example; hardening systems and improving intrusion detection systems) or by strengthen physical security around an asset (for example restricting access to servers).

Our approach

- Identifying the sector's most critical systems and the potential impacts should these systems be subject to a cyber attack
- Identifying and assessing vulnerabilities
- Monitoring cyber threats by assessing and analysing pertinent intelligence
- Sharing intelligence and assessments
- Promoting uptake of threat intelligence
- Working with international partners to leverage and share expertise and knowledge

2. Continuously mitigate identified issues and vulnerabilities

What is happening now?

The civil nuclear sector have identified assets that are critical for nuclear safety and have processes in place for managing any risks identified in there systems. Successfully mitigating cyber risks is a process of continuous improvement, and the flexible approach afforded by outcome-focused regulation used in the UK offers real benefits to making this possible. It enables the industry to own and develop security solutions which most appropriately meet their unique situations as well as any risks not associated directly to nuclear regulations for safety and security (for example their own intellectual property, or issues of commercial sensitivity).

Aim

For amendments to nuclear plants and the new generation of nuclear plants to be cyber secure by design and implementation. The nuclear new build programme offers an opportunity to mitigate the cyber security risk in the design phase by a combination of both physical and cyber controls so that nuclear new build will be cyber secure by design.

For duty holders to work with the civil nuclear supply chain to ensure that the supply chain to have the appropriate level of cyber security in their risk profile. It is important that as the civil nuclear sector improves their civil nuclear capability they also work to improve the capability of their supply chain. Duty holders are best placed to work with their supply chain to support this change. This will allow duty holders to better understand the cyber risk that they are carrying in their supply chain whilst simultaneously ensuring that the appropriate standard is being met.

Our approach

- Implementing and refreshing appropriate good practice, controls, and mitigations
- Ensuring that systems and digital assets (including data) are proportionately and appropriately protected
- Supporting industry with access to technical assistance and tools
- Developing nuclear new build and other new facilities so that they are cyber secure by design
- Enhancing cyber security throughout the civil nuclear supply chain
- Identifying processes to provide appropriate assurance for (critical) digital assets

3. Improve the sector's capability to detect, respond, and recover from cyber incidents

What is happening now?

The civil nuclear sector has a strong safety culture and a mature exercising programme. To date these programmes have focused on a safety incident or mechanical failure. However industry is in the process of building up its experience in responding to a cyber incident. This has included a number of table top exercises where the communication channels between duty holders and Government have been tested. The lessons learned from these exercise have been tested as part of a technical exercise. This raised personnel's understanding of the challenges a cyber incident poses for governance (for example smaller command chains, and the importance of record keeping), communication between the different parts of incident response (for example personnel manning perimeter defence and intrusion detection systems) as well as the need to fully understand what is on your network.

Aim

For organisations in the civil nuclear sector to include cyber within their exercise programme. The sector will benefit from including cyber within their incident response progamme. This would include ensuring that as part of all incidents cyber is considered as a potential vector and the necessary precautions are taken before it is ruled out. In addition, Government, industry, the regulator and other stakeholders should develop appropriate lines for a cyber incident (including speculation that cyber is the cause for a non-cyber incident).

For the civil nuclear sector to be resilient to a cyber attack. By taking part in technical exercising the sector will gain an understanding of what an adversary will do when attempting to compromise a system, and test whether they would detect an intrusion. This should result in sites being able to improve their protective monitoring and detection systems as well as provide a potential opportunity for Information Technology and Operational Technology personnel to get a broader understanding of the difference between their roles. In addition, the sector will develop plans to identify how it will respond and recover from an incident effecting one of its critical digital assets.

Our approach

- Ensuring that the sector has the capability to detect, defend against, and effectively respond to cyber security incidents
- Ensuring that robust incident management procedures are in place, mature, and well implemented across the sector
- Testing complex cyber incident response capability through exercising

- Promoting industry's sharing of vulnerability/incident information and good practice
- Sharing lessons learned across CNI sectors

4. Ensure sufficient resources are allocated to cyber security and resilience to transform capability in the sector

What is happening now?

The sector currently has a mature and established safety culture, which has supported their cyber position. Sites are subject to inspections to ensure that they meeting their security and safety obligation. All sites have programmes in place to improve both their cyber and physical security. However, the resources allocated to cyber are usually a small percentage of the total budget

Aim

Ensuring that boards and executive directors understand their cyber risk leadership responsibilities. The improvement in the distribution of threat information from objective one will support this objective. This will allow non-executive directors to hold boards to account, and boards to make better decisions on how much resource to provide to mitigate the cyber risks, and ensure that organisations future plans are not increasing the organisation cyber risk without taking appropriate action.

Growing the base of civil nuclear cyber security personnel. The civil nuclear sector needs to attract cyber security professionals now and in the future. To achieve this there needs to be a clear career path for cyber security professionals that are interested in joining the sector. This will be achieved by the sector taking an active role in the Cabinet Office's cyber apprentice scheme. This will need to include a clear path for how a job holder can develop their capability and gain increasing responsibility if desired. This will be supported by providing cyber training to all professionals within the organisation, including graduates and operational technology personnel as well as encouraging regular UK personnel attendance at appropriate IAEA courses.

Our approach

- Ensuring that the regulatory framework is enabling and fit for purpose
- Promoting an integrated approach to security and safety
- Ensuring that boards and executive directors understand their cyber risk leadership responsibilities and accountabilities with regard to controls and mitigations
- Ensuring that boards fully understand cyber risks, risk controls and risk appetite
- Growing the base of suitably qualified cyber security professionals in the sector
- Improving the cyber security proficiency and awareness of both specialists and generalist staff
- Growing cyber security as a fundamental component within existing organisational cultures

Annex B: Acronyms

BEIS	Department for Business, Energy and Industrial Strategy
CERT-UK	Computer Emergency Response Team UK
CISO	Chief Information Security Officer
CNC	Civil Nuclear Constabulary
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
CNS	Civil Nuclear Sector
IT	Information Technology
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NCSP	National Cyber Security Programme
NDA	Nuclear Decommissioning Authority
ONR	Office for Nuclear Regulation
OT	Operational Technology
SIA	Security and Intelligence Agencies

Department for Business, Energy & Industrial Strategy
3 Whitehall Place, London SW1A 2AW
www.gov.uk/beis