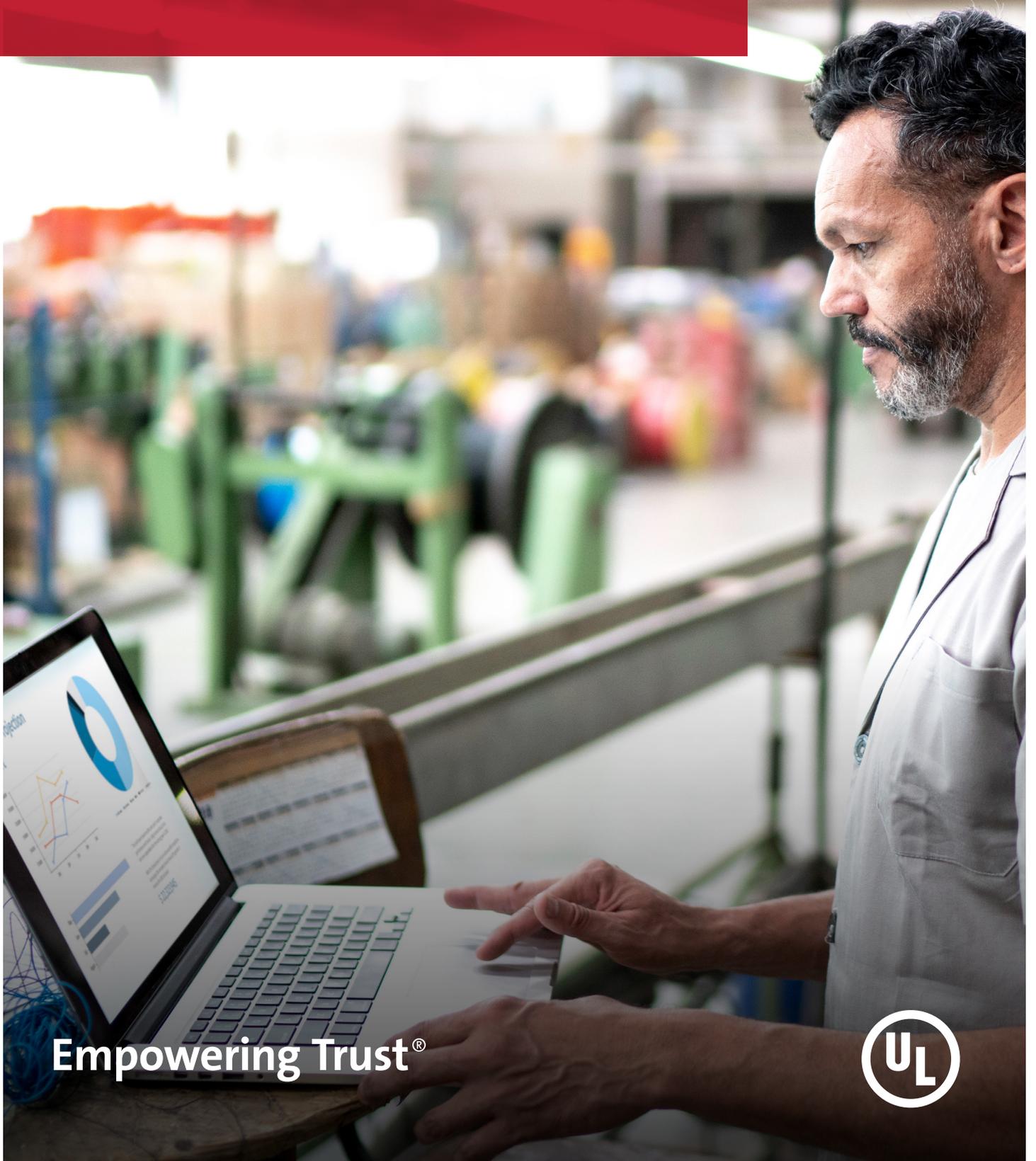


Leveraging Cybersecurity for Industry 4.0 into a Business Advantage



Empowering Trust®



Executive summary



While much has been written about Industry 4.0 and the Industrial Internet of Things (IIoT), its supply chain function has become increasingly more complex. In this respect, integrating processes among supply chain members is essential.

