Office for Nuclear Regulation

Regulation of Cyber Security across the UK Civil Nuclear Sector

US NRC RIC Cyber Security Panel – 10 March 2020

Paul Shanes
Superintending Inspector
Professional Lead for Cyber Security

1

Office for Nuclear Regulation

Scope

- Introduction to ONR
- Our Legislative Remit
- Our Transition to Outcome Focused Regulation
- The Graded Approach to Cyber Security
- Government Strategy & Direction
- Our View of Cyber
- Current and Future Challenges
- What We've Learnt – A Radical Departure
- Questions

Office for Nuclear Regulation

Introduction to ONR

3

Office for Nuclear Regulation

Our Legislative Remit

- **Nuclear Industries Security Regulations 2003**
  - Licensed sites are required to have a Site Security Plan approved by ONR.
  - The arrangements in the security plan are to be complied with at all times.
  - Arrangements within the plan must cover the security of Nuclear Material and Sensitive Nuclear Information.

Importantly, the Regulations do not state what those security arrangements should be.

Office for Nuclear Regulation

Our Transition to Outcome Focused Regulation ~ Step 1

- **Technical Guidance & Recommendations 2007**
  - Intended to provide useful guidance on what security standards, procedures and arrangements may be appropriate.
  - Not prescriptive, however licensees copied or referenced large sections into their own security plans.
  - Led the regulator and industry down a path of prescription.

Office for Nuclear Regulation

Our Transition to Outcome Focused Regulation ~ Step 2

- **National Objectives, Requirements & Model Standards 2012**
  - Goal setting and objective focused.
  - Flexible and enabling to encourage innovation.
  - However, too tactical and directive in tone.
  - Lack of clarity between the objectives, requirements and model standards.
  - Conditions not right to exploit the opportunity – culture of prescription embedded.

