Civil Nuclear Security

Robert M Rodger
Nuclear Triple S

Potential Hazards from

- Normal Operations and Accidents
- Diversion of Nuclear Materials and Technologies
- Malicious Actions

Safety

Safeguards

Security
Nuclear Security

- Gates
- Guards
- Guns

- Legislation and Policy
- Physical Protection System
- Cyber Security
- Information Security
- Personnel Security
# Objectives and Essential Elements of a State’s Nuclear Security Regime

## Sabotage and Unauthorised Removal

<table>
<thead>
<tr>
<th>Threat</th>
<th>Protection</th>
<th>Response</th>
<th>Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Characterisation</td>
<td>Physical</td>
<td>Armed Response</td>
<td>Security Plan</td>
</tr>
<tr>
<td>Threat Assessment</td>
<td>Technical</td>
<td></td>
<td>Nuclear Security Culture</td>
</tr>
<tr>
<td>Design Basis Threat</td>
<td>Information Security</td>
<td>Unarmed Guards</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>Assessment Methodologies</td>
<td>Cyber</td>
<td></td>
<td>Sustainable Programme</td>
</tr>
<tr>
<td></td>
<td>Personnel Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nuclear Material Accountability and Control</td>
<td>Contingency Plans</td>
<td></td>
</tr>
</tbody>
</table>

## Practical Implementation

- New Build
- Reactors
- Fuel Cycle
- Decommissioning
- Disposal
- Transport
Structure of a Legislative Framework for Nuclear Security

- **Binding International Treaties, Resolutions and Conventions**
  - CPPNM

- **Non-Binding International Codes and Documents**

- **Nuclear Legislation**
  - **Peaceful use**
    - Commitment to the Peaceful use of NM
    - State system of accounting and control
  - **Criminalisation**
    - Penalties
    - Sanctions
    - Law Enforcement

- **Competent Authority**
  - Regulation
  - Licensing
  - Inspection
  - Enforcement

- **Regulatory Framework**
Legislation and Policy

• Convention on the Physical Protection of Nuclear Material
• International Convention for the Suppression of Acts of Nuclear Terrorism
  ★ Nuclear Terrorism Convention
• United Nations Security Council resolutions
  ★ 1373 (2001)
    ❖ Threats to international peace and security caused by terrorist acts
  ★ 1540 (2004)
    ❖ Non-proliferation of weapons of mass destruction

• Nuclear Industries Security Regulations (as amended)
• Anti-Terrorism, Crime and Security Act 2003

• National Objectives, Requirements and Model Standards
• Classification Policy for the Civil Nuclear Industry
• Civil Nuclear Personnel Security Standard
Defence in Depth

Preventative Controls

External Hazard

External Threat

Internal Threat

Internal Hazard

Preparedness Controls

Asset Event Risk

Consequences

Engineering activities
Maintenance activities
Operations activities
Design and Evaluation Process Outline

Define PPS requirements

Process of design and evaluation

Facility characterisation

Target identification

Threat definition

Design PPS

Physical Protection System

Detection

Intrusion detection

Alarm assessment

Access control

Alarm communication and display

Delay

Barriers

Response

Armed and Unarmed

Evaluate PPS

Adversarial Sequence Diagrams

Single Path analysis

Neutralisation analysis

Scenario analysis

Insider analysis

Final PPS design

Redesign PPS
Physical Protection System – Threat

• External threat
  ★ Terrorists
  ★ Protestors
    ❖ Demonstrators
    ❖ Activists
    ❖ Extremists
  ★ Criminals

• Internal threat
  ★ Insider is anyone with authorized, unescorted access who could:
    ❖ act alone or in collusion with external threat
      ➢ May be passive or active
      ➢ May be violent or nonviolent
Physical Protection System – Threat

- Motivation
  - Ideological
  - Personal
  - Economic

- Intention
  - Theft
  - Sabotage

- Strategies
  - Stealth
  - Deceit
  - Force

- Current Trends and tactics

- Capabilities
  - Group size
  - Weapons
    - Specific types
  - Explosives
    - Types and quantities
  - Tools
    - Hand and power tools
  - Transportation
    - Land, air, water
  - Collusion from insider(s)
  - Skills
  - Funding
  - Support structure
Target Identification

- Nuclear Material
- Other Radioactive Materials
- Containment
- Cooling
- Control of Criticality
- Unacceptable Radiological Consequences
  ★ Vital Area Identification
  ★ Malicious Action Assessment
**Vulnerability Assessment**

<table>
<thead>
<tr>
<th>Planning</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Cost</td>
<td>Schedule</td>
<td>Risk Identification</td>
<td>Security Classification</td>
<td>Assets</td>
<td>Personnel Security</td>
<td></td>
</tr>
</tbody>
</table>

**Information Collection**

| Characterisation - Facility or Activity | Threat Definition | Target Identification |

