Industry 4.0 and Cybersecurity

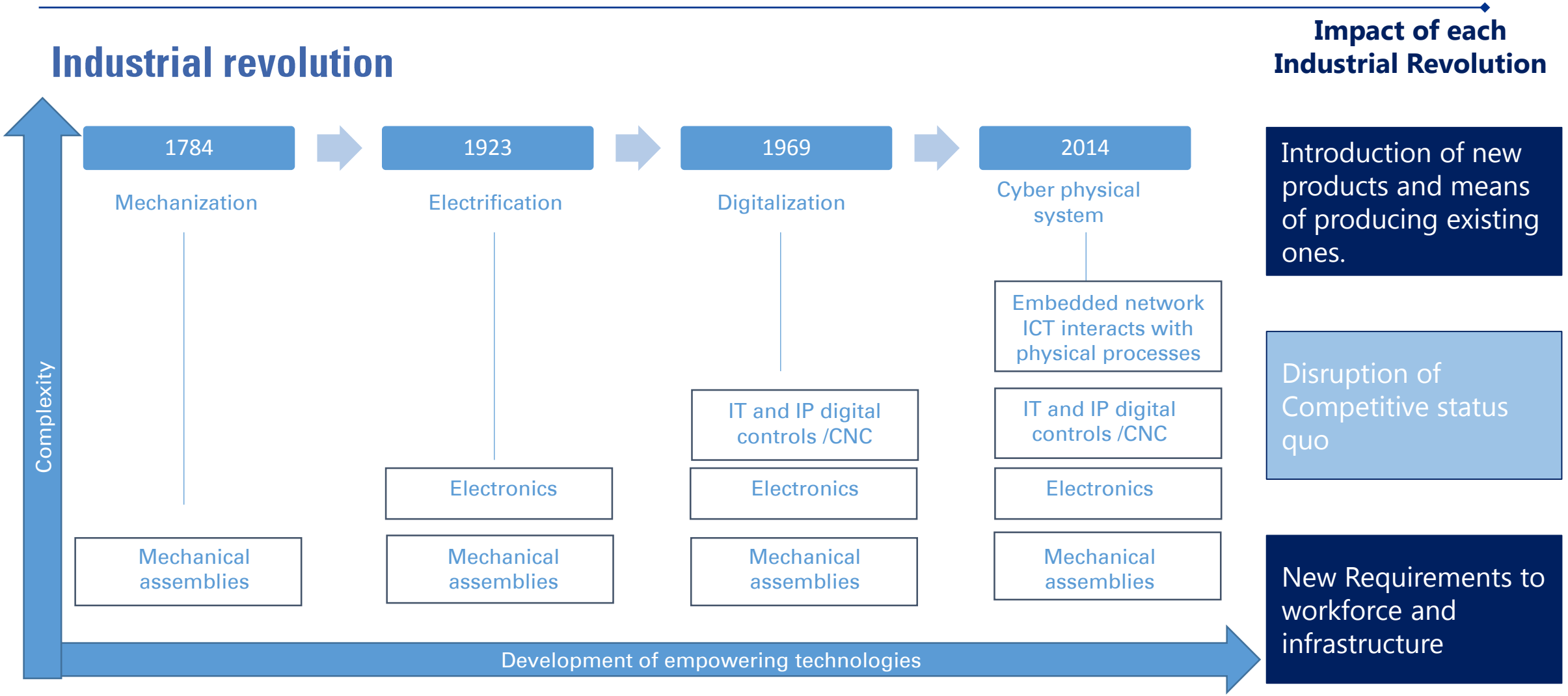
KPMG

02nd May 2017

Agenda

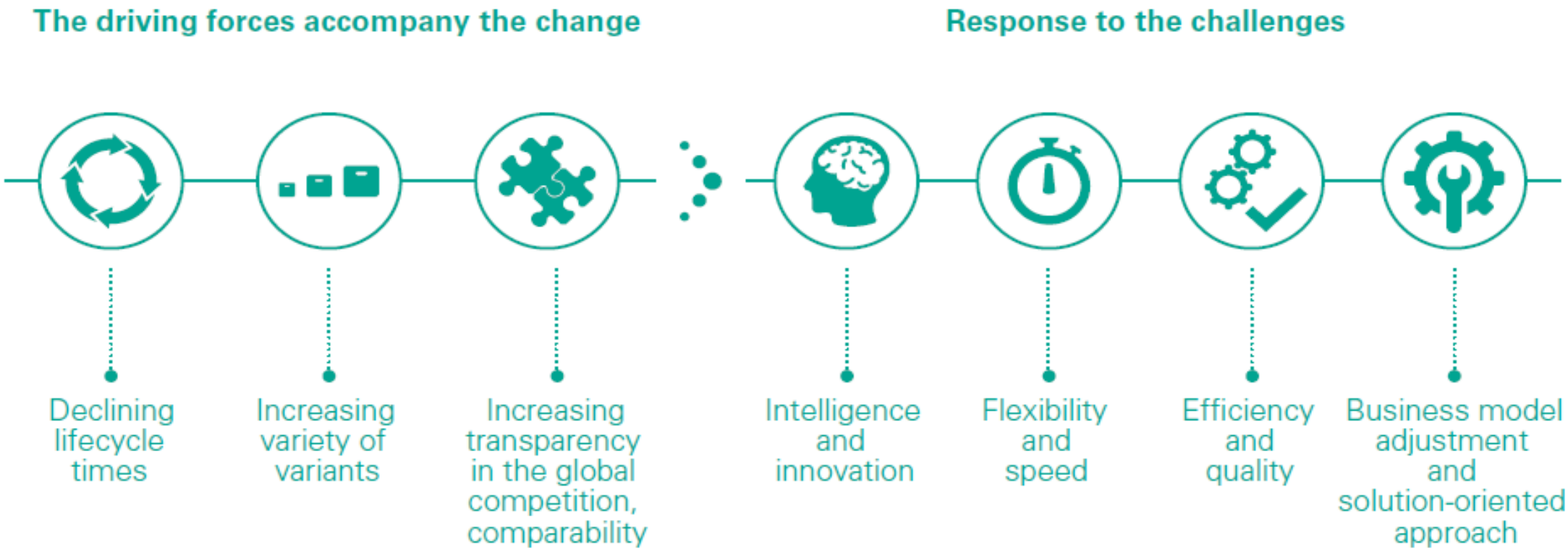
1. What is Industry 4.0
2. Disruptive technologies
3. Operational Technology
4. Cyber threats
5. Threat actor
6. Cyber attacks
7. Cyber security

Industry 4.0


Industrial revolution
Impact of each Industrial Revolution
Complexity
1784
Mechanization
Mechanical assemblies
1923
Electrification
Electronics
Mechanical assemblies
1969
Digitalization
IT and IP digital controls /CNC
Electronics
Mechanical assemblies
2014
Cyber physical system
