RECONCEPTUALISING NUCLEAR SECURITY AS A BUSINESS ENABLER: Opportunities and Challenges

K. DEWEY
King's College London
London, United Kingdom
Email: karl.f.dewey@kcl.ac.uk

C. HOBBS
King's College London
London, United Kingdom
Email: christopher.hobbs@kcl.ac.uk

G. FOSTER
Amport Risk Limited
Andover, United Kingdom

D. B. SALISBURY
King's College London
London, United Kingdom

S. TZINIERIS
King's College London
London, United Kingdom

Abstract

This paper explores the importance of reframing nuclear security as a business enabler, before discussing how this might be achieved, with a particular focus on its promotion at the corporate level. It draws lessons from the authors' experiences working within UK industry and internationally through the UK's Nuclear Security Culture Programme (NSCP).[1] It is argued that the negative impact of a nuclear security incident will likely far outweigh the costs of implementing proportional and robust security measures. However, despite this seemingly clear financial driver, nuclear security is arguably still viewed by many within industry as rules and regulations to be followed, and often as a burden, rather than as a key organisational goal. The barriers to changing beliefs and attitudes on the fundamental importance of security will be discussed, as well as strategies that can lead to increased engagement in this area, particularly with respect to senior management. Finally, suggestions for incorporating these lessons into international nuclear security engagement programmes are outlined.

1. INTRODUCTION

The Nuclear Security Summit (NSS) process led to an unprecedented level of political attention directed towards nuclear security, helping to build a broad international consensus on the need to tackle the risks of nuclear terrorism and other unauthorised acts involving nuclear and radioactive materials. Since the summit process ended in 2016, however, high-level political momentum driving reforms and initiatives has slowed. Government commitment and leadership remain vital to sustain the international nuclear security architecture, but it is nonetheless increasingly evident that this also requires the active participation of other stakeholders, especially licensees. Here there has been progress with many industry actors taking steps to strengthen systems that secure nuclear and radioactive facilities and assets.

Nevertheless, nuclear security in generally is still arguably regarded within industry as an operational burden, rather than a core business enabler. This viewpoint presents a major obstacle to further progress, particularly given waning political momentum, post-NSS. Rather than nuclear security being recognised as fundamental to the

[1] Consortium partners, 2014-2018: King's College London, Imperial College, University of Central Lancashire and National Nuclear Laboratory; 2018+: King's College London, International Nuclear Services (INS) and Amport Risk Ltd.

peaceful use of nuclear technology, this aspect of the nuclear enterprise is too often considered first and foremost as a drain on the bottom line [1]. As a result, personnel directly responsible for nuclear security face perennial challenges in, for example, negotiating adequate security budgets with management, launching new security initiatives and increasing the involvement of non-security personnel. These challenges are further exacerbated by a relatively low level of publicised security incidents, and a lack of information sharing on near misses, which can contribute to a sense of complacency and resulting organisational inertia, mitigating efforts to strengthen security. This is despite the potentially highly significant and wide ranging consequences of a nuclear security incident, which in the case of a sabotage attack, may include not just disruption and lost revenue but also broader reputational and operating costs.

Given the multitude of competing priorities faced by nuclear stakeholders, security can seem an expensive requirement and less urgent than other key concerns such as nuclear safety. However, efforts to improve nuclear security, need not necessarily be expensive. In particular there is much that can be done at relatively little cost when it comes to strengthening the human factor within nuclear security systems. This is a critical element of nuclear security as illustrated by recent incidents, which have demonstrated how even technologically advanced security systems can and will break down if they are not appropriately designed, maintained, operated and tested [2]. The importance of the human dimension to nuclear security has been recognised and promoted through the NSS process, with the International Atomic Energy Agency (IAEA) developing guidance for assessing and strengthening nuclear security culture. In this context the importance of nuclear security leadership cannot be underestimated. Indeed, it is a key component of the organisational culture framework developed by the IAEA [3]. However, despite the existence of high-level guidance, few studies have examined how organisations have sought to develop an effective nuclear security culture, underpinned by strong leadership buy-in and engagement.

