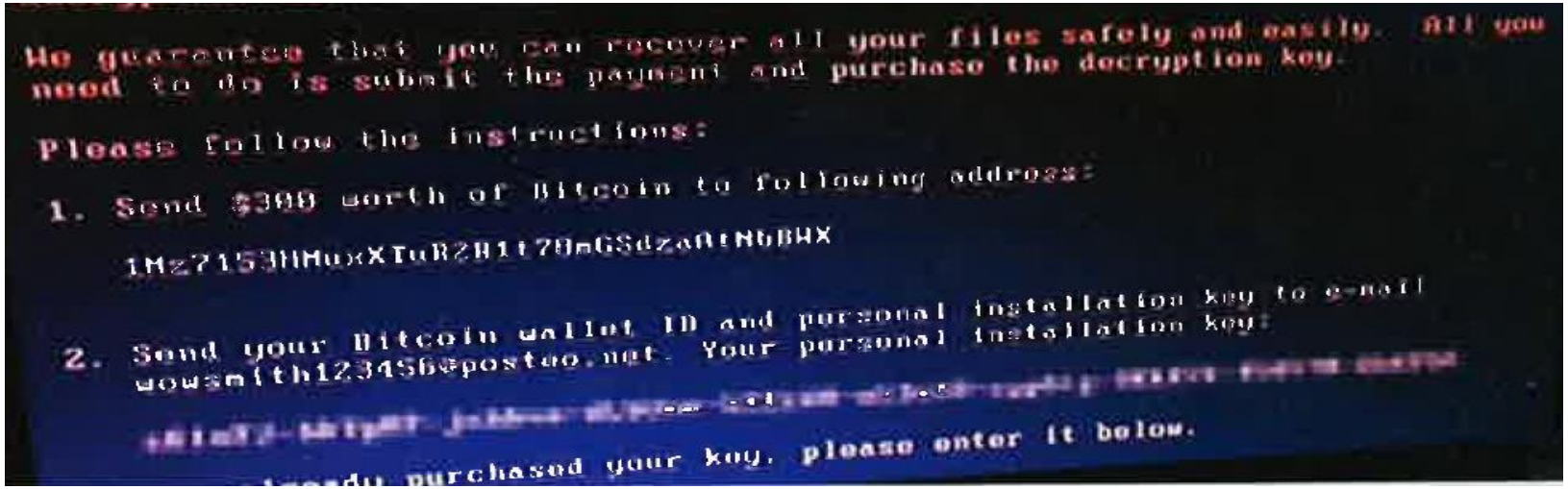
Health and Safety
Executive

Cybersecurity

Sarabjit Purewal

Principal Specialist Inspector



Recap-Why cybersecurity is a risk Technology

- Increased use of programmable systems
- Convergence of technologies used for industrial automation control systems (IACS) and IT systems – OS, network protocols etc.
- Not just plant control systems – also power management, utilities, building management, phones (VoIP) etc.
- Also management systems – e-Permits, e-Procedures…
- Increased connectivity between industrial control systems and business systems and ‘the cloud’ (internet, remote access, cloud services)
- Much greater potential attack space

Recap- Why cybersecurity is a risk Increased likelihood?

- Increased capability – state actors and criminals
- Availability of hacking hardware and software ‘toolkits’ and coordination – reduced entry level
- Social engineering techniques / Spear phishing
- Average time to detect intrusion into your corporate network is months.

Ransomware attack hits Chernobyl, Cadbury, Maersk

RADIATION monitoring systems at the Chernobyl nuclear plant were put out of action by a ransomware attack which began in Ukraine on 27 June and hit companies around the world.

Chernobyl workers had to manually monitor radiation after the cyberattack knocked out the operation's Windows-based systems.

The attack, a modified form of existing *Petya* ransomware, dubbed by some security firms as *NotPetya* or *Nyetna* to distinguish it, was first reported in Ukraine. It spread around Russia, Europe and Australia affecting firms including Rosneft, Merck, Reckitt Benckiser and Beiersdorf.

Victims were told they must pay US$300 in Bitcoin to recover their encrypted files.

The Maersk Group said IT systems went down across its business units including its oil and drilling activities, though they were "not operationally affected", while local news in Australia reported that computers at a Cadbury factory in Hobart owned by Mondelez were displaying messages demanding payments to release files.

There is no clear indication of who was behind the latest attack.

The Chemical Engineer (July / August 2017)

Why cybersecurity is a risk Design

- Traditional design concepts based upon independent layers of protection, i.e. the likelihood of all the protection layers failing at the same time is very low.
- Risk assessments didn’t consider multiple failings or malicious intent as credible.
- In reality, we know that accidents are more often due to common cause or systemic failures (inadequate functional safety management, competence leading to human error)
- Cyber attack (intentional or otherwise) is another potential common cause failure.

Recap- What are the risks?

- **Safety / Environmental** – increased risk of accident
  - Mal-operation or loss of a control system leading to an unsafe state- an initiating event
  - Mal-operation or loss of a safety system such that it does not operate- protection layers fail
  - Loss of other utilities – power, comms etc. (for incident response)
  - All can occur at the same time → common cause failure

– regulated by HSE and the CA (for COMAH sites)

Recap- What are the risks?