Embedded network ICT interacts with physical processes
IT and IP digital controls /CNC
Electronics
Mechanical assemblies
Development of empowering technologies
Introduction of new products and means of producing existing ones.
Disruption of Competitive status quo
New Requirements to workforce and infrastructure

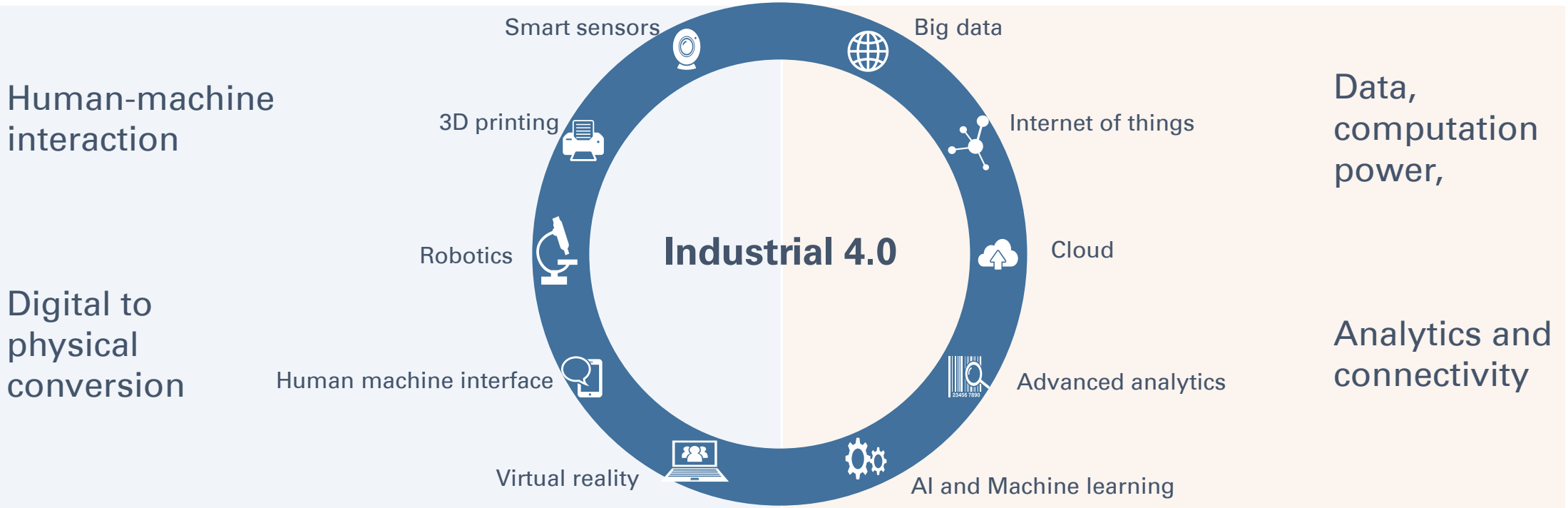
Factory of the Future

Driving forces for digitization and embracing to industry 4.0 technologies



Disruptive technologies

Technologies contributing for Industry 4.0 revolution



Operational technology

Changing phenomenon in OT environment

Information Technology (IT)