This article discusses why nuclear security should be seen as a business enabler, before considering different strategies for promoting this message within industry. It draws insights from activities conducted under the UK's international Nuclear Security Culture Programme (NSCP), as well as from the experience of nuclear organisations in the UK. It begins by exploring some of the different factors that drive nuclear security within industry, noting a disconnect with how discussions are typically framed at the international governmental level. The costs of nuclear security are then considered, relatively to the impact of potential incidents, drawing on recent cases. A range of different strategies targeted at achieving buy-in from senior management and developing an effective nuclear security culture are then outlined. Finally, the implications for programmes that seek to engage industry on these topics are discussed.

2. NUCLEAR SECURITY DRIVERS – PERSPECTIVES WITHIN INDUSTRY

The NSS process helped sensitise key states to the threat posed by nuclear terrorism and hence the importance of nuclear security. However, there exists a far wider range of drivers and broader organisational factors that influence nuclear security practice. Here it is also important to note that the relative strength of these may differ considerably from one organisation to another. This is in part due to responsibility for nuclear security being devolved to the state level, where national threat perceptions and risk appetites vary. Although even within an individual country, there may be significant variation when it comes to the size of nuclear facilities, range and type of activities conducted, and ownership-operator models, all of which can influence how nuclear security is implemented. Consequently, when considering strategies for strengthening nuclear security at the operational level, it is important to recognise that there is no 'one size fits all' approach. As such not all the suggestions outlined in this paper will apply equally to every organisation. Instead these should be considered as part of a tailored approach to security, that both satisfies operational standards and national regulations. Given the central role of individual licensees in providing effective nuclear security, it is important to interrogate what fundamentally drives operators in their development of nuclear security programmes. Key factors shaping behaviour explored in this paper are: commercial interests; legal and regulatory requirements; and, broader ethical and societal considerations.

Commercial interests: Many nuclear organisations operate in a commercial environment and consequently are fundamentally driven by the need to make their activities profitable, while even wholly government-owned organisations, will be incentivised to provide 'value for money' [4]. In this context nuclear security can be viewed as a means of protecting against the potential costs that would be incurred by, for example: a shut-down or

disruption to operations; the theft of valuable materials, technology or intellectual property; and the loss of current or possible future contracts due to broader reputational damage.

Past incidences have shown that the financial costs of disruption can be very high, for example, in February 2017, a fire in the turbine hall at the Flamanville nuclear power plant forced a shut down, costing between an estimated $1.2-2.2 million a day [5]. Although the shutdown at Flamanville was safety related, commercial power plants have also experienced disruption due to security incidents, as seen in the 2014 sabotage at Doel-4 that saw lubricant oil deliberately drained from a turbine resulting in repair costs of €30 million [6]. With Doel-4 out of action the operator lost around €40 million a month – a total of around €160 million [7]. Delays and accidents may also impact share prices. For example, the share price of TEPCO, the operator of the Fukushima Daichi plant dropped by around 90% in the weeks after the 2011 disaster – a safety incident but something that could arguably be caused by a malicious actor – and has barely recovered to greater than a quarter of its pre-incident value in the eight years since [8]. Smaller nuclear operators are also susceptible to significant costs from a delay of operations. For example, in 2018 a safety-related two-week shutdown at the Australian Nuclear Science and Technology Organisation (ANSTO), a major radioisotope producer, cost "ANSTO a significant proportion of its revenue due to the need for the importation of generators from abroad [in order] to ensure supply to Australian hospitals" [9].

