OT Cybersecurity for Food & Drink Manufacturers:

Where to Start and What Matters Most

Food & Drink Federation

Quentin Menusier

SE ADVISORY SERVICES

Quentin Menusier

Cybersecurity Business Consultant

Focus on OT cyber security for the UK&I zone

SE ADVISORY SERVICES

F&B challenge

Food & beverage manufacturers are rapidly digitalising their operations, connecting production environments to IT systems and external partners.

However, these OT environments were not designed with cybersecurity in mind, creating significant operational risk.

As a result, organisations face increasing exposure to cyber threats while maintaining strict constraints on uptime, safety, and compliance.

Agenda

01 IT vs OT

02 The new paradigm

03 Regulation overview

04 Cybersecurity activities vs risk

05 Key activities in F&B

Introduction

Cyber

People, Human error, such as falling for phishing scams, is a major vulnerability. Effective security relies on training, creating a culture of awareness, and defining roles and responsibilities

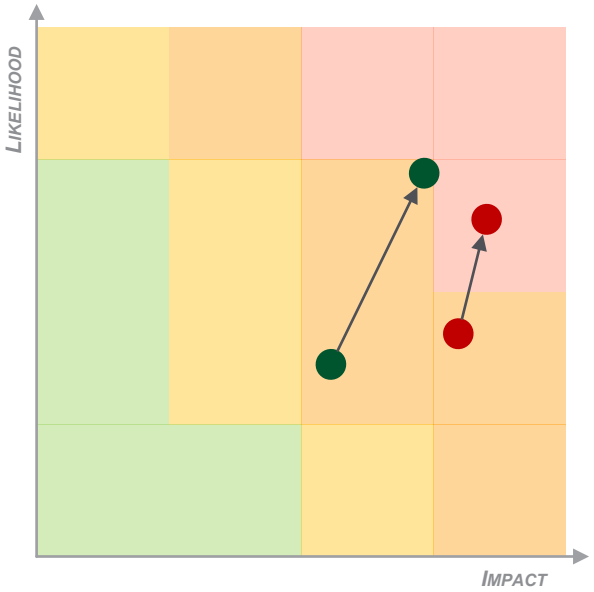
Processes, These are the policies and procedures that define how technology is used and how threats are managed, including incident response plans and access control policies

Technology, Hardware and software solutions that protect digital assets, such as firewalls, antivirus software, encryption, and intrusion detection

SE ADVISORY SERVICES

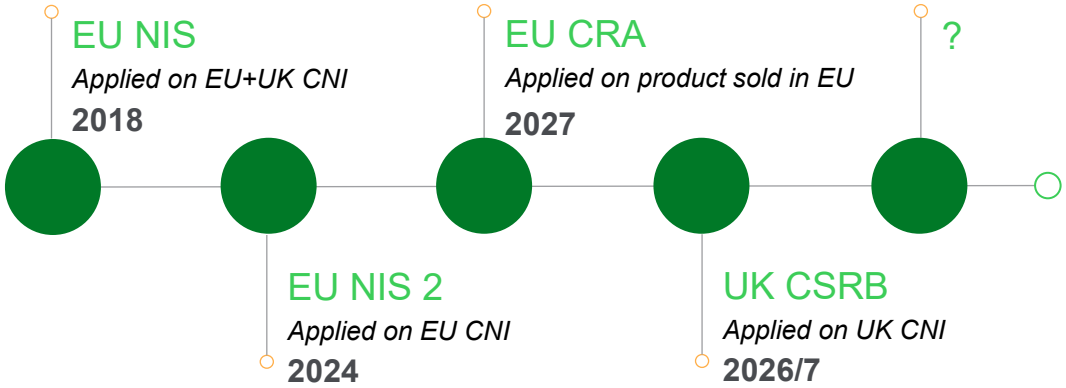
The new cybersecurity threat paradigm

CYBER ATTACK VS COMPLIANCE RISK



The measures implemented by governments and institutions require organisations to adapt to increasingly prevalent cyber threats, which in turn increases the risk of non-compliance

CYBER REGULATION LANDSCAPE



- **Country regulation** says "Manage your risks"
- **CAF** says "This is what we believe good looks like when you manage your risks"
- **ISO 27001 / IEC 62443** "here are some lower-level things you should do to manage your risks"

