Nuclear Security Culture: From Theory to Practice. Christopher Hobbs (King's College London) Karl Dewey (King's College London) George Foster (Amport Risk)

Abstract

Considerable attention has been devoted to the human dimension of nuclear security in recent years. Efforts in this area are typically framed in terms of security culture, a term intended to capture the nature of shared responsibility for nuclear security. However, there have been only very limited studies into the challenges faced in establishing effective nuclear security culture programmes in industry and how these can be overcome. This paper seeks to help fill this gap by providing new practical insights into how the human factor within security systems can be strengthened. It does this through an examination of security culture initiatives that have been launched by the global nuclear industry over the last ten years, with a particular focus on the United Kingdom. In contrast to other studies that have tended to focus on cases of 'worst practice' this paper seeks to provide insights into how successful nuclear security culture programmes can be developed, through overcoming different internal and external barriers. In doing so it identifies a number of common challenges, as well as essential elements that underpin successful programmes. These include high-level organisational buy-in and engagement, exploiting the overlap between safety culture and security culture, targeted awareness programmes, training to different occupational groups and regular benchmarking.

Introduction

The last decade has seen an upsurge in international efforts aimed at promoting the importance of the human factor within nuclear security systems, with nuclear security culture featuring in at the 2010 to 2016 Nuclear Security Summits, within the summit communiques, workplans and the commitments made by the states in attendance.[1] Nuclear security culture has also been further codified in guidance published by the International Atomic Energy Agency (IAEA), both in relation to how it may be self-assessed and strengthened.[2] Crucially this increased international focus has also translated down to the operational level, with nuclear regulators and operators around the world launching new nuclear security culture initiatives.

This paper seeks to explore these efforts with a focus on the operational level, in an attempt to yield new practical insights into the establishment of nuclear security culture programmes. Here, focus is placed on the United Kingdom and initiatives launched within the nuclear industry over the past decade. In support of this work interviews were conducted with practitioners from four distinct UK-based nuclear organisations over a period of 15 months.[3] This data has been utilized in the analysis below, which attempts to illuminate some of the common challenges encountered when seeking to develop nuclear security culture and different ways in which these may be overcome.

UK national initiatives for strengthening nuclear security culture

For over a decade the UK has launched new national-level initiatives aim at strengthening security culture. This includes the launch in 2007 of the Centre for the Protection of National Infrastructure (CNPI), which functions as the national technical authority for physical and personnel protective security.[4] In 2016 a National Cyber Security Centre (NCSC) was also established to provide advice and support for the public and private sectors in countering computer security threats.[5] Both of these organisations publish information and resources aimed at helping businesses and their staff understand and counter physical and cyber related

threats. These can be readily integrated into organisational security awareness and training programmes, with the interviews conducted as part of this study demonstrating that these are widely utilised within the UK nuclear industry. In addition, CNPI have developed a survey-based security culture assessment tool (SeCuRE 4), which is regularly used within the UK nuclear industry to provide insights into the different aspects of security culture and the effectiveness of programmes launched in this area.[6]

Another key national-level contributor to the development of nuclear security culture, identified in this study was the UK's transition from a prescriptive to goal-setting approach to nuclear security regulation. This was initiated in the late 2000s and cemented in 2017 with the publication of Security Assessment Principles (SyAPs) for the civil nuclear industry.[7] This revised approach to nuclear security regulation places greater onus on licensees to evaluate their security risks and devise appropriate security solutions, rather than working towards prescribed standards. Interviews revealed that this has helped in transferring ownership of security from the regulator to operators, leading to the allocation of additional resources and increased focused on security, with corresponding improvements in culture. For example, the security manager of one of the organisations studied noted how the regulatory transition was used as a trigger for engaging the senior leadership on security, helping gain high-level buy-in and support, whilst also providing an opportunity to conduct a comprehensive review and revision of security processes and procedures, in collaboration with other departments. [8]

Practical lessons in the development of nuclear security culture programmes

Ensuring Leadership Support

One major impediment to implementing an effective nuclear security culture remains the common perception that security is an unnecessary and expensive cost. However, our research shows that engaging with an organisation's leadership and ensuring their active support — particularly at the senior and executive levels—is key to driving change, including organisational attitudes to nuclear security.[9] Yet an organisation's leadership must still balance many competing priorities, even if an organisation believes that credible threats exist and that nuclear security is important.Without this Executive support efforts to strengthen security culture are likely to be limited at best and fail at worst.

