KPMG

IIoT future state development

Safely embracing the Industrial Internet of Things (IIoT)

KPMG Switzerland

kpmg.ch

'Smart factories' are forging a revolution that's redefining the way things are produced

The IIoT is being heralded as a paradigm shift that will transform the way things are produced. Beyond delivering crucial new business benefits and competitive advantages, the IIOT will require organizations to adopt strategic approaches to effectively manage emerging new cyber security risks. In the article below, KPMG provides an overview of what's unfolding and some insights on how businesses should be approaching the revolutionary changes — and new risks — that are emerging around them.

With the Internet of Things (IoT) poised to create an unprecedented explosion of smart device connectivity — connecting billions of internet products and generating an endless array of data — the application of IoT concepts to industrial environments is forging a revolution of its own that will transform the way things are made.

The IIoT — automation and data exchange in manufacturing technologies — is the primary force behind what's being called the fourth industrial revolution or Industry 4.0, the creation of 'smart factories' that combine cyber-physical systems, the IoT and cloud computing.

Industrial organizations are already turning to the IIoT for real-time access to endless amounts of operational data and new analytics capabilities, all delivered at unprecedented levels of speed, accuracy and efficiency. Immense new production, operational and supply-chain advantages are rapidly emerging for businesses amid vastly improved connectivity, information sharing, scalability and time and cost savings across every automated work process. From executive offices and production floors to suppliers and other stakeholders, networks of emerging smart devices are breaking down traditional data silos and instantaneously connecting people, processes and technologies.

But as the IIoT, like the Internet of Things, opens an uncharted new frontier of enterprise-wide connectivity, automation, data and results, it becomes critical for organizations to understand what's in store in terms of the emerging cyber security risks that will need to be managed.

Today's corporate and industrial networks are relatively contained, manageable and predictable. But the IIoT transforms the risk and threat landscape, as industrial automation and control systems — once isolated and secure — are increasingly connected to corporate networks and the internet. Individual devices across enterprise Information Technology (IT) and Operational Technology (OT) networks — from smart digital equipment and tools to robots, vehicles and more — will present potential new pathways to cyber attack, including malicious data infiltration, denial of service (DoS) attacks and devastating proliferation of malware or viruses.

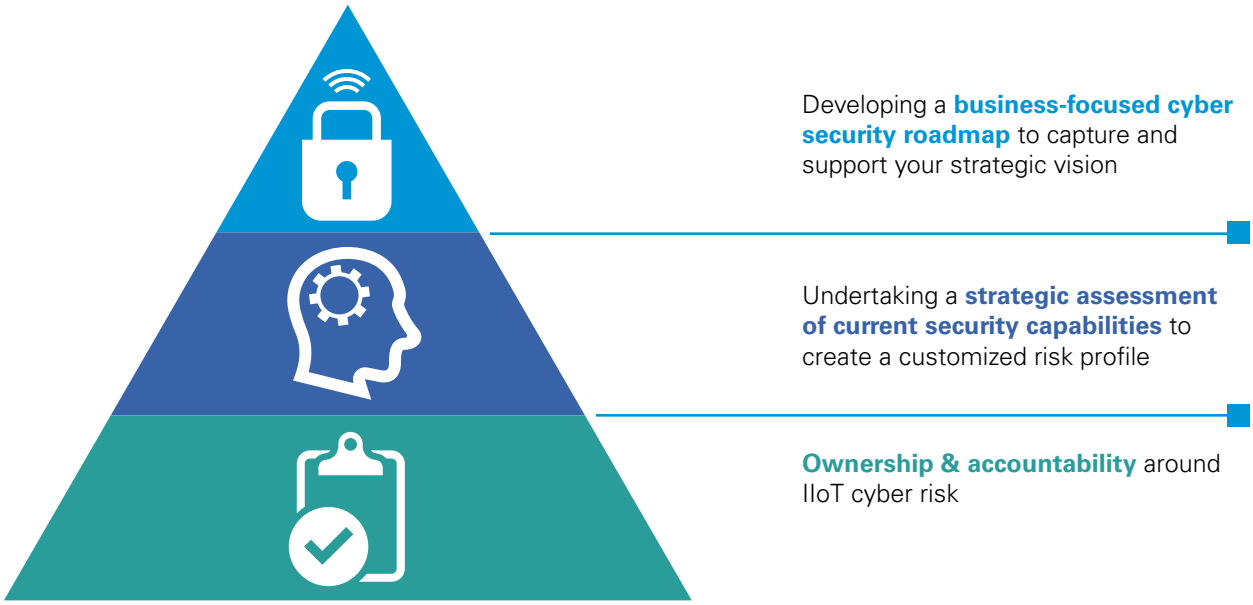
Businesses are facing new challenges on the cyber security front

As the IIoT environment explodes to create Industry 4.0 and all of its anticipated benefits and competitive advantages, organizations will also need to adopt strategic approaches and innovative architectures that foster reliable, safe, secure work environments. To that end, organizations should already be addressing some key questions about IIoT security, including what their immediate priorities are for IIoT capabilities, the level of automation needed for machine-to-machine communication, and the appropriate security program and architecture required to secure the IIoT environment.

It's also important for businesses to quickly understand that IIoT cyber security is not simply a new problem for the IT team or the OT folks to manage but an overarching business issue that warrants the full attention of senior leaders. Executives and boards can therefore begin acting as 'agents of change'

on the IIoT front today, becoming fully informed and driving collaboration across the enterprise to produce appropriate new cyber security measures.

KPMG's approach to developing a secure IIoT future state combines a sound understanding of your business objectives with marketing-leading knowledge of emerging IIoT threats and vulnerabilities. We work closely with clients to create a unique IIoT security strategy and architecture that minimizes risk and supports your organization's mission within a stable and predictable environment.



We take a 'modular approach' to each security solution, precisely identifying and mapping out logical, sequential steps that produce increasing levels of IIoT cyber security. Our strategy on every project therefore includes: determining ownership and accountability around IIoT cyber risk; undertaking a strategic assessment of current security capabilities to create a customized risk profile; and developing a business-focused cyber security roadmap to capture and support your strategic vision. This includes collaboration with stakeholders to identify gaps in their ecosystems that could inhibit your security program.

With our help, companies are replacing uncertainty with confidence in their industrial cyber security strategies and embracing new opportunities without fear of a crippling cyber event as Industry 4.0 unfolds.

Where to begin? As your organization faces the challenge of implementing IIoT, begin by exploring some key questions

- What are your organization's immediate priorities for IIoT capabilities?
- What level of control and automation will your M2M communications technology perform?
- How will IIoT data be collected, stored and transmitted and into what classification category will the data fall?
- Do proven technologies exist for applications under consideration?
- How will M2M communications technology address challenges such as data encryption, network access control and signal interference?
- What security mechanisms, if any, are being provided with IIoT-enabled devices and are you receiving current threat and vulnerability information for each?
- What external factors (environmental, regulatory, etc.) might affect reliable data transmission from one end point to another?
- Have you considered both cyber security and physical security for this deployment?
- What ongoing improvements, updates and maintenance will you conduct or receive from vendors?

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Matthias Bossardt
Partner, Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Roman Haltinner
Director, Cyber Security

+41 58 249 42 56
rhaltinner@kpmg.com

Michael Nordhoff
Manager, Cyber Security

+41 58 249 40 89
mnordhoff@kpmg.com