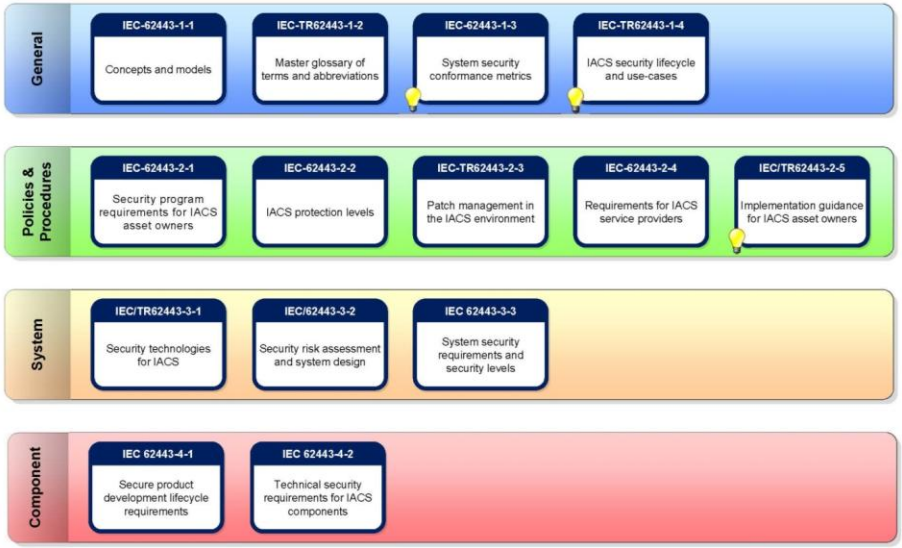
SE ADVISORY SERVICES

Regulatory Content

Objective	• Protect a country's critical infrastructure and essential systems
Scope	• Critical National Infrastructure / Operators of Essential Services • Critical suppliers
Defined Regulator Powers	• Introduces **stricter, earlier and broader** incident reporting obligations. • Requires organisations to notify regulators faster and with more detailed information on disruptive cyber events.
Cyber risk management	• Regulators gain authority to conduct **proactive investigations**, not only to react after incidents. • Strengthens ability to set and enforce requirements across sectors.
Incident detection & response	• Water, energy, transport, and other CNI operators must implement stronger **supply-chain oversight and governance**. • Regulators can directly regulate high-risk suppliers through "Critical Supplier" designation.
Incident Reporting Requirements	• Regulators can **charge organisations** to recover the costs of enforcement, oversight, and investigations.

IEC 62443 as a reference standard

IEC 62443 is an international series of standards that addresses cybersecurity for operational technology in automation and control systems



Asset owner operator	System Integrator	Product / solution provider
Sections 2-1, 2-3, 2-4	*Sections 2-4, 3-2, 3-3*	*Sections 3-3, 4-1, 4-2*

Security levels within IEC62443

SL1 — Employee errors

SL2 — Cyber crime, hackers

- Low Resources
- Low Motivation
- Simple Means
- Generic ICS Skills

SL3 — Cyber terrorism, hacktivist

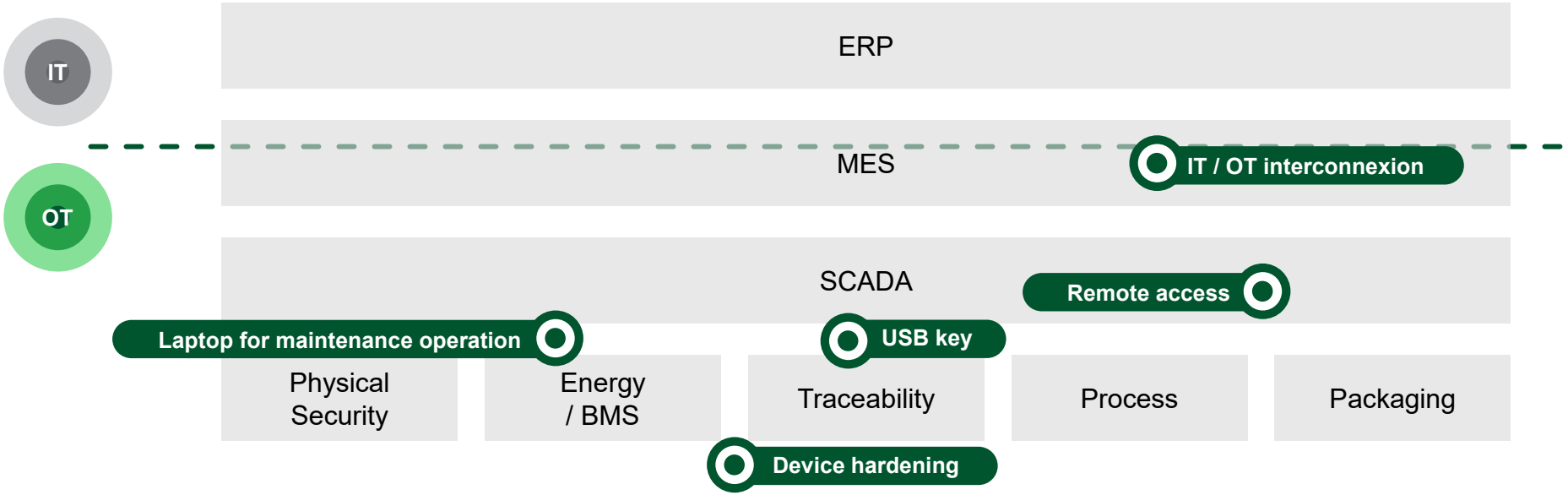
- Moderate Resources
- Moderate Motivation
- Sophisticated Means
- Specific ICS Skills