Rather than a cost, security may be best viewed as a 'business enabler' without which other business operations would be unable to sustainably take place.[10] In doing so, there is an opportunity to frame security issues in a manner consistent with IAEA guidance,[11] but also in 'the same language' as other Board business. By changing the framing of security issues to a business enabler, the topic may be more easily placed within an overall profile of Enterprise Risk Management (ERM), where overarching business risks are considered. Here, security cuts across numerous areas of Enterprise Risk, including Compliance; Financial; Operational; Reputational; and Strategic risks. By placing security issues in an ERM framework, Board members are better sensitised to "the costs of getting it wrong," in each of the business areas and the need to mitigate particular business risks. To illustrate this, Table 1 includes some of the potential negative impact licensees may face following a nuclear security incident, across the broad range of business areas.

	Shorter term	Medium term	Longer term
Financial / Market and Sector	Response Operational slowdown/shutdown	Potential clean-up Operational slowdown/shutdown Impact on share prices	

		Costs of meeting new standards / regulatory requirements	
	Share price impact	Reduced longer term opportunity, loss of investor confidence	
Legal/Regulatory	Regulatory fine Operational slowdown/shutdown	Operational slowdown/shutdown Loss of facility license	Legal proceedings against operator
Reputational / social	Negative media coverage		Loss of trust Loss of initial contract and other business opportunities

Table 1: Outlining the Potential Costs of a Security Incident
Source: Dewey, Hobbs, Foster & Tzinieris (2020). Reconceptualising Nuclear Security as a Business Enabler: Opportunities and Challenges, in IAEA International Conference on Nuclear Security (ICONS 2020), 10 February.

The framing of poor security as a business risk encourages the 'ownership' of that risk and representation on the Board as part of a director's portfolio. However, because security issues cut across all areas of an organisation, the creation and inclusion of security-related metrics into corporate milestones and renumeration packages for all Board members helps to ensure alignment across different business areas, as well as continued and common focus.

In turn, this Executive 'buy-in' helps ensure that, consistent with IAEA guidance, security risks are clearly articulated across an organisation through security policy statements, and that risks are mitigated through appropriate management structures and resources.[12] Adding security metrics into corporate milestones also helps incorporate them into an organisation's wider business-cycle, thus facilitating a programme of review and improvement. Such metrics also provide auditable demonstrations of an organisation's commitment to security, which can be demonstrated to national regulators.

Although Executives may use their authority to drive change, at the practical level changes are overseen by the senior leadership team and other managers. Indeed, managers are also highly influential to an organisation's security culture and "With sustained effort, and by employing the incentives and disincentives at their disposal," managers are encouraged to "establish [positive] patterns of behaviour and even alter the physical environment".[13] Therefore, enlisting management support is critical to fostering an effective nuclear security culture. This is by no-means automatic and Executives must work with managers to ensure that security risk management aligns with business objectives .

<u>Awareness raising and training</u>

Similar to tailoring communication styles at the Executive level, at the manager and staff level raising awareness and training messages are particularly effective where they complement existing work patterns and competencies. Here, the overlap between safety culture and security culture provides an excellent opportunity to begin discussions. However, one organisation may have a multitude of environments and care is needed to ensure training and messaging is relevant to specific work environments. For example, the potential security risks faced by an office environment will differ significantly from those at an operational setting. Indeed, interviews showed that training is much more likely to be retained, if people can understand the relevance to their roles and what should be done, rather than it being explained as high-level principles or in abstract terms.[14]

Organisations may conduct various training programmes, although for many staff security awareness begins as they join a nuclear-organisation and undergo security vetting and induction. The vetting process acts as a significant catalyst for security awareness. However, periodic training—beginning with induction training—allows for employees to become familiar with an organisation's values and expectations. Such values and expectations may manifest through an organisation's "Challenge Culture," where employees (regardless of position) are expected to openly question the behaviours of their fellow employees; or an "arms around" culture where staff are encouraged to get to know their colleagues and work with management should they suspect their colleagues are experiencing difficulties. Refresher courses reinforce these messages and provide an opportunity to update staff with new procedures. These efforts cannot take place in isolation, and enlisting the support of teams such as Human Resources (HR) and Occupational Health (OH) adds reinforcement of security expectations within the overall working culture.

