How to implement IMO 2021 in a way to pass an audit

Hanne Wesselsen
Hanne.Wesselsen@devoteam.no

Cicilie Hennig-Till
Cicilie.till@devoteam.no

devoteam

The main differences between IT and OT

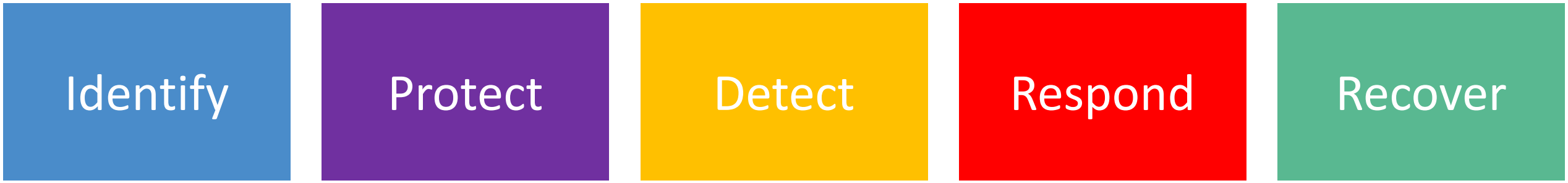
IT

1. Confidentiality
2. Integrity
3. Availability

OT

1. Safety
2. Reliability
3. Productivity

IMO 2021 MSC-FAL.1/Circ.3


Identify
Protect
Detect
Respond
Recover

Tiers to assess the maturity

C2M2 maturity assessment

1 Partial

Not formulated/**ad hoc.**
Limited awareness of cyber security risks.
Limited ability to **collaborate** with other organizations for cyber security risk management.

2 Risk-Informed

Risk management practices are **not organization-wide.**
Awareness of cyber security risk with **informal sharing** of cyber security information within the organization.
No formal interaction with other external organizations for cyber security risk management.

3 Risk-Informed and repeatable

Formal risk management process.
Organization-wide management of cyber security risk.
Receives information from external organizations and uses this in risk management decisions.

4 Adaptive

Practises **adapt** based on lessons learned and predictions.
Cybersecurity risk management is part of the **culture.**
Two-way sharing of information with external organizations.