SL4 — Nation state

- Extended Resources
- High Motivation
- Sophisticated Means
- Specific ICS Skills

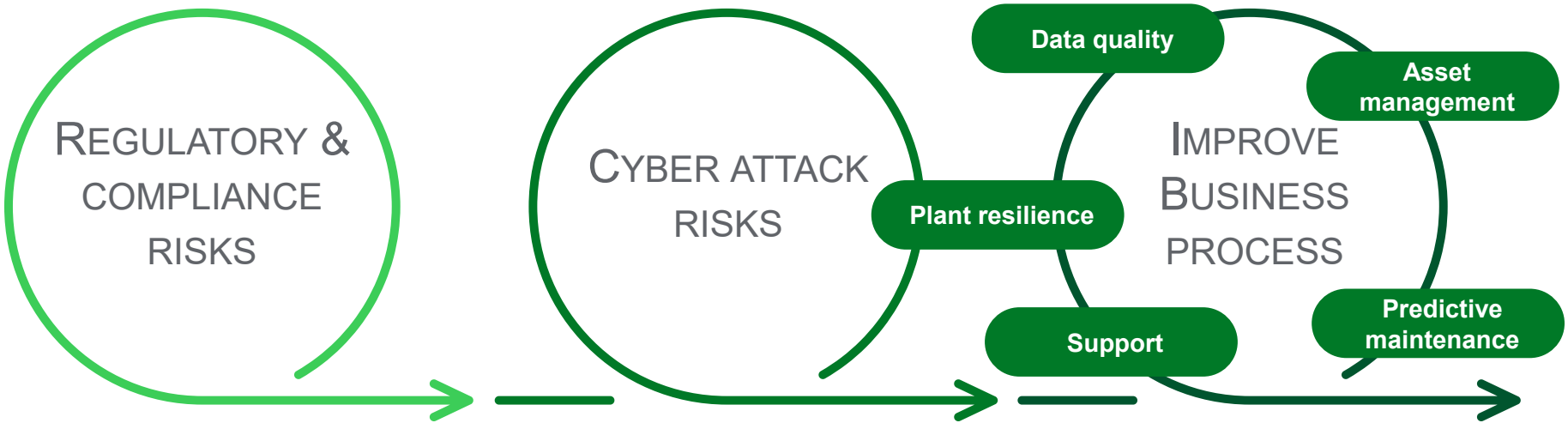
SE ADVISORY SERVICES

Major intrusion vectors with OT (risk points)



SE ADVISORY SERVICES

Turning Cyber Risk into Business Value



SE ADVISORY SERVICES

Typical OT Cybersecurity Journey in Food & Beverage

Establish OT Security Foundations

Security assessment
Risk analysis
OT policies & governance
Cybersecurity roadmap

Gain Visibility of OT Environment

Asset inventory (know what's connected)
Network mapping

Secure Access to Critical Systems

Network segmentation
Secure remote access
Least privilege
Multi-factor authentication (MFA)

Detect and Respond to Threats

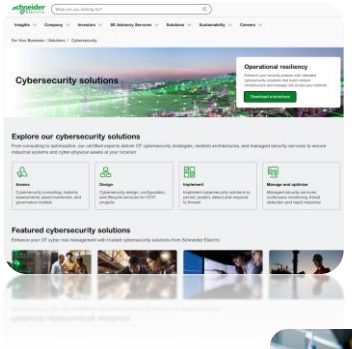
Anomaly detection
OT-specific incident response

Take away

- OT cyber risk is business risk
- Start with visibility, Segmentation + access control
- Use frameworks, but stay pragmatic
- Prioritise what impacts production

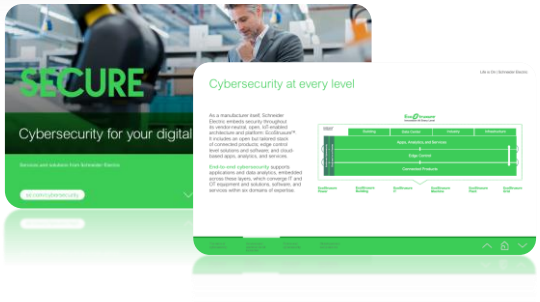
Interested in knowing more?

Find out more how Schneider Electric deliver on OT Cybersecurity



Visit website

Download Brochure



Contact Quentin Directly

Email: quentin.menuisier@se.com

SE ADVISORY SERVICES