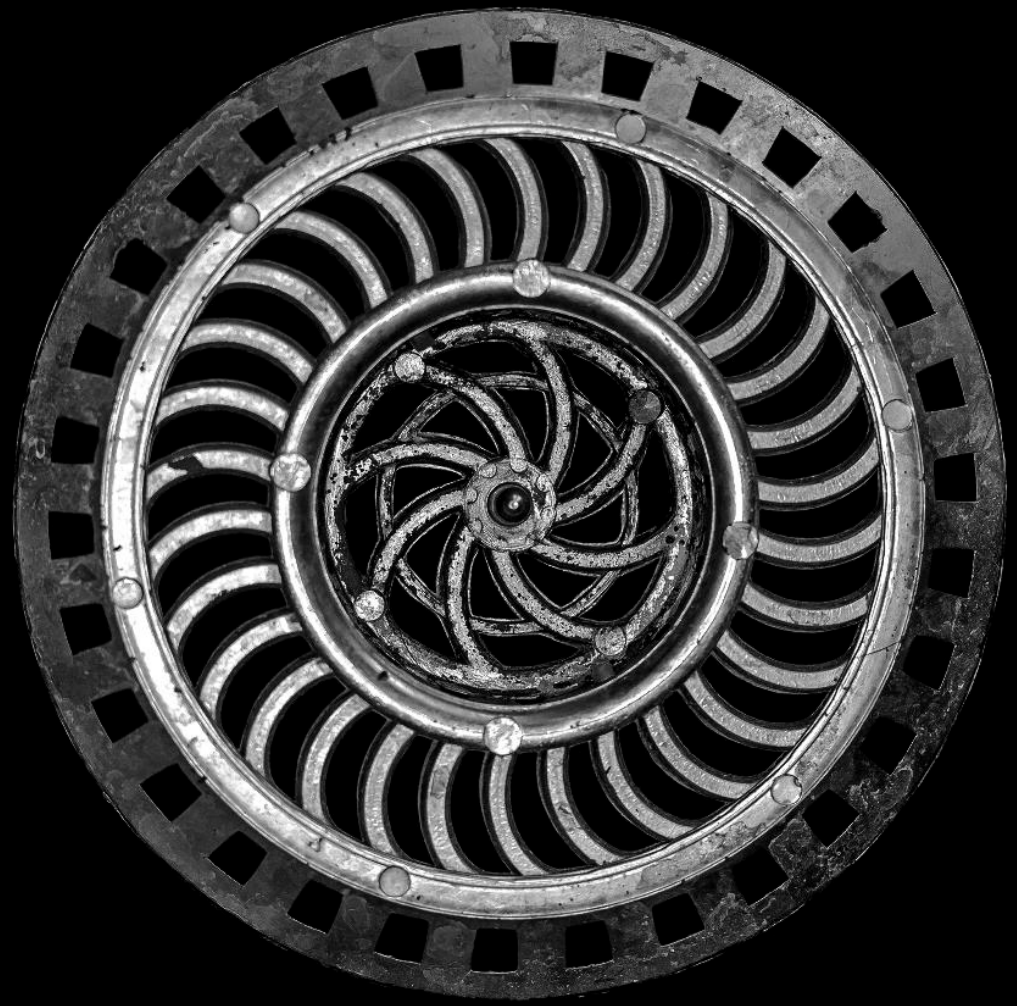
Deloitte.



