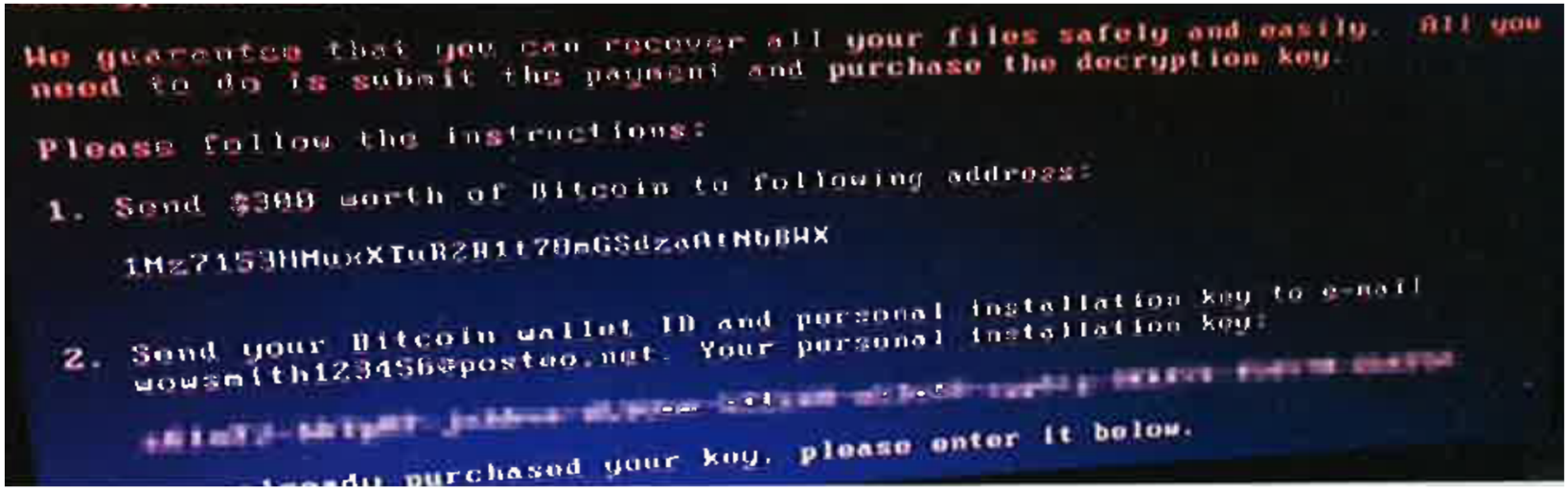
Health and Safety
Executive

Cybersecurity

Sarabjit Purewal

BSc; ACGI; PGDip; CEng; MIET

Principal Specialist Inspector



Why cybersecurity is an issue
1 - 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

Why cybersecurity is an issue 2 – 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 an issue
3 - 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.

What are the risks?

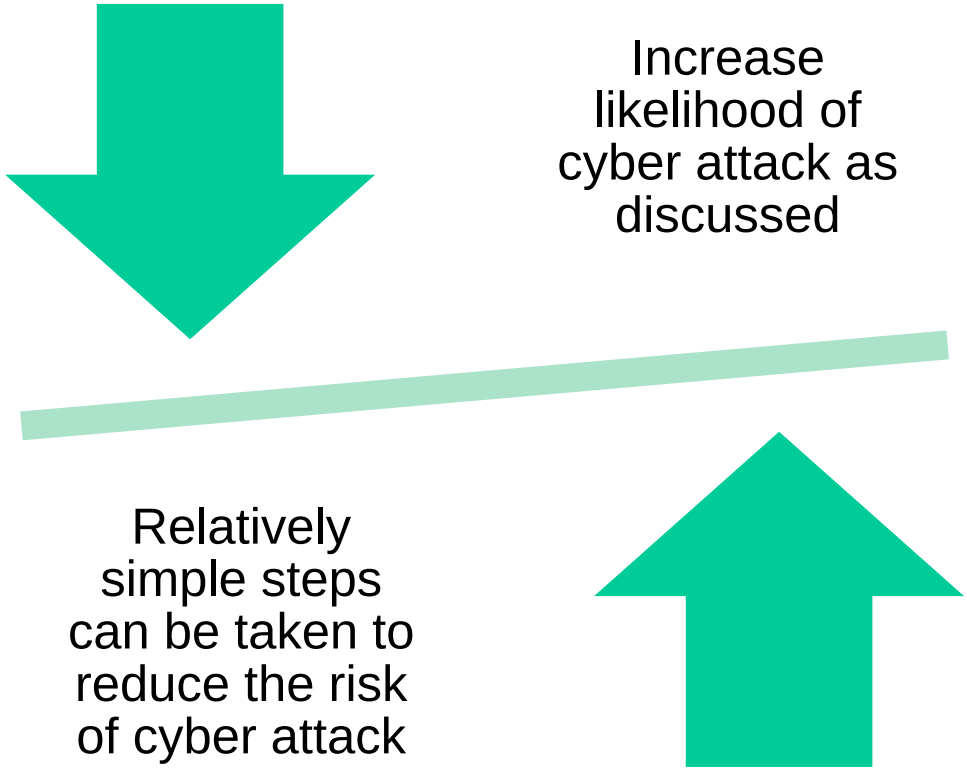
- Safety / Environmental – increased risk of accident
  - Mal-operation or loss of a control system leading to an unsafe state- an initiating event
  - Mal-operation or loss of a safety system such that it does not operate- protection layers fail
  - Loss of other utilities – power, comms etc. (for incident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

