Health and Safety
Executive

HSE

MJV Malta

Cyber Security and the UK's current regulatory approach

Matt Lea

Cyber attack

Taken from BBC News website:

“NHS trusts were left vulnerable in a major ransomware attack in May 2017 because cyber-security recommendations were not followed, a government report has said.

More than a third of trusts in England were disrupted by the WannaCry ransomware, according to the National Audit Office (NAO).

At least 6,900 NHS appointments were cancelled as a result of the attack.

NHS England said no patient data had been compromised or stolen and praised the staff response.

The NAO chief said the Department of Health and the NHS must now "get their act together".

Cyber Attack

The Chemical Engineer (April 19):

“Cyber Attack hits aluminium firm”

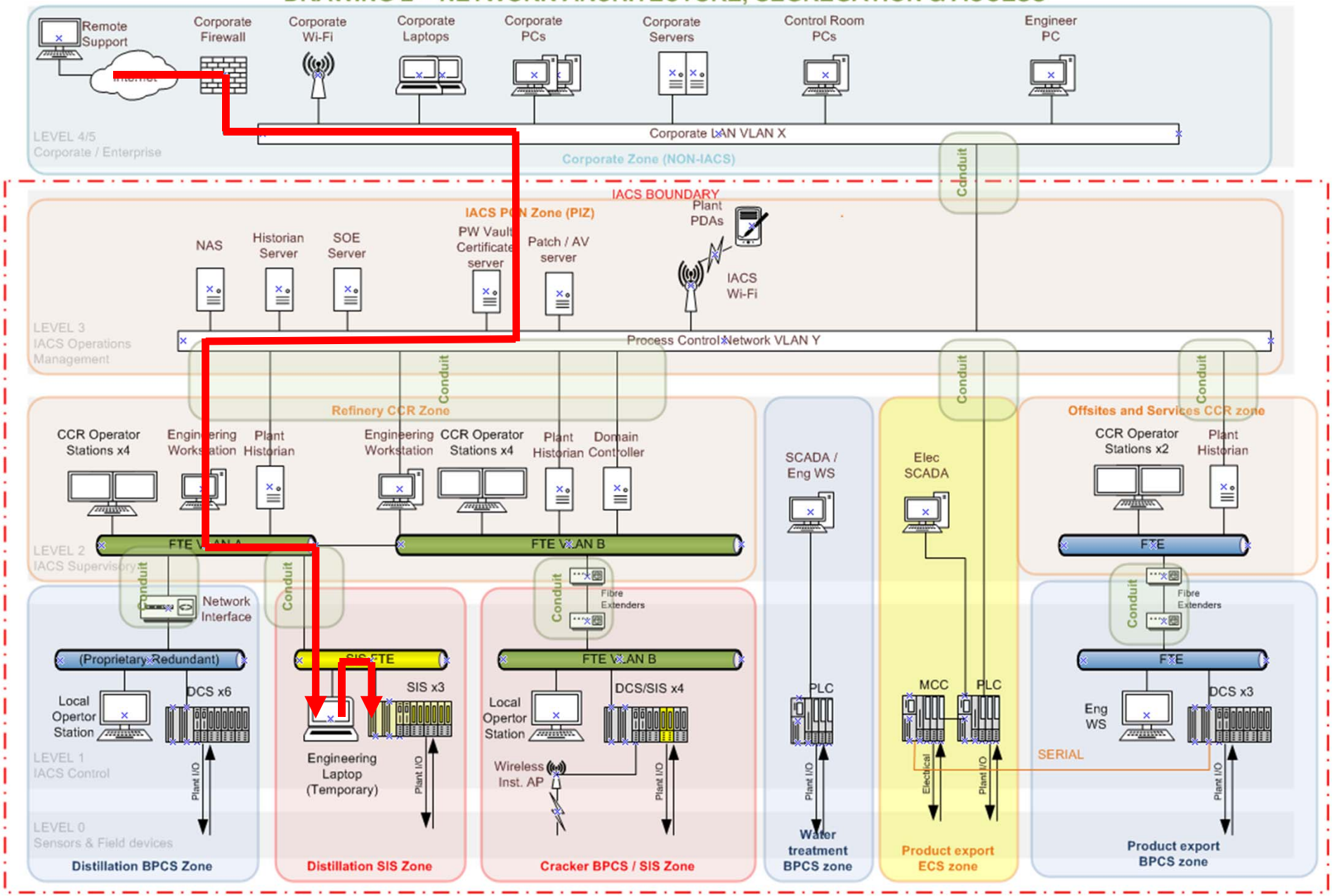
Norsk Hydro ransomware attack 18 March 19