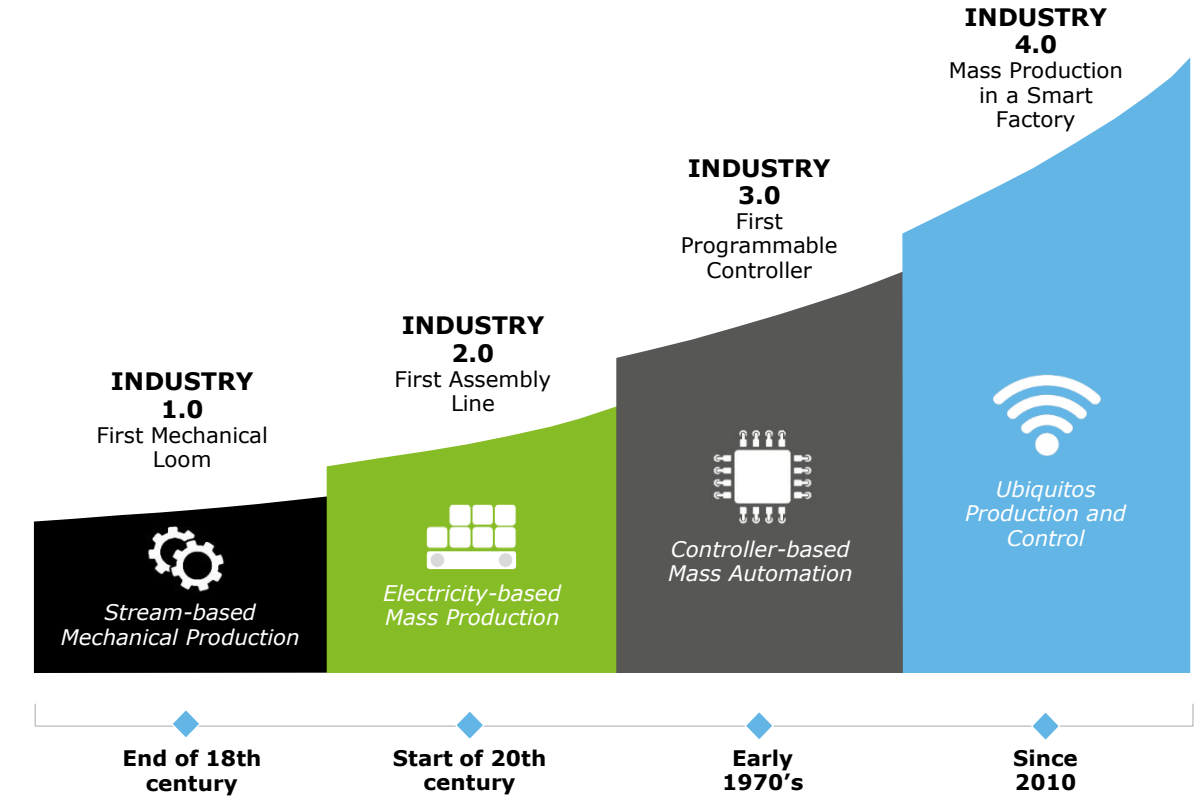
exclusivIT_Cyber and Emerging Technologies