Today, through the emergence of the fourth industrial revolution — better known as Industry 4.0 — there are ample opportunities to integrate and connect companies and their respective resources in order to increase performance in terms of time, money and efficiency. In this whitepaper, Industry 4.0 refers to the growing use of technologies (especially digital technologies for automation and communication) to make the industry more productive, efficient and competitive.

In line with Industry 4.0, most firms are now experiencing increased supply chain digitization, where they are moving toward a completely integrated sequence of planning and production solutions that work in tandem to create a more visible supply stream across each touch point of the value chain. Of course, there are many more examples, including IIoT, which increasingly touches almost every point of a modern supply chain.

All these technologies have things in common; they are all digital, they are designed to streamline and optimize industrial and related processes, and they drive up the efficiency, accuracy, transparency, accountability, flexibility and agility of the business. It is little wonder that Industry 4.0 is moving at such speed.

However, the digital supply chain also massively extends the area of digital real estate available for cybercriminals to hack, increasing the attack surface. Instead of the few access points that a relatively closed network might present, the digital supply network generates many

potential points of vulnerability, perhaps spread across a wide geography and accessible through multiple individuals, systems or devices.

The real impact of Industry 4.0 on the supply chain is difficult to quantify. The world has become dependent on industrial systems for everyday digitized processes. Subsequently, this reliance can incur cybersecurity vulnerabilities if such systems are compromised using complex cyber or physical hacking scenarios.

Complexity is the enemy of security. As supply chains become more complex through the interconnected nature of increased digitization, keeping the security to an acceptable level becomes rapidly more difficult.

This white paper aims to identify and analyze these vulnerabilities to enable manufacturers to plan long-term, sustainable business strategies, including leveraging cybersecurity as a business advantage.

Challenges in supply chain security

Traditional manufacturing industries, which are currently at various stages of Industry 4.0 adoption, rarely have defined security programs in place and generally lack comprehensive programs that consider security and safety in conjunction.

Given the commercial value of industrial data and the possibility of industrial espionage, industrial sites are attractive targets for cybercriminals. The industry is also at risk from attacks that are less likely elsewhere. Data traveling along the supply chain, e.g. from manufacturer or maintenance personnel to device, can be intercepted, changed or redirected, leading to equipment failure or data breach, compromised outputs or even plant closure. Devices can be counterfeited or their software tampered with, leading to stolen access credentials and thus control of equipment.



The challenges for industrial businesses

For the manufacturing industry, digital transformation presents specific challenges. For example:

- Equipment has a high capital cost and an extensive life cycle (measured in decades), making 'replacement' upgrades to fix issues unaffordable for most. Therefore, digital transformation must be incremental.
- Many industrial sites must integrate legacy systems into Industry 4.0 cybersecurity measures, possibly for a limited time (depending on equipment life cycles). This problem is exacerbated by the range of standards and protocols found in industrial applications, many of which were never designed with security in mind.
- Elements of the manufacturing supply chain may be at different points in their digital transformation process, which can make integration difficult.
- Cybersecurity of third-party providers must be assured as some, e.g. maintenance or original equipment manufacturers (OEMs), require direct access to plants and systems.
- A culture shift is required: manufacturing has traditionally prioritized the protection of people and on-premises objects. Augmenting that focus to include cybersecurity can be a significant change.
- The factory requires a customized form of cybersecurity that takes into account the standard monitoring, obscuring and blocking approaches but extends to cover specialized equipment and operations.
- Designing cybersecurity into manufacturing elements, such as industrial equipment, is an emerging discipline with its own challenges.
- The addition of cybersecurity measures can, in some cases, affect operational processes or outcomes.

