

Reconceptualising Nuclear Security as a Business Enabler: Opportunities and Challenges

Monday 10 February 2020 16:30 (15 minutes)

Synopsis

This paper will outline the potential benefits of taking a business-orientated approach to nuclear security and the opportunities and challenges that may offer. It draws on experiences of UK industry and activities conducted under the UK Government's Global Nuclear Security Programme (GNSP) (formerly Global Threat Reduction Programme, GTRP), which has been designing and delivering international nuclear security education, training and support for more than 20 years. This work forms the basis of the Nuclear Security Culture Programme (NSCP), an industry-academic consortium dedicated to supporting operators, regulators, academics and government agencies around the world. Led by King's College London since 2014, the NSCP is increasingly recognising the application of concepts from the field of business administration and strategic management to nuclear security. Reflecting this new approach, the NSCP's workshops and other activities now often include business-orientated topics such as risk management, leadership and business assurance.

The recent Nuclear Security Summit process led to an unprecedented level of attention directed towards nuclear security and helped to consolidate an international consensus at the governmental level on the need to mitigate the risk of nuclear terrorism. However, since the summit process ended the political momentum driving reforms and innovations has slowed. Government commitment and leadership remain vital to maintain the international nuclear security framework, but it is increasingly evident that this also requires the active participation of industry actors and the private sector.

Nuclear and radiological source licensees around the world are demonstrating ever greater responsibility and commitment to securing nuclear and radioactive materials and sensitive information. This is a commendable achievement, and a development that is reframing the normative context for nuclear security practices and behaviours. However, there remains a major obstacle to further progress: namely, nuclear security still tends to be regarded as an economic burden for operators. Rather than nuclear security being viewed as an enabler in disseminating the peaceful uses of nuclear technology, this aspect of the nuclear enterprise is too often considered as a drain on the bottom line. This presents challenges for nuclear security personnel trying to negotiate security budgets with the management level or governing board within nuclear organisations. The relatively low level of recorded security incidents exacerbate such complacency, despite it being widely accepted that calculations on risk must also factor in likely consequences of a given scenario; in the case of a nuclear terrorism event, these would be catastrophic.

Drawing on interviews with nuclear security managers and other personnel, the paper will explore implementation challenges faced by stakeholders charged with responsibility for nuclear security. In so doing, it will propose new ways of conceptualising nuclear security as a business enabler. The paper will detail the approach of the NSCP to its international workshops and other activities, with a focus on how business and strategic management concepts can be articulated to reframe nuclear security as a core business function providing value. The development of these workshops is not a simple endeavour in view of the difference in civil nuclear programmes, the range of licensees and the diverse national contexts and regulatory systems*. Nevertheless, the NSCP has observed that a business-orientated approach has worldwide relevance. Indeed, the evolution in funding mechanisms for new nuclear power plants is likely to bring core business functions and their associated costs under greater scrutiny as part of the commissioning and construction process. Likewise, shareholders are increasingly concerned by broader issues such as reputational damage and corporate social responsibility.

In particular, the paper will focus on the topic of risk management which now features across the NSCP workshops and other training and educational activities. A risk management approach emphasises how risk identification, risk assessment, risk reduction planning and risk audits are key business assurance processes. These processes are designed to ensure that security arrangements are proportionate, appropriate and affordable. Nuclear operators are encouraged to create links between the component parts of the risk framework, namely: critical asset and vital area identification; threat assessment and risk appetite; and risk reduction treatment. In so doing, business value is placed on the reduction of security risks. There is also an emphasis on leadership, management and governance within this context, enabling risk management to be positively enforced across the organisation. The paper will present an innovative and interdisciplinary approach to the area of nuclear security, providing new insights on what might be termed a 'virtuous circle'*** in aligning security best practice with business value.

*Participants at NSCP workshops include stakeholders from nuclear power plants, the regulator, government bodies and research, as well as those working with radiological sources at universities, healthcare, oil and gas companies, and other industries.

**For more on this concept, see Laura S. H. Holgate, 'Virtuous Circles: Linking Business and Nuclear Security', paper presented at the High-Level Panel on Nuclear Security, Norwegian Nobel Institute (8-10 June 2017).

Gender

Female

State

United Kingdom

Authors: HOBBS, Christopher (King's College London); TZINIERIS, Sarah (King's College London, UK); SALISBURY, Daniel (CNS)

Presenter: HOBBS, Christopher (King's College London)

Session Classification: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification: CC: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data