May 4, 2021

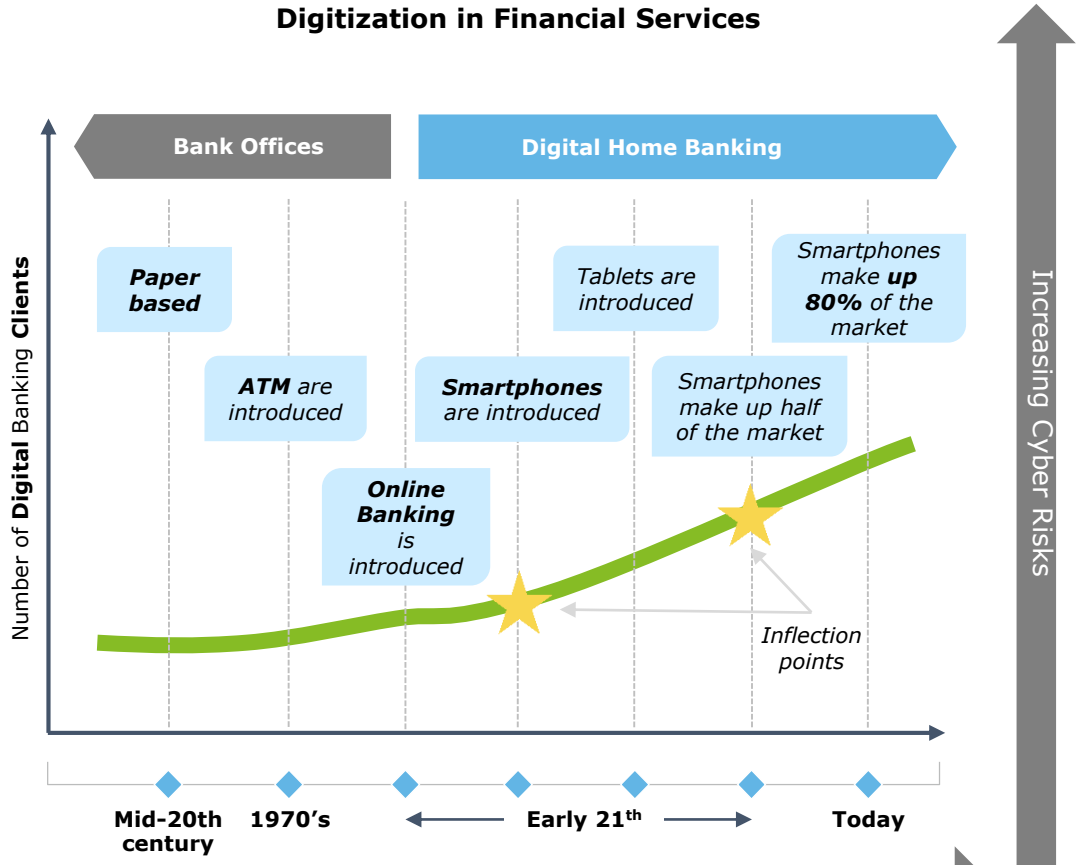
The trend towards digitizing core business elements through Emerging Technologies continues to accelerate across all major sectors and industries, also increasing cyber risks