- **Business** – Loss of data, intellectual property – for business to manage (GDPR applies to certain sensitive data) – not regulated by HSE
- **Critical National Infrastructure (CNI)** – e.g. loss of power, utilities – to be regulated under new NIS directive from May 2018. HSE discharging CA functions under agency agreement to BEIS for the energy sector

Guidance applicable to process sector

- Lots of good guidance available, but it can be overwhelming, and it's not all limited to safety and environmental risks.
  - ISA-TR84.00.09-2013- Security Countermeasures Related to Safety Instrumented Systems (SIS).
  - National Cyber Security Centre – Security for Industrial Control Systems
    www.ncsc.gov.uk/guidance/security-industrial-control-systems
  - NIST Publication 800-82 – Guide to Industrial Control Systems (ICS) Security
    nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
  - 10 steps to Cyber security
    https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Standards for process sector

- Functional safety. IEC 61511 Ed 2 has specific requirements for cybersecurity threats. This is the benchmark Standard HSE uses for safety instrumented systems.
- Security standards developing

  IEC 62443. Note this is not limited to functional safety.
  - Part 1: Framework and threat-risk analysis
  - Part 2: Security assurance
  - Part 3: Security requirements
  - Part 4 Relevant to system integrators.

HSE Operational guidance (OG)

- Why was this needed
  - Provides a regulatory and technical framework which did not exist.
  - For specialist HSE C&I specialist inspectors – a basis against which we will train and this is what we will regulate against for H&S risks
  - It provides for proportionate risk reduction and one means to demonstrate ALARP which other guidance does not cover.
  - For MH regulated industries – could provide one means of compliance.
  - Consistent with the wider available guidance (which is a moving target)
  - http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

HSE Operational guidance (OG)

- Some of the considerations we had in mind
  - It needs to be achievable and understandable by our inspectors
  - It is not the end result – cyber attacks and risk is changing rapidly over time
  - Target the ‘low hanging fruit’ – i.e. simple good practice measures where risk is highest.

Current status of HSE OG

- Published on HSE website in March 2017
- Consultation with industry, trade bodies, institutions, other Government departments and other interested parties
- Trial inspection at a range of sites completed.
- Update of the OG after the trials and to align with NIS guidance.

Trials

- Test the OG in the field
- Provide an indication of the sector
- Draft report completed and shared with trade bodies. Key findings and recommendations for industry, HSE and joint industry/HSE recommendations.
- Cover verbally.

OG revision

- Operator feedback on usability. More information and guidance on meeting requirements, particularly on management systems
- NIS requirements incorporated
- Aligned to the NCSC CAF framework
- Risk assessment simplified
- Controls aimed initially at lower risk only- managed approach
- Small period for comments before publication

NIS and COMAH requirements

- OG covers both requirements
- Key difference is risk assessment. Highest risk determines the control measures
- Management systems and control measures common to both NIS and COMAH
- Expect industry to carry out single exercise where NIS and COMAH is applicable.
- Single inspection from HSE to cover both.

NCSC CAF framework

- Cyber Assessment Framework published by NCSC based on principles of protect, detect, and respond.- See NCSC website
- OG now aligned to these principles- more presentational than a change in requirements.

Simplified risk assessment

- Concept of likelihood for cyber risk
- Use of vulnerability (exposure and difficulty), and consequence to identify risk
- Identification of critical assets for control measures

Control measures- managed approach

- It is recognised that improvements will take time to implement, and
- The landscape and understanding is developing.
- HSE has taken the approach that having completed the risk assessment and identified the critical assets and risk, that Operators will implement the basic controls as identified in the basic CAF profile to address lower levels of risk.
- As this beds down, and as enhanced CAF profile is developed to address higher risks, industry would then be expected to put higher controls as required from their risk assessments.

Managing cybersecurity – longer term

- Designing software from security integrity as well as safety integrity- role for vendors and system integrators
- As standards develop we expect new products and security to be built in to IACS
- You have a role to play – putting security requirements into project requirements etc. (intelligent customer)
- Until then and for legacy systems – you can take steps to address basic level of controls.

Next Steps – key issues for HSE

- To raise awareness in Industry so they start to address:
  - Implement CSMS
  - Ensuring staff are competent and become an intelligent customer
  - Develop adequate safety management systems that address cyber risks
  - Assess current installed systems and identify gaps
  - Put programmes in place to address risks at basic level .
- Gain an understanding of where industry is w.r.t. cyber risks
- Continue to build our own capability ahead of inspection from 2018 onwards
- Continue to develop in line with standards and NCSC guidance

Next Steps – 2018-19

- We want industry to take the lead. Assess, and manage the risks.
- Will share the findings of summary report on the outcomes from the trials
- Inspection programme for COMAH in 2018-19 starting in Q4
- NIS self assessments starting in Dec 2018 for submission in April 2019- used to assess and prioritise future inspections by HSE

Next Steps – 2018-19

- Work in partnership with and support industry
- Common approach to inspecting NIS and COMAH at a single site visit.
- NCSC is producing guidance for CA to use for NIS regulations. We will develop a common guidance between NCSC and HSE OG to ensure there are no conflicts or gaps.

Key messages

- Cyber is an increasing risk
- Industrial control and safety systems are vulnerable
- There is potential for cyber attack to lead to major accidents
- Risk can be reduced through relatively simple countermeasures
- HSE has developed internal guidance for its inspectors to regulate against but this may also be useful to Operators
- Cyber risks are a rapidly changing topic – this is a work in progress

Thank You

Questions