IIoT cyber security simulation

Prepare for cyber incident response in the Industrial Internet of Things (IIoT)

KPMG International

kpmg.com

> “In the Industrial Internet of Things (IIoT) era, visionary concepts, automation technologies and capability models are integrated to generate new operational intelligence and industrial insights. A robust approach to IIoT cyber security is imperative to drive business value and efficiencies. Are you prepared for a cyber incident? KPMG member firms can help you with this challenge.”

How to know you're prepared

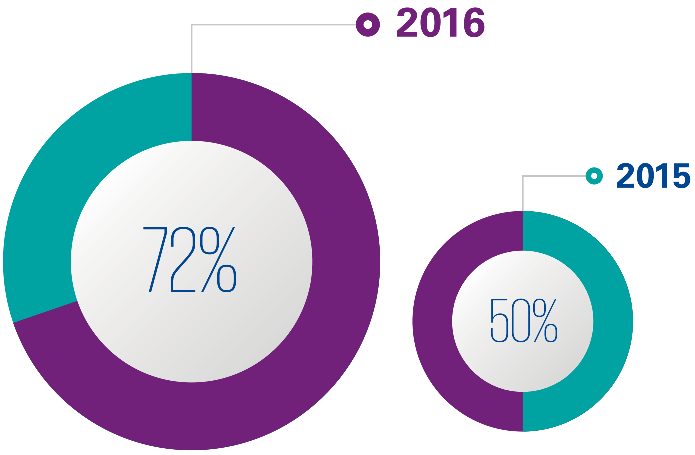
Industrial control systems developments

Economies and societies around the globe depend on the uninterrupted operation of critical infrastructures and their services. Industrial control systems (ICS) are crucial for the functioning of key processes in most critical infrastructures (and many other organizations). Once confined in benign environments, 21st century business requirements often make it necessary to integrate ICS with external systems and networks to more efficiently harness sensor data, machine-to-machine (M2M) communication and automation technologies that have existed in industrial settings for years. Together, these elements create the IIoT, promoting more agile ways of delivering services.

Cyber incidents in the IIoT era

Alongside the early developments in the ICS space, cyber security challenges crept into organizations without being fully recognized or understood. Inevitably, ICS and the processes they controlled became more susceptible to malware, hacking and deliberate network disruptions. Malware, such as Stuxnet, Duqu, Night Dragon and Flame, has intentionally and unintentionally targeted industrial automation environments. These attacks can be devastating to both the environment and public safety.

Considering the societal implications of ICS cyber attacks, organizations should keep their cyber incident response plan up-to-date.



> "In a recent survey conducted internationally by KPMG International, **72%** of CEOs stated they are not fully prepared for a cyber event, significantly higher than in 2015, which was **50%**. During the interviews, CEOs frequently said: "We are as prepared as we can be," or "You can never be fully prepared.""

How do you know you're prepared? By practicing the ability to respond to cyber incidents. Companies need to be agile in order to deal with the unexpected.

Cyber game simulation

The KPMG Cyber Security practice has developed a realistic cyber defense training environment used by both executive management and operational staff to experience a simulated incident in order to learn how to respond to cyber threats, enhance cyber intelligence and detect indicators of compromise. The training environment comprises of 15 simulations including ICS simulations in the following sectors.

Energy — oil and gas; electric power

Water — waste water treatment; water supply

Transportation — railway; aviation; traffic control

Manufacturing — food and beverages; chemical and high tech

The simulated environment has been developed to be as close to real world as possible, and contains all the components that you expect in an operational environment — HMIs, EWS, DCS, OPCs.

Why KPMG?

The occurrence of a significant cyber incident can disrupt one's daily business. The cyber defense training environment provides participants with strategic, operational and tactical insights pertaining to cyber incidents in ICS environments.

Moreover, it can help your organization train cyber defense teams with the use of ICS simulation. During the game participants' cyber security knowledge is tested as well as their decision-making ability to mitigate cyber risks. As a result, the individuals, and in turn the company, will be more resilient when lessons learned are internalized and applied.

Information Security and Operational IT should not be the only groups responsible for handling cyber incidents. A cross-functional cyber defense team (comprised of IT operational staff, OT, Human Resources, Legal, Communications, the board, and external third parties) can help your company address cyber attacks more quickly and efficiently.

Communication and cooperation between all parties involved are the key to effective cyber incident response and increased cyber resilience.

Meet our ICS environments

Cyber attacks in the **oil and gas industry** quickly affect the entire automation of production, putting at risk the provision of products in a wider societal scale. In recent years, cyber attacks have materialized through malware infections, DDos attacks or malicious insiders leading to severe machine malfunction, pollution through the spillage of toxic waste, program wipeout, tangible asset or economic loss and irreversible loss of strategic data.

Breaches in the **electric utility industry** have risen over the years with stolen information misused as an act of sabotage. Disruptions resulted in several cases of power outages with severe consequences to health, safety and economic activity. As smart grid technology continues to gain momentum, more new energy systems will be connected to the Internet of Things, opening routes for misuse by malicious entities.

The attack surface of **modern railway systems** is enlarging due to the presence of new solutions, including connected systems and infotainment services. Although hackers have infiltrated rail infrastructure, these breaches have been exploratory (as far as we currently know) rather than disruptive. However, breaching related systems runs the risk of causing injury or death.

Cyber attacks in the **aviation industry** could impact core operations with the potential to seriously disrupt flight schedules and endanger the safety of passengers. The diverse nature of the airline business in terms of geography, customer lines, public and private systems and multiple interfaces with third parties establishes an environment of great risk.

Food and beverage manufacturers could experience attacks that involve tampering with production systems such as the destruction of pumps and mixers. If a machine or piece of software is immobilized by the attack and the problem is not promptly detected, the consequences range from a costly loss of production to potentially harmful products reaching the consumer.

Modern traffic control systems are able to execute multiple timing plans, communicate in real time with a huge quantity of networked sensors and manage traffic flows in the most efficient way. These systems can be targeted just like any other device. An unnoticed service attack or malware spread within a network connected by these systems could result in traffic jams or even accidents.

The design and production of industrial products, particularly in the high tech industry, involve complex networks of partners managing valuable patents, designs and formulas. Protection of intellectual property is a key concern. Potential attacks could aim to steal manufacturing metrics, production line information and also to tamper with production equipment inflicting financial losses and jeopardizing the market position of the targeted manufacturer.

Chemical process industries are invariably reliant on the integrity of industrial controllers for their smooth operation and viability. If an attacker decides to tamper with operations or equipment, it may cause critical damage that jeopardizes production availability. The most significant issues include attacks that would impact the safety of personnel, people in the vicinity or the environment from dangerous and toxic substances.

Contact us

Dani Michaux
Lead, Global Industrial Internet of Things Cyber Security
KPMG International
T: +60377213388
E: danimichaux@kpmg.com.my

John Hermans
Lead, Cyber Security Services, Europe, Middle East and Asia
KPMG in the Netherlands
T: +31 (0)6 51 36 63 89
E: hermans.john@kpmg.nl

Ronald Heil
Director, Cyber Security Services
KPMG in the Netherlands
T: +31 (0)6 51 36 97 85
E: heil.ronald@kpmg.nl

kpmg.com/cybersecurity

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by Evalueserve.

Publication name: IIoT cyber security simulation

Publication number: 134241-G

Publication date: May 2017