Business Digitization Trends

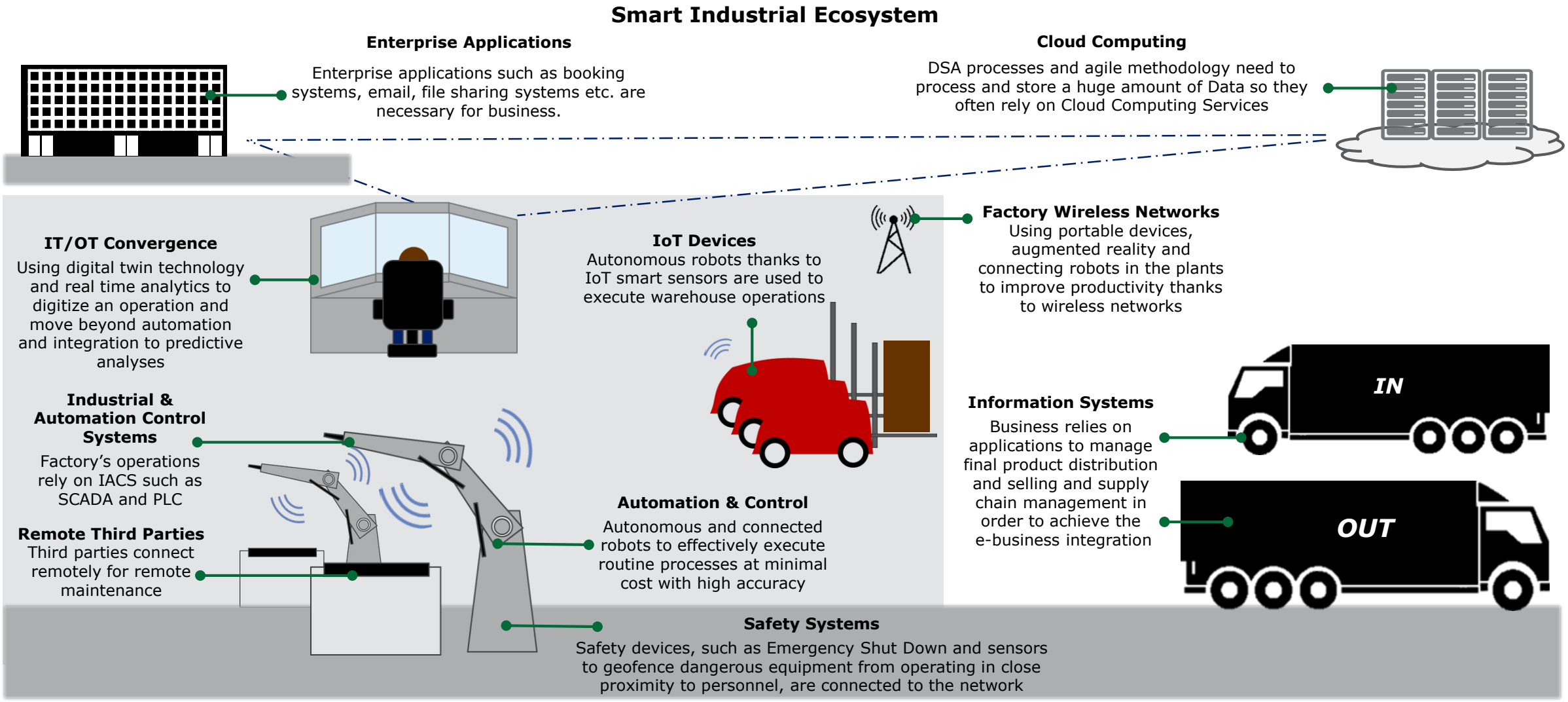
Digitization in Industrial Environments



Digitization in Financial Services

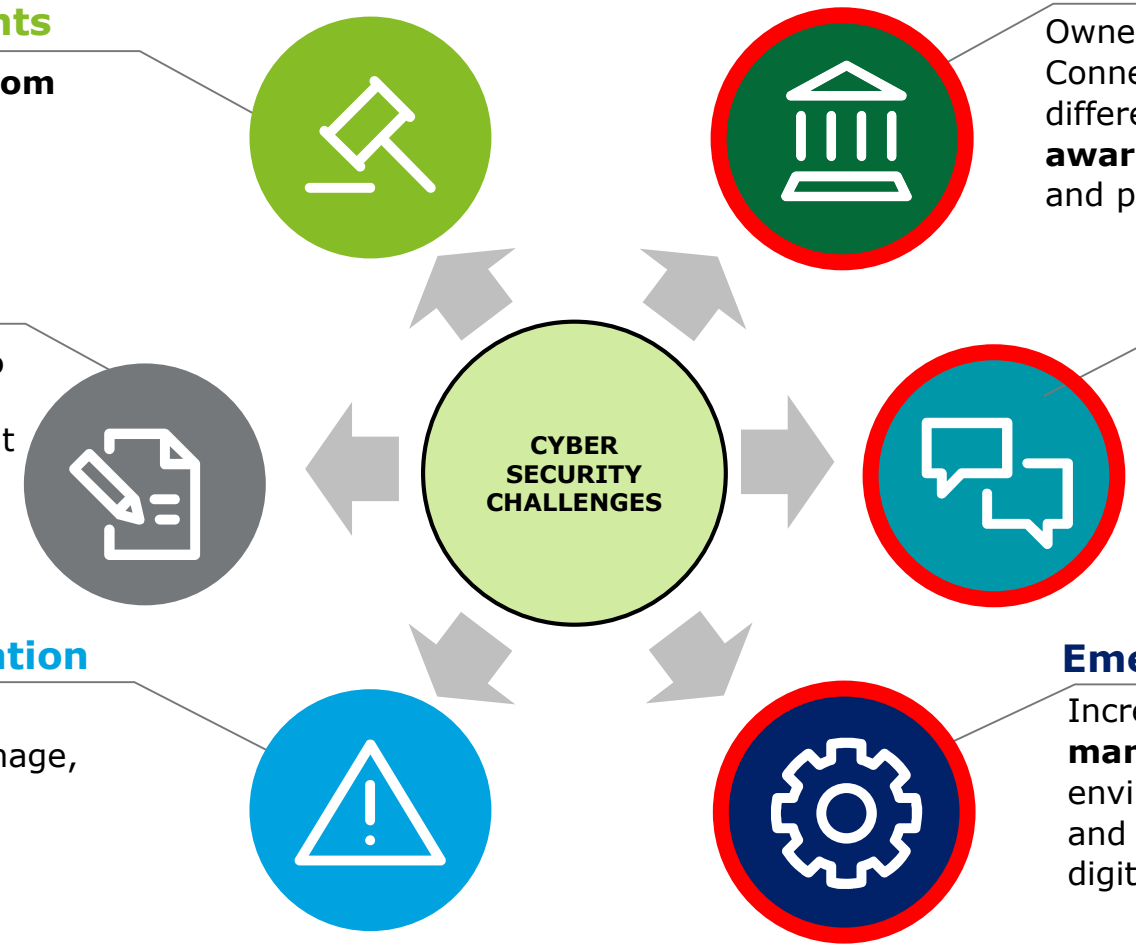


For example, the introduction of Emerging Technologies through the Industry 4.0 revolution has eradicated traditional IT / OT boundaries to create smart ecosystems



Together with benefits, this evolution also introduces new Cyber Security challenges related to Emerging Technologies that top management must understand and manage

Summary of Common Cyber Security Emerging Technology Challenges



International Regulatory and Legal Requirements

Important **developments from national and international** government bodies.

Cyber Security Governance

Ownership of cyber risk for IT, OT, and Connected Products often spread across different areas of responsibility. **Lack of awareness of mutual requirements** and practices.

Risk Management

Lack of an **integrated approach to IT, OT, and Connected Product security**. Different risk management priorities and outputs caused by inconsistent ERM processes.

Communication & Involvement

Different perspectives, approaches and sometimes **directions** followed by IT, OT, and Connected Products. **Lack of technology-specific security knowledge** inside the organization and the markets.

Cyber Threat Sophistication

Higher level of threats from cybercrime, hacktivism, espionage, etc.