A lack of security has the potential to significantly affect business continuity, reliability and product quality. Industry 4.0 is no exception given the criticality of related operations and the associated impact on safety.

Building a solution

When it comes to securing Industry 4.0 data and assets, roles and approaches can vary, particularly according to each firm's role and its place in the supply chain. For example:

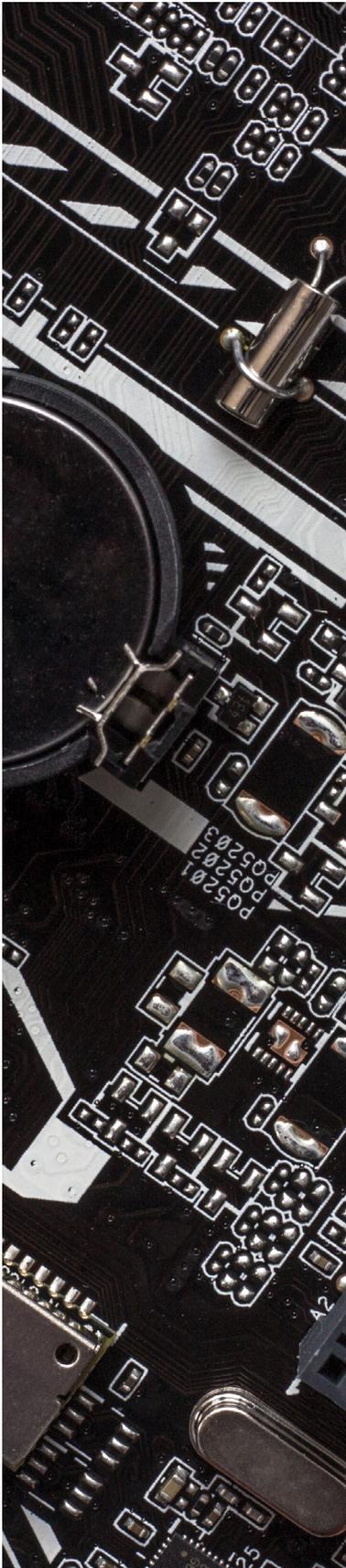
Asset owners will generally focus on the security of operations, business continuity and risk management across the supply chain.

Those responsible for system integration will be primarily concerned with the security and resilience of their systems and processes, along with the required capabilities. Their role somewhat overlaps with maintenance managers, who must also consider the life cycles of plant (which means looking ahead over decades) and the continued integration of security measures as equipment assets and requirements change.

Finally, component and product manufacturers will not only wish to secure the commercial advantage that comes from a demonstrably secure supply chain but also prove that security is built into their products.

Cybersecurity is a shared responsibility. When we talk about IoT and Industry 4.0, with complex supply chains and several actors involved, this becomes even more critical. As there are many players and thus interdependencies, collaboration is vital to secure Industry 4.0. Since many supply chain actors may be subject to different national legislative frameworks, security incidents may occur at various tiers and stages. Such incidents may be related to the exchange of goods, services or information, resulting in an increase of errors and risks across the whole supply chain. Determining the source of the problem in these complex supply chains has become very difficult. This calls for the use of security standards and solutions that are more commonly applicable for the different actors involved, regardless of their geography.





Meeting the standards

While each sector and firm will have its own challenges, Industry 4.0 implementation – particularly, cybersecurity within that context – has now matured to the point that regulations, standards and frameworks have been established.

Examples of regulations or laws that currently apply to Industry 4.0 cybersecurity in various parts of the world include:

- NIS Directive (EU)
- General Data Protection Regulation (EU) (in the U.K., the requirements of GDPR have been rolled into the Data Protection Act and thus remain applicable)
- Energy Policy Act (U.S.)
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- IoT Security Law SB-327 (California, U.S.)
- NERC Critical Infrastructure Protection (NERC - CIP) Standards (U.S.)
- Executive Order (EO) 13920 “Securing the United States Bulk-Power System” (U.S.)
- S.3688 Energy Infrastructure Protection Act (proposed – U.S.)
- Cybersecurity Act Singapore
- People’s Republic of China Cybersecurity Law 2016

Given the global nature of today’s markets, it is imperative that organizations not only prove that their products and their processes provide robust security but that they also meet global regulatory requirements. This, in turn, demands a system that has security built in, that is regularly tested and verified against established standards.