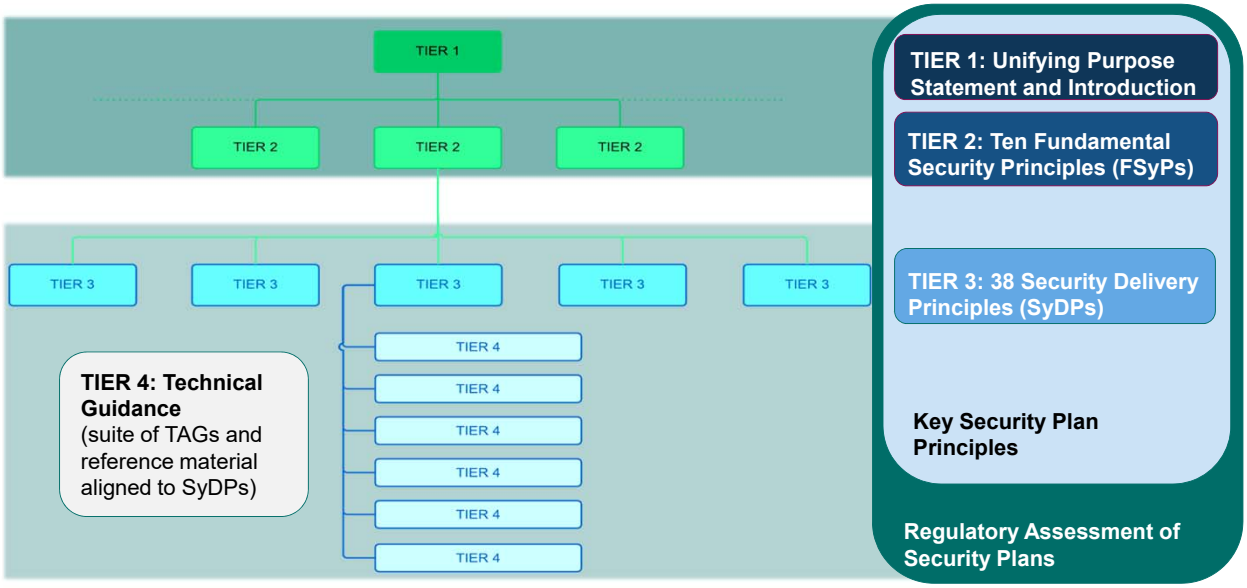
Office for Nuclear Regulation

Our Transition to Outcome Focused Regulation ~ Step 3

- **Security Assessment Principles 2017**
  - Written for ONR inspectors to assess adequacy of security plans – Not a manual for licensees!
  - High level and principle based – no model standards.
  - Greater emphasis on strategic issues (e.g. governance, culture and competence management).
  - Forced licensees to understand risks and fully justify adequacy of security arrangements.
  - Act as a framework for making consistent regulatory judgements on the adequacy of security arrangements.

Office for Nuclear Regulation

Security Assessment Principles



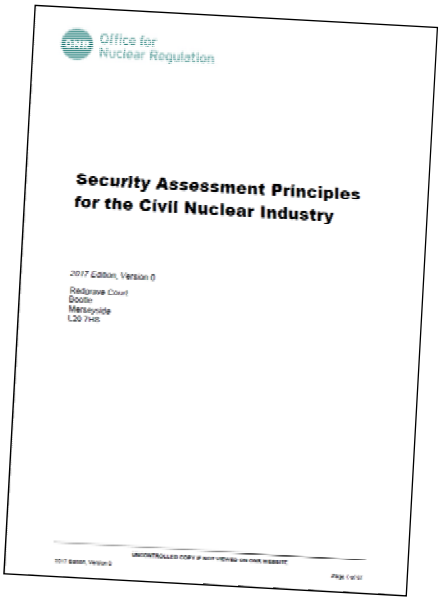
"dutyholders are responsible for the leadership, design, implementation, operation and maintenance of security"

Office for Nuclear Regulation

Fundamental Security Principle 7

"maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to…"

- **Information:** protect confidentiality, integrity and availability;
- **Nuclear Technology:** ensure that technology is able to deter, detect and defend against disruptive challenges (such as cyber attacks);
- **Resilience:** contain/defeat, mitigate the effects of, and recover from, disruptive challenges.



Office for Nuclear Regulation

CS&IA High Level Regulatory Expectations

FSyP 7 - Cyber Security and Information Assurance	Effective Cyber and Information Risk Management	SyDP 7.1
Dutyholders should maintain arrangements to ensure that CS&IA risk is managed effectively.		
FSyP 7 - Cyber Security and Information Assurance	Information Security	SyDP 7.2
Dutyholders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets.		
FSyP 7 - Cyber Security and Information Assurance	Protection of Nuclear Technology and Operations	SyDP 7.3
Dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.		
FSyP 7 - Cyber Security and Information Assurance	Physical Protection of Information	SyDP 7.4
Dutyholders should adopt appropriate physical protection measures to ensure that information and associated assets are protected against a wide range of threats.		
FSyP 7 - Cyber Security and Information Assurance	Preparation for and Response to Cyber Security Incidents	SyDP 7.5
Dutyholders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber attack), non-malicious leaks and other disruptive challenges.		

But…good Cyber Security…

…is not just about good Cyber Security

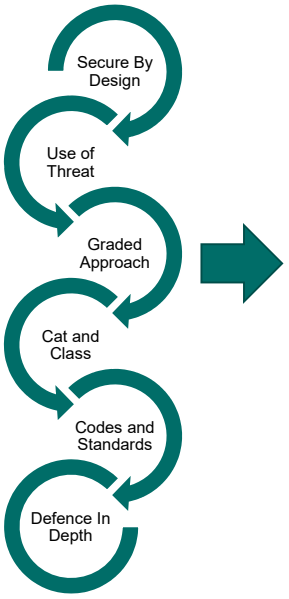
Office for Nuclear Regulation

Security Assessment Principles

Strategic Enablers - Objectives focused on creation of the right conditions to support high reliability, disciplined operations.		**Secure Operations** - Objectives focused on the implementation and maintenance of nuclear security.	
FSyP I	Leadership and Management for Security	**FSyP VI**	Physical Protection Systems
FSyP II	Organisational Culture	**FSyP VII**	Cyber Security & Information Assurance
FSyP III	Competence Management	**FSyP VIII**	Workforce Trustworthiness
FSyP IV	Nuclear Supply Chain Management	**FSyP IX**	Policing & Guarding
FSyP V	Reliability, Resilience and Sustainability	**FSyP X**	Emergency Preparedness and Response Arrangements