Emerging Technologies Convergence

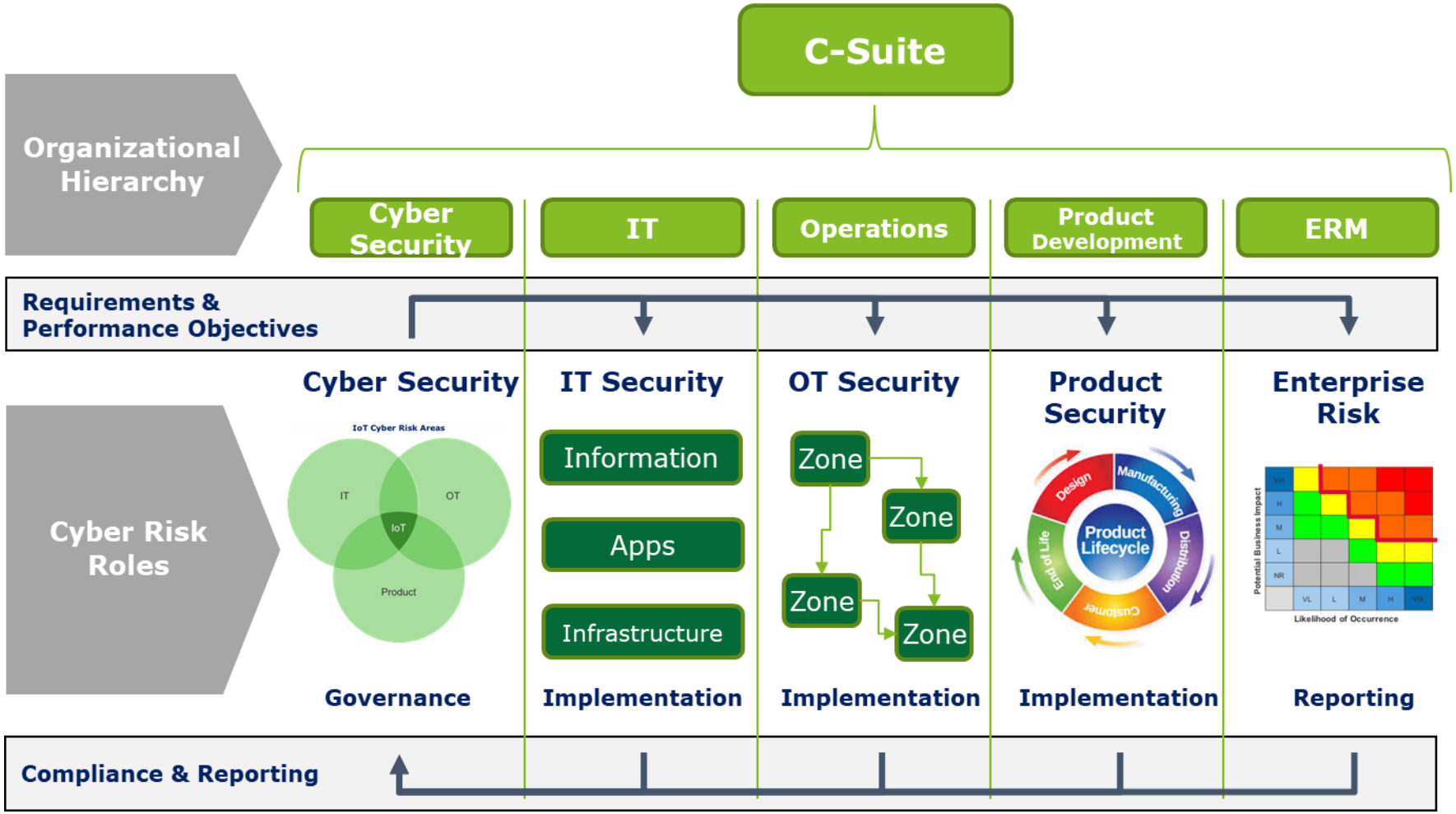
Increasingly **complex technical and managerial risks** associated with operational environments. New challenges caused by M&A and new development in terms of increased digital perimeter.

= Today's Focus

1) ICS / SCADA = Industrial Control Systems / Supervisory Control And Data Acquisition

Properly managing Emerging Technology cyber risks requires a coordinated flow of governance processes and information across a wide range of corporate stakeholders

Cyber Security Governance



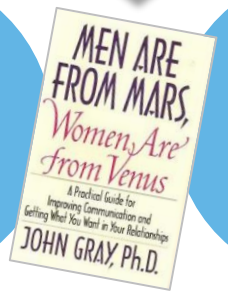
Key Points

- **Connected CISO**
  - CISO connected with other relevant cyber risk areas and communicating with the Board to report cyber risks
- **Segregation of Duties**
  - Security environment requires checks and balances across plan, do, check, act management processes to ensure business priorities do not lead to overexposure to risk by bypassing security requirements
- **Business Proximity**
  - Security functions must be close enough to business functions to understand how to balance risk reduction through security measures with the needs and objectives of the business

Key Stakeholders usually come from different backgrounds and speak different languages making hard to achieve a collaborative work flow with unified priorities