To prevent complacency and maintain motivation, training agendas should be rotated and materials regularly refreshed. Using case studies helps to illustrate relevance while changing formats, for example complementing lectures with table-top exercises or guest speakers, helps complement the diversity of learning styles. The importance of training should also be underpinned by other organisation processes, for example, linking repeated failure to follow training with the potential for HR sanctions.

Enabling effective security related communications

Clear and tailored communications can also reinforce awareness raising and training, with poster campaigns, emails, and branded merchandise all serving to remind staff of the importance of security measures. Communications are also vital to celebrate and reinforce successes. Highlighting positive staff contributions to security campaigns—for example, cleaning staff who notice unusual activity—gives validation to their actions, while also encouraging others. The UK government seeks to support such communications and the Centre for the Protection National Infrastructure (CPNI) offers free resources that can be adapted for use.[15] However, security managers noted that some methods were more successful than others. The importance of clear, concise, and jargon-free language was emphasised, as was understanding staff working patterns and how messages are consumed. For example, lengthy newsletters tend to be only read superficially, although tweets and short email campaigns are more consumable and provide greater flexibility.

In addition to reinforcing training, part of enabling effective security-related communications includes the perception of the security team itself. One benefit seen from greater departmental collaboration was greater awareness of security processes across an organisation. In turn, security teams were also able to begin repositioning themselves from compartmentalised departments that 'say no', to business enablers that support other business lines to operate securely and sustainably.[16] As part of this change, several security teams in the UK's nuclear estate noted the change in their own departmental mindsets—for example by adopting a 'need to share,' rather than a 'need to know' mentality. This approach seeks to balance legitimate security and confidentiality concerns, but rein back excess security measures to realise the benefits of greater transparency. A common theme of this wider shift was working with communication departments to help recast the image of security teams as a business impediment, to an image where security teams are 'there to help'. This now forms a part of many organisations' communications strategy, although the emphasis is on the need to engage

early with the security team. Doing so allows for security to be 'built in' from the initial stages, rather than having to be 'built on'—which adds time and expense.[17]

Clear inter-departmental communications and collaboration with other relevant departments can also have a positive impact on nuclear security culture. Greater collaboration between security with other teams such as HR and Occupational Health, allows for a common approach when considering individual staff members, as well as helping to identify potential warning signs early so that support may be put in place, referred to as the 'Golden Triangle' by one interviewee.[18] This is especially important when reporting security issues (discussed below).

Security testing and reporting

There are numerous ways in which organisations may seek to test their security culture — for example, random inspections to measure clear desks policy; 'turnstile days' where staff are surveyed during a morning arrival and reminded of specific reporting obligations; or company-run phishing campaigns to measure employee susceptibility to real phishing emails.[19]

However, utilising testing to raise awareness of security is only half of the story and to be effective it must translate into actions. An organisation's staff form the first line of defence because they are best placed to notice broken equipment and poor security behaviours. As such, staff should also be encouraged to report their concerns. These are in addition to annual appraisals with line-managers, and periodic security reviews. Due to potential sensitivities, a confidential system is paramount, but so too is engagement with other relevant stakeholders. As noted, a close working relationship between security, HR, and Occupational Health may provide an holistic means to address problematic behaviour. Organisations such as HR also play an important role in fostering an overall working environment which is receptive to open or confidential reporting. This can be done by developing a culture of "no reciprocity", wherein potential issues reported in good faith remain confidential and the reporting of poor security behaviours in others will not result in any detrimental consequences if their observations are unfounded. Such messaging can complement an organisation's challenge culture and encourage staff to be open and honest about their potential concerns.