- IT systems shut down
- LockerGaga ransomware
- Backing up data to a pre-infected state
- No reported safety incidents

Cyber Security

- What is cyber security?
- Why are we interested?
- How is the cyber world different?
- How do we Regulate?

DRAWING 2 – NETWORK ARCHITECTURE, SEGREGATION & ACCESS

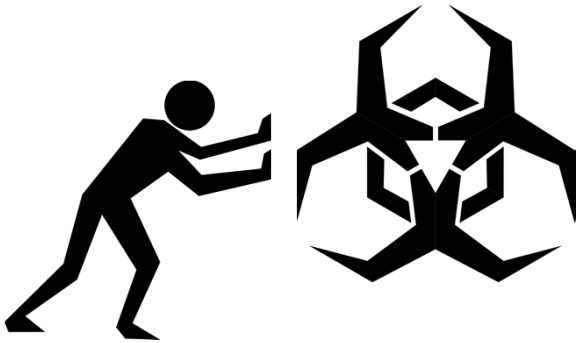


What is Cyber Security?

- The protection of devices, services and networks - and the information on them - from theft or damage.

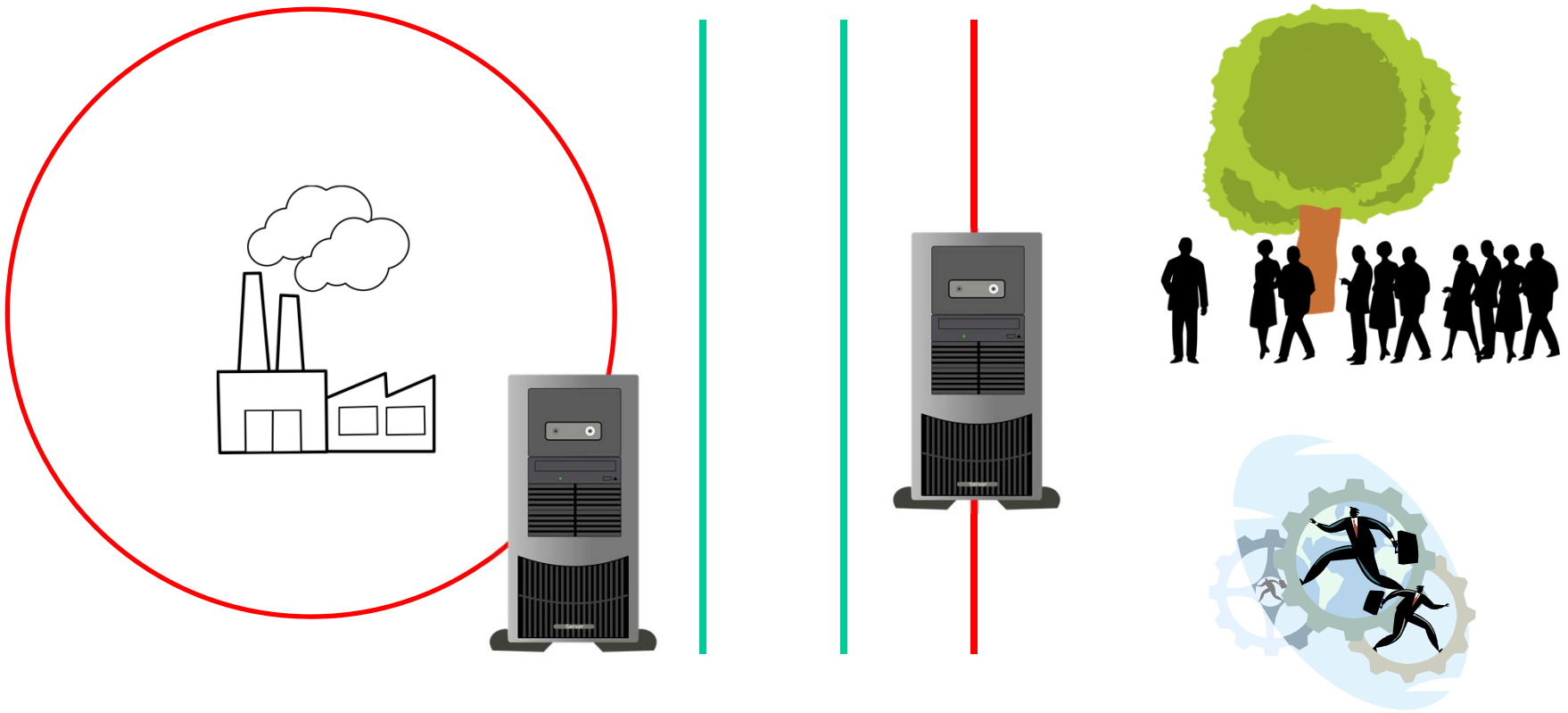
Source: National Cyber Security Centre (part of GCHQ)