**Conducting an Assessment**

| Manual Assessment | Computer-based Processes | Modelling and Simulation (M&S) | Data Library Management | Inspection | Physical and Technical Testing | Table-Top and Live-Play Exercise |

**Overall Assessment of Security**

| Strength | Weaknesses or Deficiencies | Enhancements |

**Are Security Requirements Met?**

| Yes | Compliance | No | Non-compliance |

**Additional Objectives Identified?**

| Yes | No |
Vulnerability Assessment

• Prescriptive
• Qualitative
• Quantitative (Pathway Analysis)
• Modelling and Simulation
• Exercising
  ★ Table Top
  ★ Live Play
Vulnerability Assessment Modelling and Simulation

MODEL
- Detection Systems
  - Infrastructure
  - Security layers
  - Elevation/Terrain
- Barrier Systems
  - Perimeter structure
  - Doors & Access Control
  - Delays
- Response Force
  - Patrol & response
  - Concept of operations
  - Capabilities & training

CHARACTERIZE

SIMULATE
- Automatically simulate an incident with numerous threat profiles
- Evaluate 100s of scenarios varying in security configurations and facility operations within hours rather than weeks

ANALYZE
- Visuals of attack paths & heat maps
- Detection, interruption, & neutralization analysis
- Enterprise Metrics

MODIFY
- Quickly add barriers or move officer’s post
- Compare effectiveness for each modification with the “as-is” security system design
Physical Protection System - Protection

- Physical
- Technical
- Information Security
- Cyber Security
- Personnel Security
- Nuclear Material Accountancy and Control
Physical Protection System – Response

• Armed Response
• Contingency Plans
• Concept of Operations

• Denial
• Containment
• Recapture
• Pursuit
• Recovery

• Guards
• Access Control
• Search
• Pass Issue
• Alarm Testing
• Alarm Assessment
• Control Room Operations
Physical Protection System – Security Management

- Security Plan
- Nuclear Security Culture
- Quality Assurance
- Sustainability
Security Management – Nuclear Site Security Plan

- Submit plan for approval
- Regulator reviews plan
- Approves
- Plan implemented
- Inspection
- Threat
- Annual Review
- Plan amended (if necessary)
- Regulation and Policy
Security Management – Quality Assurance and Sustainability
Cyber Security – Layers

- Internet
- Non-critical Systems
- Proprietary or Sensitive Data Systems
- Emergency Preparedness Systems
- Security Systems
- Safety and Control Systems
Computer Based Systems Important to Safety (CBSIS)

FIG. 4. Plant equipment in terms of safety function.

a In this context, an ‘item’ is a *structure, system or component.*
Are there any questions?

Thank you for listening
Cyber & Information Security

Institute of Physics Nuclear Industry Group
The Satellite Applications Catapult, Electron Building, Harwell
15 November 2016

Graham Urwin  MSc  CPP
Security Manager
Radioactive Waste Management
Agenda

• Definition of Cyber & Cyber Security
• HMG’s National Cyber Security Strategy
• Recap of the Cyber environment
• Cyber security objectives & 10 steps
• Cyber Essentials & Cyber Essentials PLUS
• Cyber incident reporting & response
• Current UK trends
• Social Engineering
• Cyber & Cyber Security Resources
Definitions

Cyber:
“Relating to or characteristic of the culture of computers, information technology … the space of virtual reality; the notional environment within which electronic communication (esp. via the Internet) occurs.” [OED, 30/08/16]

Cyber Security:
“The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user’s assets … protecting Confidentiality, Integrity, and Availability.” [Office for Nuclear Regulation, Civil Nuclear Security CSORS, August 2016]
# National Cyber Security Strategy 2016-2021

<table>
<thead>
<tr>
<th>THREATS</th>
<th>VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber criminals (&amp; competitors)</td>
<td>Expanding range of connected devices</td>
</tr>
<tr>
<td>States &amp; state-sponsored actors</td>
<td>Poor cyber hygiene &amp; compliance</td>
</tr>
<tr>
<td>Terrorists</td>
<td>Insufficient training &amp; skills</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Legacy &amp; unpatched systems</td>
</tr>
<tr>
<td>‘Script Kiddies’</td>
<td>Availability of hacking resources</td>
</tr>
</tbody>
</table>

**STRATEGY:**

1. **Defend** the UK against evolving cyber threats and respond to incidents.
2. **Deter** aggression in cyberspace by making the UK a hard target.
3. **Develop** an innovative cyber security industry.
4. **International Action** to advance UK economic & security interests.

Investing £1.9 billion over the next 5 years
Recap – the layers of Cyber Security:
Recommended cyber security objectives:

- an effective Governance regime
- visible leadership and a positive culture
- information risk management process
- value, identify, locate, account for Information
- use technology to protect information in transit & at rest
- suitable personnel vetting controls
- suitable physical security controls
- maintain & test cyber incident response procedures
Combating Cyber Attacks / 10 Steps to Security

What you can do to combat cyber attacks

Reducing the Impact
Most cyber attacks are composed of four stages: Survey, Delivery, Breach and Affect. The following security controls, applied at each stage of an attack, can reduce your organisation’s exposure to a successful cyber attack.