When paired with independent security assessments, standards can help organizations, as well as their suppliers and vendors better navigate the regulatory requirements, procurement and quality assurance processes. This is best achieved by demonstrating the trustworthiness of their security practices for their products, processes and entire systems through independent assessment.

Leveraging independent security assessors can also help manage third-party risks in your supply chain, specifically addressing security of suppliers and vendors, and facilitating third-party risk management planning and implementations. NIST predicted that 98% of manufacturers will experience a supply chain disruption in the next two years, the majority of which will be caused by supply chain cybersecurity issues. Like many facets of cybersecurity, third-party risk management is both crucial and subject to frequent change. Achieving high maturity and a stable, resilient security posture is the primary concern of today’s CISOs and leadership team members, and supply chain cybersecurity is a crucial part of that.

IEC 62443- instilling cybersecurity rigor for different actors in the supply chain

It's been noted that there is a need for harmonization of security standards within Industry 4.0, and this is where the international standard IEC 62443 comes into play. Created to lay the foundation of cybersecurity robustness, the IEC 62443 family of standards assures the security of the industrial automation and control systems (IACS) that support Industry 4.0. It provides a systematic and practical approach for firms to use to secure industrial systems and covers all aspects from risk assessment to operations.

Additionally, IEC 62443 covers:

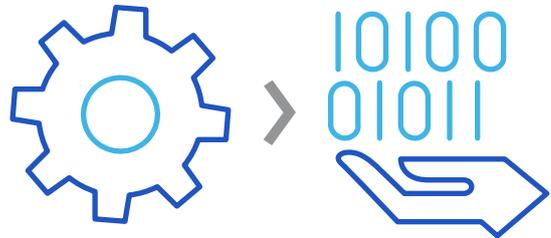
- Secure product development and maintenance processes
- Security for components, products and systems
- Security architecture and organizational process for systems in operation

General	IEC TS 62443-1-1 Concepts and models	IEC TR 62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC TR 62443-1-4 IACS security lifecycle and use cases	
Policies and procedures	IEC 62443-2-1 Security program requirements for IACS asset owners	IEC 62443-2-2 IACS protection levels	IEC TR 62443-2-3 Patch management in the IACS environment	IEC 62443-2-4 Security program requirements for IACS service providers	IEC TR 62443-2-5 Implementation guidance for IACS asset owners
System	IEC TR 62443-3-1 Security technologies for IACS	IEC 62443-3-2 Security risk assessment and system design	IEC 62443-3-3 System security requirements and security levels		
Component	IEC 62443-4-1 Secure product development lifecycle requirements	IEC 62443-4-2 Technical security requirements for IACS components			

The various standards of the IEC 62443 family are dedicated to manufacturers and system integrators, as well as end users. For component and product manufacturers, compliance to IEC 62443 can help demonstrate the security of your systems and components and enhance your market position. For Industrial Control System (ICS) integrators and users of control systems, compliance to IEC 62443 effectively achieves increased brand protection and a greater competitive advantage. This means that the value of IEC 62443 certification, particularly when provided by a trusted third-party certifier, extends beyond the factory floor and can be used to help validate the integrity of security measures throughout the supply chain.