What is Cyber Security in reality?



Threat Hazard Vulnerability Consequence

Why are we interested?



Hazard
Essential Services

Consequence

Why do we Regulate?

- Major Hazard Regulations
  - take all measures necessary to prevent major accidents and to limit their consequences for human health and the environment
  - take appropriate measures with a view to protecting persons on the installation from fire and explosion and securing effective emergency response.
- A cyber attack is a foreseeable initiator
- A cyber attack can undermine a risk control measure

Why do we Regulate?

- The Directive on security of network and information systems (NIS Directive)
  - entered into force in August 2016
- The Network and Information Systems (NIS) Regulations 2018
  - transposed into UK law in May 2018

- A cyber attack can reduce or disrupt an essential service

NIS Regulations 2018

- Regulations made in exercise of powers conferred by the 1972 European Communities Act and by the 1973 Finance Act
  - BEIS is the Competent Authority
  - HSE is acting as the CA for the Oil and Gas Sectors on behalf of BEIS
  - the primary legislation is not HSWA
  - breach is a civil offence

NIS Regulations 2018

- Regulation 10: The security duties of operators of essential services
  - take appropriate and proportionate technical and organizational measures to:
    - manage risks posed to the security of the network and information systems on which their essential service relies
    - prevent and minimize the impact of incidents

How is the cyber world different?

- Process world risk is a function of:
  - likelihood
  - consequence
- Cyber world risk involves malicious intent and is a function of:
  - threat
  - vulnerability
  - target attractiveness
  - attacker capability
  - consequence

How do we Regulate

- Inspection
  - the current benchmark is the HSE Operational Guide at least until standards become established
- Assessment
  - the COMAH SRAM has been revised
- Investigation
  - the Response Framework for NIS Notified Incidents has been produced

How do we Regulate

- Enforcement
  - enforcement remains in line with the EPS
  - but the EMM causes difficulty
    - “risk” is different in the cyber world
  - guidance on applying the EMM has been produced for Cyber Security

Cyber Security – the OG

- Cyber Security for Industrial Automation and Control Systems (IACS) – Edition 2
  - http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf
- Cyber Security Management System
- Define the IACS
  - IT and OT
- Risk assessment
- Countermeasures

Summary

- Cyber Security
  - malicious intent
  - threat & vulnerability
- Major Hazard Regulations
- NIS Regulations
- HSE Operational Guide