Communication and Involvement

Main Challenge



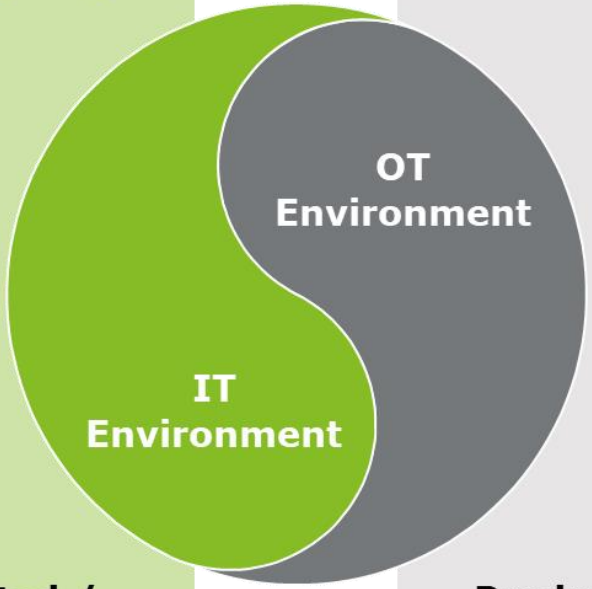
Key Cyber Security Actors	Top Management / Business Development	Chief Security / Risk Officer	Information Technology	Operational Technology	Product Development
Typical Background	MBA	Audit / Security	IT / Electronics / Communications	Industrial Process Engineering	Marketing / Pre-Sales Engineering
Daily Terminology	• Profit and Loss • Balance Sheet • Stakeholder Relations • Marketing Strategy	• BIA • COSO Model • SOX Compliance • Monte Carlo Sim	• IAM • TCP / IP • OSI Model • ISO 27001/2 (ISMS)	• PLC / Sensors • Purdue Model • HAZOPs • ISA / IEC 62443	• Prototyping • Quote Generation • Product Optimization • Title 21 CFR Part 11
Typical Vendors	• McKinsey & Co • Bain & Co • Boston Consulting Group	• Big 4 Auditors • EMC / RSA / Archer • SAS Analytics	• Microsoft • IBM / HP • SAP	• ABB • Honeywell • Emerson	• Cognizant • Gap Systems • IBM PLM
Primary Concerns	• Overall Business Success • Product Development	• Optimized Risk Portfolio	• Information Confidentiality, Integrity, and Availability	• Personnel Safety • Process Efficiency / Availability	• Time to Market • Market Share • Revenue Targets

The inherently different approaches for reducing risk in a converged environment of previously isolated or emerging technologies represents a significant challenge

EXAMPLE: Convergence of IT and OT Environments

Securing the IT environment "in the garage"

- Security updates / technologies **usually tested / installed in off-line environments**
- Non time-critical applications **resilient to service interruptions** caused by updates
- Installed infrastructure base **relatively mature / easily upgradeable** in terms of security



Securing the OT environment "on the road"

- **Production systems usually can not be taken offline** to install security updates / technologies
- Updates to live systems introduce **significant risk for industrial process interruption**
- Current global industrial base **may be too large / complex to fix**

To manage these risks, executive leadership must transform the CISO role from a techie to a strategic advisor for Top Management, with appropriate standing and independence

Current vs. Desired CISO Qualities Observed by Deloitte

Chief Information Security Officer

Strategist

Drive alignment of business and cyber risk strategy, innovate, and instigate transitional change to manage risk through valued investments

Current **15%**

Desired **32%**

Advisor

Integrate with the business and top management to educate, advise, and influence activities with cyber risk implications