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

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 May 2018. HSE may regulate energy sector under agency agreement to BEIS

The bad news and the good news



Increase likelihood of cyber attack as discussed

Relatively simple steps can be taken to reduce the risk of cyber attack

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

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 between Nov 2017 and Apr 2018
- Expect to update the OG after the trials and to align with NIS guidance in future

Risk level

- We know many systems are vulnerable but don’t know the extent of those vulnerabilities
- The extent of the threat level is being developed by the national cyber security centre which will inform risk assessment.
- The trial inspections will test the application of the guide and also inform whether the extent of controls and systems are adequate

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 some simple steps as an end user. For example:

Some simple steps

- Do you have sufficient competence to understand the risks and how to deal with them?
- Do you know what IACS systems you have and how they are connected?
- Have you segmented IACS from other systems (e.g. with unidirectional gateways)?
- Is access controlled to minimum – physical access and authorisation (e.g. passwords)?
- Have you removed unnecessary connections, applications, expired users, USB ports that are not required etc.?
- Are you in control of remote and portable connections – e.g. vendor remote access and laptops?
- Do you apply the latest security updates – caution required when it comes to IACS but are we too cautious at the moment?
- Have you got good backups and know how to restore?

Key steps within the guide

- Cyber Security Management System (CSMS):
  - Governance (roles and responsibilities)
  - Personnel screening and recruitment
  - Competence. Fist key step.This is dependent on the role you play. Operator, vendor, systems integrator etc. have different competencies.
  - Asset and configuration management
  - Planning and procedures that cover the entire lifecycle
  - Operation, monitoring, maintenance and testing of countermeasures
  - Audit and review
  - Incident management and recovery
  - Change management

(Note part of wider Management System)

Key steps in the guide

- Defining the IACS, and splitting into zones
- Risk Assessment
  - RA as we know it is not easily applied to cyber threats
  - Current methodologies not effective
  - Guidance gives a simple qualitative approach to follow to allow inspectors to consider what is reasonably practicable
  - Security threats identified in the guide
  - Proportionate to where the IACS risk reduction measures are located (BPCS and SIS but also power management etc.)
- Define and plan to implement countermeasures
  - Looking for defence in depth
  - Also recognises what is reasonable for legacy systems

Key issues

- To raise awareness to Industry so they start to address the issues.
  - 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 close those gaps.
- Ensure industry has sufficient information and guidance about the issues and compliance.
- What support do you require to do the above and what has been your experience so far?
- In order for you to become competent are the right type of training and guidance available that address your needs. Key competencies for Operators is to be able to specify the systems, assess that the right systems have been delivered and to operate and maintain the systems.

Key issues

- To specify systems requires risk assessment and controls that are proportionate to the risk.
- We know there are current gaps in both risk assessment and designing systems with proportionate controls, and need to develop our approaches.
- Is there a common understanding between vendors/ end users on what good looks like in relation to equipment/systems that is risk based.
- What do you need to assess your current installed systems which may not have or be unsuitable to have some of the controls that modern systems have.
- Have you started or have adequate management systems for cyber security. The OG provides a comprehensive guidance on what is needed with further links to other supporting guidance.

Key issues

- We know there are gaps e.g. Risk assessment, specification and design of systems etc. What is your view on how this should be taken forward and what should your role be in that?
- There are a lot of things you can do and good guidance already available. You should have well developed safety management systems that should be updated to include cybersecurity.
- What support do you require to ensure you are an intelligent customer? Is the current training and guidance adequate and targeted to your needs. If not what else is required?

Key issues for HSE

- Work in partnership with industry through such bodies as CIA, UKPIA, TSA etc.
- Work with vendors and systems integrators to ensure systems are designed with security. Not straightforward.
- Ensure inspectors are competent to address this area.
- Joined up working with BEIS, CPNI, NCSC for a consistent approach.
- Gain an understanding of where industry is w.r.t. cyber risks (as part of the trials)

Next Steps – 2018-19

- We want industry to take the lead. Assess, and manage the risks.
- Will develop an assessment guide to use to assess systems. NCSC will be publishing a cyber assessment framework
- Will publish a consolidated report on the outcomes from the trials
- Inspection programme in 2018-19

Next Steps – 2018-19

- Currently in discussions with BEIS to discharge the CA responsibilities under NIS. If successful we will have a common approach to inspecting NIS and COMAH at a single site visit.
- NCSC has produced technical guidance for CA to use for NIS regulations. If HSE works on behalf of BEIS 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 you
- Cyber risks are a rapidly changing topic – this is a work in progress

Thank You

Questions