Survey

User Education

Users are the first line of defense against cyber attacks. It is essential to educate users on recognizing and responding to potential threats.

Network Perimeter Defences

Can block malicious code from entering the network. This can be done through firewalls, intrusion detection systems, and other security solutions.

Malware Prevention

Can block attacks on websites, or any site that a user visits. This can prevent users from downloading malicious software.

Password Policy

Can prevent users from using weak or easily guessable passwords. This can reduce the likelihood of a successful attack.

Secure Configuration

Can ensure that a system is configured securely. This can prevent attackers from gaining access to sensitive information.

£600K-£1.2m

Average cost of security breach

Delivery

Network Security

Protect your networks from attacks. Defend the network perimeter, filter out unauthorized access and malicious content. Monitor and report security threats.

User Education

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware Prevention

Produce relevant policies and establish anti-malware defenses across your organisation.

Removable Media Controls

Produce a policy to control access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure Configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define baseline builds for all devices.

Breach

Making the right decisions is crucial in the event of a breach. Having a robust incident management plan in place can help reduce the damage caused by an attack.

Set up your Risk Management Regime

Access the risks to your organisation’s information and systems with the same vigour you would for legal, regulatory, financial, or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Determine your Risk Appetite

Produce supporting risk management policies

Managing User Privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and event logs.

Incident Management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc
‘Cyber Essentials’ & ‘Cyber Essentials PLUS’

Mandatory for Central Civil Government contracts after 1 October 2014 which feature handling of personal information and provision of certain ICT products and services. It defines controls which provide organisations with basic protection from the most prevalent forms of threat coming from the internet.
A Cyber Incident is defined as “a single or series of unwanted or unexpected cyber events that have a significant probability of compromising business operations and threatening cybersecurity” …:

- Denial of Service
- Malicious code
- Improper usage (organisations should take a judgement)
- Scans/probes/attempted access
- Technical failure/misconfiguration issue
- If in doubt it should be reported, to e.g.: NDA, NCSC and ONR.

Current UK cybersecurity trends

Identity fraud:
• personal identity stolen by criminals to obtain goods or services by deception

Online extortion demands (from the ‘Lizard Squad’ or ‘RepKiller Team’):
• threaten ‘Denial of Service’ attacks unless a ransom is paid

iTunes payment card fraud:
• so far this year victims have paid fraudsters over £520,000 in iTunes Gift Cards

Online dating sites:
• in 2015 ‘cyber criminals scam love-struck Brits out of £27 million’ (~£10,000 each)

Phishing emails becoming more sophisticated:
• posing as real companies that you deal with, often addressing you by name
Social Engineering

In the context of cyber and information security:

• refers to persuading people to divulge information or manipulating individuals to perform certain actions …

Uses a CONFIDENCE TRICK:

• to gather information and is often a step in a complex scheme used to gain information on employees, unauthorised access to IT systems, premises or to gain information to enable a commercial advantage …

In defence you can:

• raise awareness amongst staff, advising them against divulging any information to an unsolicited caller, unless trusted and can be verified.
<table>
<thead>
<tr>
<th>Resources</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Fraud</strong></td>
<td>National Centre for reporting online fraud and cyber-crime.</td>
</tr>
<tr>
<td><img src="http://www.actionfraud.police.uk" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td><strong>GetSafeOnline</strong></td>
<td>Advice and guidance to protect yourself and your business against online fraud, identity theft, and other cyber threats.</td>
</tr>
<tr>
<td><img src="https://www.getsafeonline.org" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td><strong>National Cyber Security Centre</strong></td>
<td>Part of GCHQ, NCSC is the UK’s authority on cyber security, acting as a bridge between industry and government. Combines Government cyber bodies CESG, CCA, CERT UK, CPNI.</td>
</tr>
<tr>
<td><img src="https://www.ncsc.gov.uk" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Essentials</strong></td>
<td>Cyber Essentials is a Government and industry-backed standard which protects your business against cyber threats.</td>
</tr>
<tr>
<td><img src="https://www.cyberaware.gov.uk/cyberessentials" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td><strong>Office for Nuclear Regulation</strong></td>
<td>ONR independently regulates nuclear safety and security at nuclear licensed sites in the UK. ONR’s duty is to ensure that the nuclear industry controls its hazards effectively, has a culture of continuous improvement and maintains high standards.</td>
</tr>
<tr>
<td><img src="http://www.onr.org.uk/index.htm" alt="Image" /></td>
<td></td>
</tr>
</tbody>
</table>
Cyber & Information Security

Thank You

Graham Urwin  MSc CPP
Security Manager
Radioactive Waste Management