Nuclear security weaknesses can also have longer-term cost implications. For example, the security breach at Y-12 National Security Complex in 2012, led to an inquiry, the results of which were published by the US Department of Energy as a special report, this was followed by a congressional hearing, with the incident also widely covered by the US and international press [10]. This resulted in a naming and shaming of the key actors involved, with the security company at Y-12 losing its contract shortly after the incident, and other contracts in the months that followed [11]. Reputational damage resulting from a nuclear security incident also has the potential to significantly affect the viability of the industry as a whole. Particularly in countries where approval for nuclear energy programmes is not universal, and where public awareness and pressure has been increased by prior safety or security incidents. When it comes to information security, past examples across a range of sectors have demonstrated how poor practices can result in substantial lost revenue. For example, in 2011 the US International Trade Commission, estimated that intellectual property theft and industrial espionage costs US industry $10s billions a year. [12]. However, so far there have been few detailed studies that have attempted to investigate how the theft of sensitive nuclear information might equate to lost revenue within the nuclear sector. Traditionally, these risks have been examined in terms of their proliferation impact, with studies focusing on how the diffusion of sensitive nuclear knowledge can further states' nuclear weapons ambitions.

Legal and regulatory requirements: The behaviour of nuclear organisations is also shaped by the legal and regulatory landscape in which they operate. Here States, via appropriate national legislation and the empowerment of competent authorities, can impose minimum security standards upon licensees through licencing, operating requirements and regulatory direction. Where licensees fall short, fines and other punitive measures may be employed in an effort to compel them to strengthen security. The threat of these costs – and fear of incurring them – can deter non-compliance and essentially drive licensees to put in place adequate security measures. However, for deterrence to function, organisations must believe that noncompliance will be uncovered and punished, while penalties must be clearly communicated and significant enough to warrant action. These drivers are undermined if national legislation and regulation is poorly drafted to this end and where regulators are poorly funded or lack the skills and capacity to fulfil their roles. In countries with well-developed legal and regulatory frameworks, the costs of non-compliance can be high, with many regulators having the power to close facilities if they do not meet the security requirements. They also can impose significant fines for serious safety and security breaches – in some cases in excess of hundreds of thousands of dollars [13]. For example, in the 2000s the US Nuclear Regulatory Commission imposed fines on operators of $65,000 and $135,000 after security guards were found to be sleeping at nuclear plants, and $208,000 after guards handled weapons in an unsafe manner [14].

The form of regulation can also influence licensee behaviour with respect to nuclear security. For example, the UK has seen a shift from traditional prescriptive-based to outcome-focused regulation. As outlined in the UK's Office of Nuclear Regulation's (ONR) 2017 Security Assessment Principles (SyAPs), the expectation is that licensees decide for themselves on what constitutes proportionate, appropriate and affordable security measures, and then justify them to the ONR [15]. The regulator retains the power to compel licensees to improve their security, although the onus is now on licensees to evaluate the security conditions of their facilities [16]. Although detailed studies have yet to be undertaken, initial research conducted by the authors, has hinted at the possible benefits of this approach. Placing the onus on the licensee to come up with solutions, has the potential to improve

organisational learning and communication with respect to security, including the active involvement of a broad range of occupational groups, including senior management as well as staff in scientific and technical roles [17].

The broad range of potential costs that might be incurred by a licensee following a nuclear security incident are summarised in Table 1, which also illustrates how these may change over time.

Table 1: Outlining the Potential Costs of a Security Incident

	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	
Legal/Regulatory	Regulatory fine Enforced operational slowdown/shutdown	Enforced operational slowdown/shutdown Loss of facility license	Legal proceedings against operator
Reputational	Negative media coverage		Loss of trust Loss of contract and future business opportunities

Ethical and broader societal considerations: The aforementioned discussion may seem to imply that a nuclear organisation's approach to security is shaped purely by financial drivers, however, licensees do not operate in a social vacuum. Those working for and leading nuclear organisations can be influenced by an intention to "do the right thing", particularly given the potentially severe societal and environmental impact of a serious nuclear security incident. Moreover, licensees are also being cognisant of the need to build public trust and confidence as a prerequisite for the continued acceptance and longer-term viability of their business. In this context, nuclear security should be perceived across the nuclear enterprise as creating business value, by minimising risk and creating the conditions necessary to sustain an organisation in its specific national, regional or global context.

