Contribution ID: **298** Type: **Paper**

How a Goal-Setting Approach Enables Effective Cyber Security Regulation

ONR is the UK's independent nuclear regulator of nuclear safety, security and conventional health and safety at licensed nuclear sites in GB. This includes the existing fleet of operating reactors, fuel cycle facilities, waste management and decommissioning sites.

This paper will explore how our goal-setting approach enables effective cyber security regulation by placing clear accountability on dutyholders to demonstrate effective risk identification and management; agility to operate, improve and manage emergent risks; and to deliver a supportive organisational culture that recognises the risks associated with nuclear operations in a digitised, globalised, data-rich society. It will further look at the resource requirements for the effective regulation of cyber security in this outcome-focussed way.

Through an examination of examples generated through regulator-led duty holder-supported projects, it will illustrate how an enabling regulatory attitude has pushed forward understanding of good practice in the areas of:

Assessment of Assurance in the Operational Technology Domain
Partnering with a commercial provider, through a range of exercises we aimed to learn the extent to which a regulator could expect duty holders to conduct assessment of assurance in the operational technology domain. This included consideration of nuclear safety as well as organisational considerations. The approach considered built on good practice from other sectors, and incorporated the use of a threat led approach, and the mapping and testing of security controls, security systems and technologies that cover the various stages of the ICS cyber kill chain.

Use of Commercial Products to Compliment National Intelligence

Again with a commercial partner, with developed expertise in the area of commercial threat intelligence, we sought to understand from a regulatory perspective what expectations we could have on duty holder organisations in respect of their use of commercial products as a compliment to national intelligence. Through a series of experimental products we aimed to understand how effective and continuing access and consumption of up to date threat reporting that can be used to provide education, understanding and threat-informed mitigation strategies that specifically address the threat landscape for IT and OT in the organisation.

Resourcing Effective Regulation of Cyber Security

Using the evidence from the examples the paper will examine the developing need for competent resource in duty holder organisations, the regulatory body, and technical support organisations.

ONR's own journey has seen it use contracted support from a commercial partner, as outlined previously, but additionally it has also recruited more than 10 new staff into the cyber security regulatory team over the past 4 years.

The paper will reflect on the journey from establishing the case for recruitment, through how recruited in a congested in-demand discipline, it will examines how we absorbing new recruits into a previously small team, finally it will look at how we are generating regulatory expertise, and managing the impact of increased capacity on the duty holder community.

Aim

The aim of this commentary is to provide other organisations seeking to enhance their capability with some considerations and lessons learnt.

State

United Kingdom

Gender

Male

Primary author: PARKHOUSE, Thomas

Presenter: PARKHOUSE, Thomas

Track Classification: CC: Information and computer security considerations for nuclear security