The need for expertise

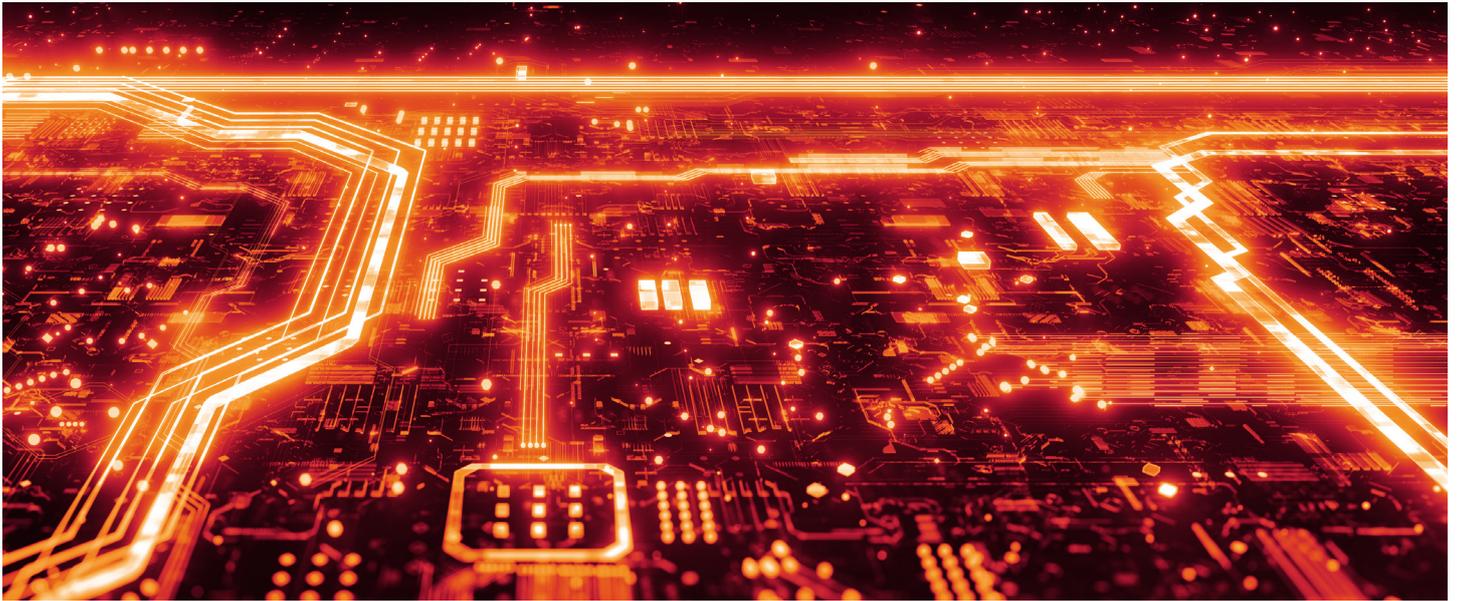


Given the evolving nature of both Industry 4.0 and IIoT, along with the constant advances in technology and the increasing willingness of authorities to strictly regulate security, Industry 4.0 security systems must be continuously monitored and upgraded. They must deal with diverse plant, technological changes and evolving threats – over decades.

All of this to the backdrop of increasingly stringent regulations.

In many cases, the knowledge required to do this will exceed the capabilities of in-house IT staff and therefore it seems likely that industrial cybersecurity will rapidly become a discipline in its own right. Companies will likely be recruiting on that basis or working with expert third-party firms to test and verify their cybersecurity arrangements – for their own equipment, supply chain integrity and manufactured items.

Working with a respected and expert third-party certifier to assess, test and certify their cybersecurity protocols not only provides peace of mind but may also bring trust and confidence for customers, prospective business partners and other stakeholders, making them more likely to favor the firm, product or brand.



Implications of the shifting cyber-risk landscape

The industrial world stands at an interesting point in its history. Industry 4.0 brings great opportunity but also substantial risk. If manufacturers can mitigate risk appropriately, the potential gains can be quite significant.