Current **12%**

Desired **35%**

Guardian

Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber risk program

Current **41%**

Desired **22%**

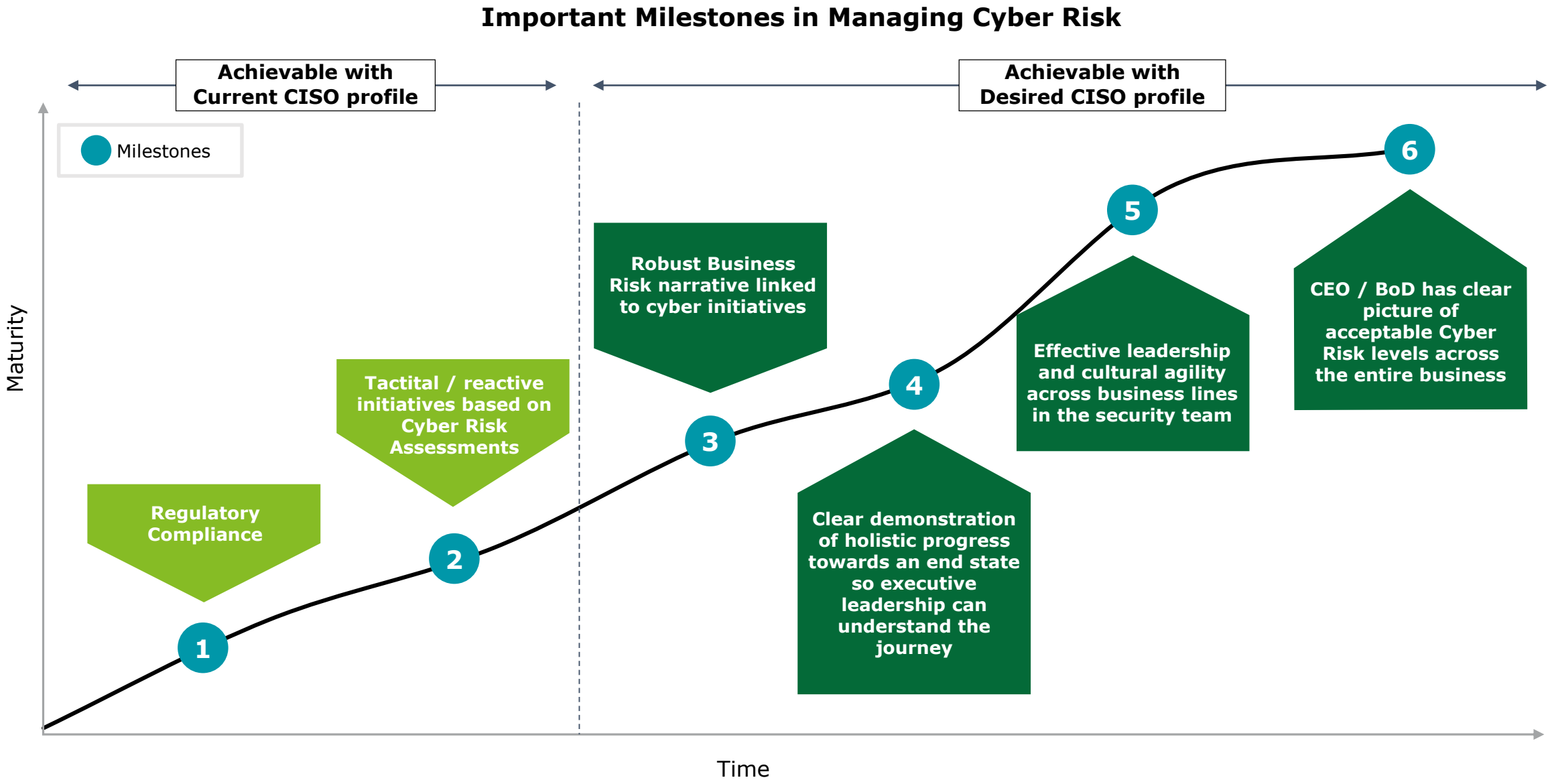
Technologist

Assess and implement security technologies and standards to build organizational capabilities and compliance

Current **33%**

Desired **12%**

A properly positioned CISO with CEO / BoD support will help reduce cyber risks to an acceptable level at a pace that suits your resource availability and business needs



Deloitte.