In the same way that 'soft' issues such as human rights, climate change and local job creation have come to feature in strategic planning – as part of an organisation's commitment to corporate social responsibility (CSR) – nuclear security should be regarded as a prerequisite to doing business ethically and responsibly. Particularly given the increase in construction of new nuclear reactors and associated facilities in 'newcomer' countries, with funding sources shifting from government-led arrangements to greater investment from global capital markets and other new types of financial arrangements [18]. In turn, this is placing core business functions under greater scrutiny as part of the commissioning and construction process. CSR and other ethical aspects of doing business represent an area that investors are taking increasingly seriously, mainly due to the risk of reputational damage but also because of growing client demand for ethical investment vehicles [19].

A number of nuclear regulators and licensees have developed CSR programmes and publish regular reports on their progress. There have also been efforts to develop a shared set of standards in this area, for example, the Nuclear Power Plant and Reactor Exporters' Principles of Conduct (NuPoC) [20]. However, as highlighted in a study by the World Institute for Nuclear Security (WINS), security does not always feature prominently in these initiatives, relative to, for example, safety [21]. The development of CSR programmes is also uneven, with 'some countries place[ing] a much higher priority on public and stakeholder engagement than other[s]' [21].

3. COSTS OF NUCLEAR SECURITY

Given that nuclear security can be viewed as a financial burden, it is important to explore how this breaks down in order to identify where potential savings or low cost-improvements can be made. Some of the major costs of developing and maintaining security for a nuclear facility are outlined in Table 2.

Table 2: Breaking Down the Costs of Nuclear Security

Type of Cost	Specific Cost	Explanation / Examples
Human	Security function at the corporate and management levels	Representation at Board/Executive Committee level, Head of security, security administrative and supporting functions, such as procurement, project management and maintenance.
	The Armed Response Force (if recharged to the Licensee)	Daily costs magnified by multiple rank and operational shift layers, equaling high headcount numbers.
	Unarmed Guard force	Training, Security licensing, staffing Security Control Centres, manning access points, providing security patrolling etc.
	Contractors	Advising, project managing, installing and maintaining security systems.
	Consultancy	Consulting on systems, equipment and the threat.
	Training	To establish Suitably Qualified and Experienced executive, security and supporting staffs. To maintain suitable levels of awareness across all staff.
	Personnel security	The application of vetting processes, personal security culture, administration of processes and liaison with government and external bodies.
	Inspection, testing and quality assurance	Internal and external audit.
	Engagement with government	Maintaining compliance with security regulations.
	Regulator	For regulatory intervention where costs of the regulator are attributed to the Licensee
Hardware and software	Physical protection systems	Gates, fences, cameras, hostile vehicle mitigation etc.
	Armed Response Force (if recharged to the Licensee)	Vehicles, training facilities, weapons, uniforms, personal protective equipment, etc.
	Guard force equipment	
	Network and workstation preventive and protective measures	Cyber protection software and systems, in-house and external response capabilities. Integration with PPS and Information Technology and Operational Technology

The relative cost of these will clearly vary considerably based on the size and type of facility. Annual costs for security at large nuclear sites can easily run into the tens or hundreds of millions of dollars a year. For example, the annual security budget at Y-12 in 2012 was $150 million [10]. However, as illustrated by the Y-12 break-in the magnitude of nuclear security spending does not necessarily equate to system effectiveness. The weaknesses identified in this and many other nuclear incidents stemmed from issues with how security was implemented at the facilities [2]. In these cases, perpetrators actions were effective due to weaknesses that included: the ineffective design and maintenance of security systems; staff not following security procedures; and a failure to identify and report suspicious activity in advance of an incident. As will be briefly discussed in the next section the costs of developing an effective security culture where staff comply with security procedures, are vigilant to potential threats and report security concerns are relatively low in comparison with some of the hardware costs outlined in the above table.

4. STRATEGIES FOR PROMOTING NUCLEAR SECURITY AS A BUSINESS ENABLER

There are, of course, many possible mechanisms for strengthening nuclear security and engendering buy-in from senior staff. Outlined below are just some possible and low-cost approaches, drawn from recent efforts to promoting nuclear security within UK industry.