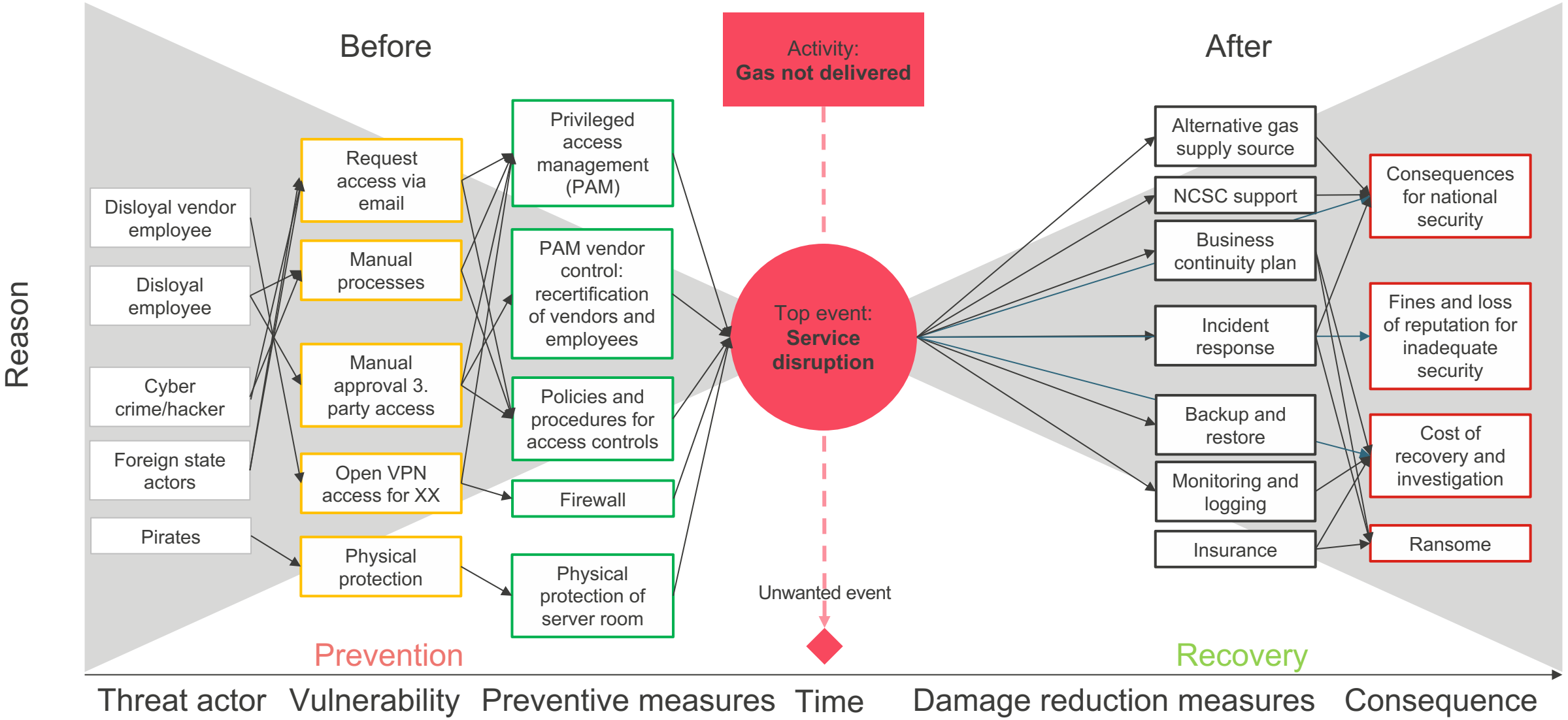
Increasing rigour and sophistication

You can't protect what you don't know you have

MNEMONIC, OT Miniseries Podcast

So, keep the business and the auditors happy !

Bowtie


Before
Activity:
Gas not delivered
After
Reason
Consequence
Disloyal vendor employee
Disloyal employee
Cyber crime/hacker
Foreign state actors
Pirates
Request access via email
Manual processes
Manual approval 3. party access
Open VPN access for XX
Physical protection
Privileged access management (PAM)
PAM vendor control: recertification of vendors and employees
Policies and procedures for access controls
Firewall
Physical protection of server room
Top event:
Service disruption
Unwanted event
Alternative gas supply source
NCSC support
Business continuity plan
Incident response
Backup and restore
Monitoring and logging
Insurance
Consequences for national security
Fines and loss of reputation for inadequate security
Cost of recovery and investigation
Ransome
Prevention
Recovery
Threat actor
Vulnerability
Preventive measures
Time
Damage reduction measures
Consequence

Supply chain risk principles

1. Integrate cybersecurity in all organizational governance
2. Keep updated overview of critical components and suppliers
3. Include cybersecurity into contracts with critical suppliers and customers
4. Closely collaborate with key suppliers
5. Include key suppliers in resilience and improvement activities
6. Assess and monitor throughout the supplier relationship

What do we mean by access management?

Governance					
Ethics	Routines	Education & Awareness	Responsibility	Laws & Regulations	Management

Identity Management	Workflows & policies	Ease of use	API Management
Identity and access management tools			

Privileged access represents a significant security risk for every organization, and privileged access management (PAM) is a discipline that must be considered a core part of every security program.

Gartner, 2021 Buyers' Guide for Privileged Access Management,

12 February 2021, Michael Kelley, Felix Gaehtgens, Abhyuday Data

The IACS UR Requirements E26 and E27 say that vendors of OT systems must have control over remote access to be certified.

95% of cybersecurity breaches are caused by human error

Cybint

Karsten Warholm på Olympiastadion i Stockholm. Foto: Christine Olsson/TT (NTB scanpix)

Cyber awareness program

- Phishing tests on a regular basis
- E-learning, games, or trivia for all employees
- Targeted training for managers, administrators, and other vulnerable groups
- Establish good security culture
  - Never let anyone tailgate on your way into the office
  - Always lock your computer when leaving your desk
  - Never click on links before checking for red flags


Detect
MEET THE PRESS
Global ECC Escalations
Google
Photo: ITSEC


Håndsprit dreper IKKE Norovirus
HÅNDVASK MED SÅPE VANN!
VAKTLISTER
MOTOROLA
SIVILFORSV
LEDE
NNIG-TILL


Medical
ZOGEAR


Respond

Backup and Recovery

- Backup plan and strategy
- Disaster recovery plans for critical systems
- Set recovery time objectives
- Regular drills
- Include critical suppliers in drills

Summary – what to do

1. **Maturity assessment**
2. **Identify**
   - Identify assets
   - Asset criticality
   - Risk analysis
3. **Protect**
   - Supply Chain risk principles
   - Identity and Access Management
   - Awareness program
4. **Detect**
   - Security Operation Centre (SOC-service)
5. **Respond**
   - Incident response plan
   - Training and drills
6. **Recover**
   - Disaster recovery plan
   - Objectives and drills
   - Backup

devoteam

Creative tech for Better Change

Hanne Wesselsen
Hanne.Wesselsen@devoteam.no

Cicilie Hennig-Till
Cicilie.till@devoteam.no