- IT stores, retrieves, transmits and manipulates data
- Traditional security needs:
  CIA
- An attack on IT could lead to data theft

Convergence

Operational Technology (OT)

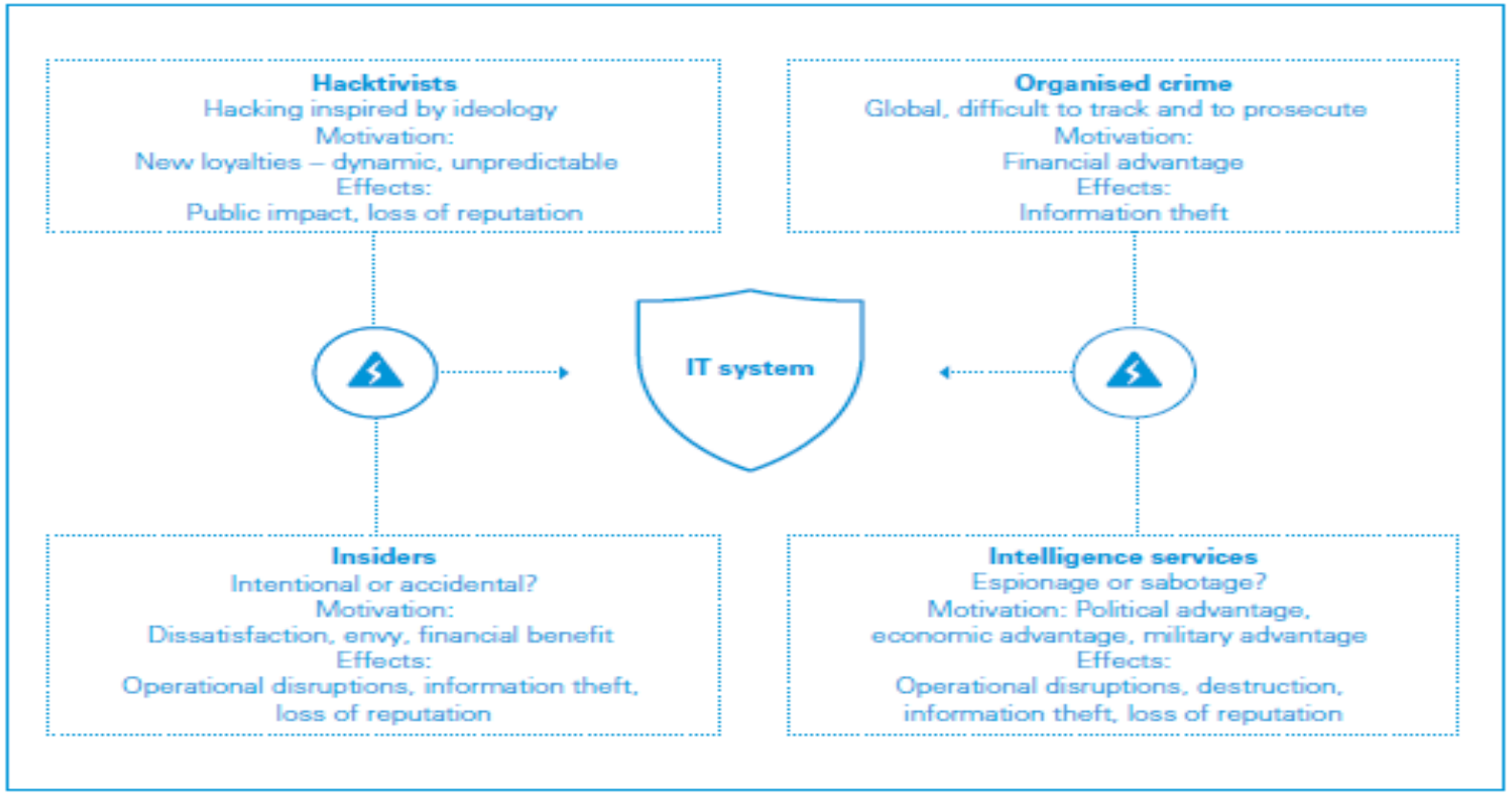
- OT uses that data to monitor, control and operate physical devices, processes and events
- New Security needs Availability, Up-time, safety
- Attack on OT could affect the physical world (people, environment and assets)

Operational technology (OT) is a category of hardware and software that monitors and controls how physical devices perform.