Office for Nuclear Regulation

The Graded Approach to Cyber Security



1. Dutyholders categorise assets:

SNI (includes IT)

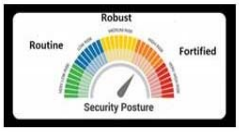
Critical	Large Off Site Release
Major	Limited offsite release
Significant	Significant release in area of plant not expected by design
Minor	Minor Contamination in plant area not expected by design

OT

2. Determine Outcome:

1	Complete confidence it will protect against attack
2	High level of confidence it will protect against attack
3	Resistance to attack
4	Identify an attack has taken place

3. Apply:



Posture

to each

Identify
Protect
Detect
Respond
Recover

Function

Office for Nuclear Regulation

What Constitutes Relevant Good Practice

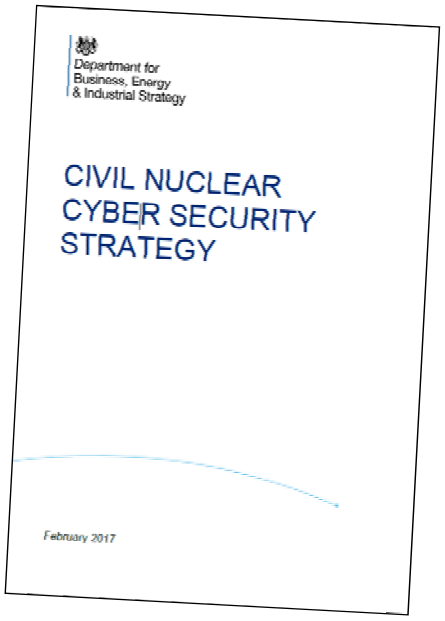
Standard	Definition	
Defined	Minimum standard specified by Acts, Regulations, Orders and Approved Codes of Practice (ACoP). e.g. Nuclear Industries Security Regulations 2003.	
Established	Codes of Practice and other standards linked to legislation, published or commonly known standards of performance interpreted by regulators or other specialists, industry or other organisations. e.g. Licence Conditions, Security and Safety Assessment Principles, Cabinet Office Security Policy Framework, TIGs, TAGs, IAEA Standards, NIST, ISO Standards, NCSCs CAF, Cyber Essentials, CPNIs CMAT.	
Interpretative	Standards which are not published or available generally, but are examples of the performance needed to meet a general or qualified duty. e.g. Industry Cloud Security Principles.	

Office for Nuclear Regulation

Government's Civil Nuclear Cyber Security Strategy

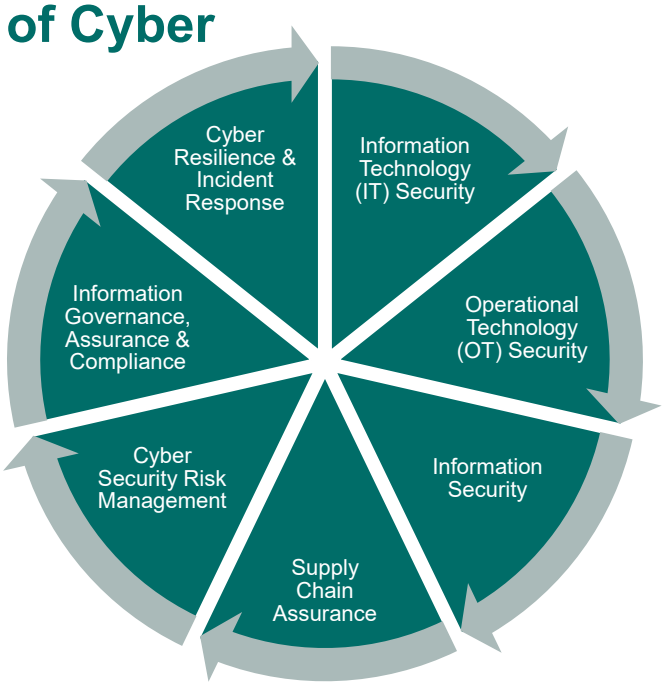
Four distinct activities:

1. Deliver a comprehensive understanding of the cyber vulnerabilities across the civil nuclear sector.
2. Continuously mitigate identified issues and vulnerabilities.
3. Improve the sector's capability to detect, respond to, and recover from cyber incidents.
4. Ensure sufficient resources are allocated to cyber security and resilience.



Office for Nuclear Regulation

Our View of Cyber



Office for Nuclear Regulation

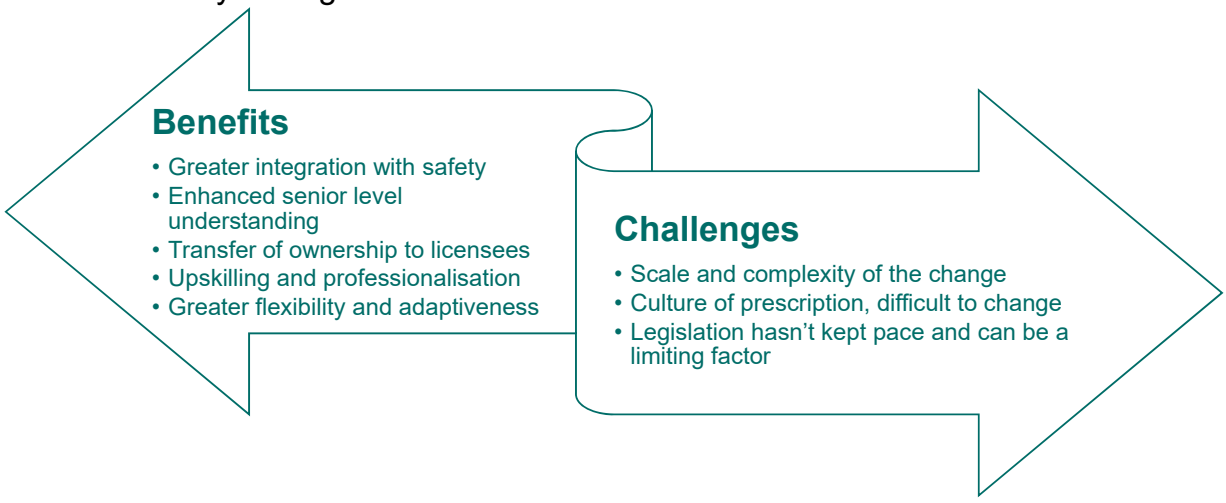
Current and Future Challenges…

- Legacy OT systems weren't designed to be exposed to the internet, and it isn't always obvious when they have been.
- Convergence with enterprise IT – new OT can be attacked like enterprise IT.
- Complexity and rate of change of technology – we lack natural instincts.
- Software always has bugs – no amount of testing can find them all.
- Vulnerabilities in the supply chain – an ever increasing problem.
- High risk vendors vs the need for dutyholders to encourage innovation.
- Vulnerability data available from governments, vendors, specialist companies, presenting both an opportunity and a challenge.
- Insufficient cyber-trained staff (globally), and large proportions of the population (globally and within nuclear businesses) do not understand the implications of their personal actions on organizational cyber security.

Office for Nuclear Regulation

What We've Learnt…A Radical Departure

- High level and principle based – no model standards
- Greater emphasis on strategic issues (e.g. governance, culture and competence management)
- Forced licensees to understand risks and fully justify adequacy of security arrangements



Office for Nuclear Regulation

Thank You

Any Questions?