Conclusions

There are many interrelated ways in which nuclear organisations can look to improve their security culture, including awareness raising, training, testing and reporting, the impact of which can be greatly enhanced by the active support of the Executive and senior management. In their implementation focus should also be placed on the varying and tailoring of efforts, with materials regularly refreshed and consideration given to how different occupational groups can best be targeted. To develop a robust security culture, programmes must be sustained for many years and overcome a multitude of challenges that are likely to be encountered along the way. For example, changing 'traditional' mindsets more inclined to the compartmentalising, as opposed to sharing, of non-sensitive security-relevant information. In support of these efforts there now exists an array of international guidance, although careful consideration must be given as to how these can be effectively translated into different national and organisational contexts.

Acknowledgements

This work was funded under the UK's Nuclear Security Culture Programme, managed by the UK Department of Business Energy and Industrial Strategy (BEIS).

[1] "Key Facts About the Nuclear Security Summits", The White House, Office of the Press Secretary https://obamawhitehouse.archives.gov/the-press-office/key-facts-about-nuclear-security-summit (13th April 2010).
[2] "Self-assessment of Nuclear Security Culture in Facilities and Activities", Nuclear Security Series No. 28-T (Vienna, 2017); "Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material", Nuclear Security Series No. 38-T (Vienna, 2021)
[3] The organisations that took part in this study were EDF Energy, Radioactive Waste Management (RWM), International Nuclear Services (INS) and Direct Rail Services (DRS). In February 2021, INS and DRS were merged into a new business, Nuclear Transport Solutions (NTS). Detailed nuclear security culture case studies for each organisation can be found within 'Karl Dewey, George Foster, Christopher Hobbs and Daniel Salisbury', Nuclear Security Culture in Practice: A Handbook of UK Case Studies', CSSS Occasional Paper (2021) https://www.kcl.ac.uk/csss/assets/nuclear-security-culture-in-practice-2021.pdf
[4] Centre for the Protection of National Infrastructure (CPNI), https://www.cpni.gov.uk/ (website accessed August 1 2021).
[5] National Cyber Security Centre, https://www.ncsc.gov.uk/ (website accessed August 1, 2021).
[6] SeCuRE 4: Assessing Security Culture, Centre for the Protection of National Infrastructure (CPNI) https://www.cpni.gov.uk/secure-4-assessing-security-culture (website accessed, August 1, 2021)
[7] "Security Assessment Principles (SyAPs) for the Civil Nuclear Industry", Office for Nuclear Regulation, https://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf (2017)
[8] Dewey et al., *Nuclear Security Culture in Practice: A Handbook of UK Case Studies, p. 16*.
[9]Karl Dewey et al., *Nuclear Security Culture in Practice: A Handbook of UK Case Studies*, King's College London (London, 2021)..
[10] Karl Dewey et al., "Reconceptualising Nuclear Security as a Business Enabler: Opportunities and Challenges" (paper presented at the IAEA International Conference on Nuclear Security (ICONS 2020), Vienna, 2020).
[11] *Nuclear Security Culture: Nuclear Security Series No. 7*, IAEA (Vienna, 2008).
[12] *Nuclear Security Culture: Nuclear Security Series No. 7*.
[13] *Nuclear Security Culture: Nuclear Security Series No. 7*, 12.
[14] Dewey et al., *Nuclear Security Culture in Practice: A Handbook of UK Case Studies*.
[15] "Security Campaigns," in *Centre for the Protection of National Infrastructure* (August 3 2021). https://www.cpni.gov.uk/security-campaigns.
[16] Dewey et al., *Nuclear Security Culture in Practice: A Handbook of UK Case Studies*.
[17] See RWM case study in Dewey et al., *Nuclear Security Culture in Practice: A Handbook of UK Case Studies*.
[18] See EDF case study in Dewey et al., *Nuclear Security Culture in Practice: A Handbook of UK Case Studies*.
[19] Dewey et al., *Nuclear Security Culture in Practice: A Handbook of UK Case Studies*.