OT systems and components were non-networked, standalone devices that never touched the enterprise or IT side of the business.

Cyber threats

‘Threat actors’ responsible to impact or potential to impact security



Cyber attack

IOT DDOS attack

October 21, 2016

Major DDoS attacks, disrupting a host of websites, including the likes of Twitter, Netflix, PayPal, Pinterest and the PlayStation Network, amongst many others

Thousands of endpoint IoT devices transform in a botnet and flooding traffic to DNS hosting provider Dyn

Rampant Ransomware

Q3 and Q4 2016

Many ransomware made headline in 2016 including Locky, DMA Locker, Surprise, Ranscam

There was even mobile ransomware, and a version of Locky which could operate offline

Video of cyber attack on ICS environment

Link to the video of real cyber attack on ICS environment by exploiting common vulnerabilities.

Cyber security

1. Cyber Governance

Top management commitment is key factor to drive industry 4.0 implementation

- ✓ **Engage management and employees**
- ✓ **Integrate cyber security into core processes**
- ✓ **Develop cyber security policy and standard operating procedures**
- ✓ **Define cyber security roles and responsibilities**
- ✓ **Collaborate and share cyber security incidents**

Cyber security

2. Framework and Standards

Executive Order 13636 by US Government

The White House
Office of the Press Secretary

For Immediate Release February 12, 2013

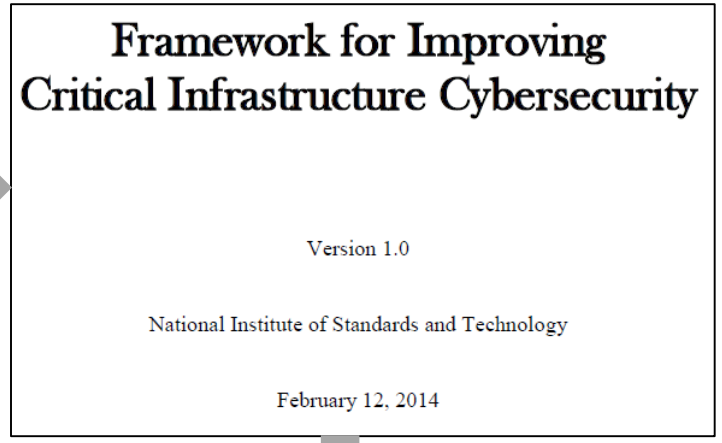
Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

- - - - - - -

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

NIST actioned on Developing the Framework



Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

NIST upgrades the Framework after industry feedback

USA | January 25 2017

The National Institute of Standards and Technology (NIST) issued an update to its Framework for Improving Critical Infrastructure Cybersecurity ("Framework") on January 10, 2017. The updated draft Version 1.1 ("Draft")1 was issued after NIST's review of considerable public and private-sector feedback on Version 1.0.2 The updated Draft includes improvements but is intended to remain a voluntary cyber risk management tool that organizations can customize.

Cyber security

3. Cyber risk assessment

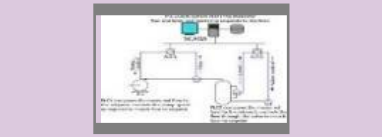
- ✓ **Starting Point of cyber journey in Industry 4.0**
- ✓ **Coverage is important – IT, OT, ICS, Third Parties, Ecosystem, Entry/Exit points, End points etc.**
- ✓ **Think and Stick to Business Risks rather than operational/technical issues**
- ✓ **"Convergence" is the key for any Industry 4.0 implementation**
- ✓ **Not One Time activity**

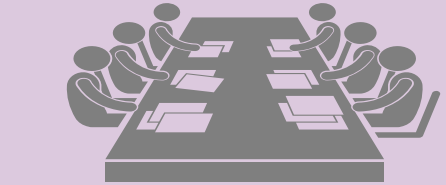
Cyber security

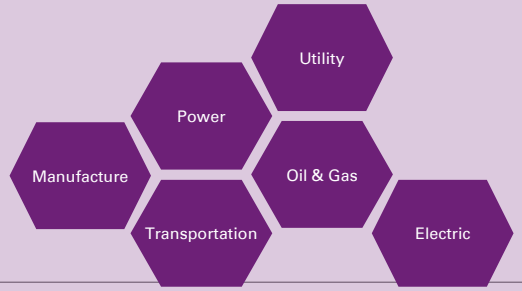
3. Cyber security controls

Control Process Understanding

01







Control System Security Assessment

02

- Control System Architecture Review
- \+ Security Gap Analysis
- \+ Cyber Vulnerability Assessment
- \+ Operational Technology Policy Design
- \+ Physical Security Assessment
- \+ Security Awareness Workshop

The fourth industrial revolution starts with one very important point:

Trust

Thanks you