a focus on manufacturing and distribution clients. He brings over 18 years of technical experience using emerging technologies to solve business problems. He holds an MSc in information systems and has been a CISSP since 2003.

ROBERT CARTON

Robert Carton is a specialist master in the Advisory practice of Deloitte & Touche LLP and serves as a subject-matter expert in automotive and IoT device security. He has over 18 years of cybersecurity experience and helps clients identify solutions for their most complex cybersecurity challenges to include enterprise and connected device security.

ACKNOWLEDGEMENTS

The authors would like to thank **Brenna Sniderman** of Deloitte Services LP for her contributions to this article.

CONTACTS

Sean Peasley
Partner
Deloitte Advisory
Deloitte & Touche LLP
Mobile: +1 714 334 6600
speasley@deloitte.com

René Waslo
Principal
Cyber Risk Services
Deloitte & Touche LLP
Mobile: +1 412 400 1638 | Office: +1 412 338 7302
rwaslo@deloitte.com

Tyler Lewis
Senior manager
Cyber Risk Services
Deloitte & Touche LLP
Mobile: +1 214 504 4902 | Office: +1 214 840 1072
tylewis@deloitte.com

Ramsey Hajj
Senior manager
Cyber Risk Services
Deloitte & Touche LLP
+1 561 809 2314
rhajj@deloitte.com

Robert Carton
Specialist master
Cyber Threat Management
Deloitte & Touche LLP
Office: +1 855 816 2404 | Mobile: +1 858 335 9183
rcarton@deloitte.com

 Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

About Deloitte