The value of data and digital communications across the industrial enterprise is becoming clear. When properly applied, digital transformation via Industry 4.0 and Industrial Internet of Things (IIoT) can:

- Optimize productivity, reduce downtime and cut costs.
- Generate meaningful insights into customer behaviors and preferences that can translate into new product lines and better customer service.
- Streamline the supply chain and operational processes.
- Integrate data from legacy systems to enhance operations across departments throughout the enterprise, from the C-suite to the factory floor. This will generate comprehensive and reliable data sets.
- Assure the accuracy of data that informs strategic and operational decisions

- Provide managers with a 24-7-365 view of all data and the security of knowing what data they hold and where it is
- Facilitate regulatory compliance and documentation of compliance
- Enhance the business's reputation for reliability, security and quality

However, Industry 4.0 also faces unique challenges through the requirements of high availability, costly technical debt and legacy systems, and the need to provide safe working environments. Building out a mature security posture is difficult for the most advanced IT company, and the difficulty of doing this in an industrial environment must be recognized.

This does not abrogate the need for action on security, of course, but it does speak to fact that Industry 4.0 is not about IT security, and cannot always easily be solved by applying the same rules that apply in commercial environments.



In short: by engaging. Industry 4.0 cannot be secured via silos; it is an ideal focused on transparency, integration and sharing of data across departments and disciplines. Firms must map their data and its journey; they must collect this data at multiple points, aggregate it across a range of sites and operations, and protect it where necessary. Only then can the true value of that data be realized.

Cybersecurity, in an Industry 4.0 business as much as any other, is a board-level, strategic issue. Business plans must have cyber resilience built in, and the need for addressing security must be understood and driven from the top down.

The business must strategize its approach and engage with staff to communicate cultural change. All must perceive the network/IIoT infrastructure as a single asset to be managed and mined for value, rather than a collection of various roles and departments. Only when staff understand the business as a network, in which all devices and potential attack points must be secured and updated regularly, even those deemed obsolete or in far-flung parts of the business, can a culture of IIoT cybersecurity grow. Security responsibilities must be embedded across the organization, not left entirely to IT.

The security of Industry 4.0 is not an IT problem. It is a companywide issue that often, but not always, has IT solutions that need to be applied.

Of course, there are common-sense steps the business can take to secure its network and connected systems – such as minimizing access rights, using both edge computing and cloud as appropriate, automation of security tasks, robust authentication protocols – but ultimately, new recruits or third-party expertise may also be needed. Cybersecurity in this area is continually evolving as are the threats it tackles, and industry faces specific issues that may exceed the scope of a standard IT department. A specialist third party can advise on best practices, share practical experience and certify security quality on an ongoing basis.



The value of cybersecurity to manufacturing is obvious, but its role as a business asset is frequently overlooked. This is unfortunate because, just as poor security can devastate a firm's reputation, good security can promote it.

Customers and partner organizations are increasingly aware of cybersecurity issues and make choices based on that awareness. A firm with a reputation for high standards in this area – ideally bolstered with regular and documented testing, evaluation and upgrading – is likely to have the advantage.

This issue is particularly crucial for businesses looking to partner with manufacturers – for example, in the virtual or smart factory – since they know that their reputation can be tainted or enhanced by those they work with.

Robust and proven cybersecurity can also aid recruitment, drive down financing costs e.g. insurance and extend commercial opportunities.



Bringing it all together

It is now imperative for manufacturers to adopt the Industry 4.0 model, and in most cases, that means joining the IIoT. Information must be shared for industry to thrive. And if that information is secured, that is good news for everyone.

Fortunately, protocols and standards now exist that help define what is required. These are invaluable for all firms, regardless of how far they have come in their digital transformation journey. Using IEC 62433 as the gold standard allows a business to systematically and practically embed robust cybersecurity within Industry 4.0, reassuring stakeholders that the company has optimized its operations while enhancing and securing the interests of all parties, from supply chain partners to end users.

To learn more, visit [UL.com](https://www.ul.com) or email us at imsecurity@ul.com.



UL.com

UL and the UL logo are trademarks of UL LLC © 2021.

Distribution Number (e.g., MMY)