Ensuring top-level engagement and advocacy: As has been briefly discussed in this paper and highlighted in detail elsewhere an organisation's leadership and management have a critical role in driving effective nuclear security, as "through their behaviour, managers demonstrate their commitment to nuclear security and, in so doing, play an important role in promoting nuclear security culture within the organization" [3]. According to the IAEA "the management of relevant organizations must appoint an individual responsible for nuclear security who has

sufficient authority, autonomy and resources to implement and oversee nuclear security activities. This individual is required to report to the top manager or to an appropriate senior manager of the organization with the responsibility defined and documented in sufficient detail to prevent ambiguity" [3]. Ideally, detailed security related discussions should occur at the highest decision making of an organisation. To this end organisations should consider appointing appropriately equipped personnel at the executive and board level. Such an individual does not need to necessarily be responsible solely for security, but maintaining the focus at the highest levels of a licensee's management will help ensure that security issues are prioritised throughout an organisation. Engagement with security issues at a high-level can be further enhanced by writing security metrics into board-level performance objectives and targets. In addition to individual targets and bonuses, linking security performance to (portions of) the bonuses of other directors will help ensure a vested interest in, and collective focus on security. Such metrics should be positive (i.e. active measures) taken by the board, as well as negative (i.e. an absence of security indicators). These should also be defined and assessed by an independent body such as a regulator, international sponsor, or non-executive directors, who would work with the licensee to ensure a tailored approach, taking into account current resourcing and organisation levels. In addition to positive inducements, increasing corporate accountability – for example by making directors personally accountable for security decisions – will also help focus activity. Though far-reaching, such accountability has precedent in legislation such as the US Sarbanes-Oxley Act (SOX) of 2002 where Chief Executive Officers and Chief Financial Officers are personally responsible for their company's internal accounting controls [22].

Articulating and demonstrating the 'value of nuclear security': As discussed earlier there are strong commercial, legal and regulatory reasons why the organisations should invest in and develop strategies for promoting effective nuclear security. However, these are not necessarily articulated in their entirety to senior managers and board members of nuclear licensees. Consequently, greater efforts should be placed on outlining the full-range of potential costs that may follow from a serious nuclear incident. In order to strongly convey the message, real-life nuclear cases drawn from the around the world should be utilised as well as relevant incidents drawn from other sectors. However, nuclear security should not just be viewed as means of avoiding punitive action, there are positive benefits to developing effective programmes in this area, that should also be promoted. For example, the UK take a tiered approach to nuclear security regulation, under which licensees are able to reduce their level of regulatory focus by demonstrating over time that they have developed strong security systems and internal assurance programmes. This can serve to reduce the frequency and costs of regulatory inspections and provide a positive indicator for the board that nuclear security is being effectively implemented. A similar approach could also be considered with respect to nuclear insurance i.e. organisations that clearly demonstrate a high performance level with respect to security would pay a reduced premium. More broadly, CSR programmes incorporating nuclear security, should also be viewed as more than just 'being a good corporate citizen' but also as a means of 'driving innovation and promot[ing] learning', ultimately helping 'companies increase their value and business' [21]

Establishing and maintaining the profile of security: There are many possible and low-cost mechanisms for promoting understanding and direct engagement with security across a broad nuclear workforce. In UK the past decade has seen the launch for a number of new initiatives aimed at strengthening nuclear security culture. This includes guidance, tools, training and awareness programmes by government authorities and public bodies such as the Centre for the Protection of National Infrastructure (CPNI) and the Nuclear Decommissioning Authority (NDA) [23]. These can be readily utilised by organisations to enhance security procedures, internal training courses and assess the state of security culture within different occupational groups. They can also serve to facilitate the sharing of nuclear security relevant information across organisations. For example, the NDA, hosts a regular forum for security attended by subsidiaries and site license companies from its estate, at which information on incidents, near misses and evolving security practice is shared. Within individual organisations, there are a number of simple steps that can be taken to support wider staff engagement with security. For example, through the inclusion of a safety and security 'moment' at the start of all meetings, the inclusion of security appraisals within annual performance reviews, and mechanisms for sharing feedback and suggesting improvements to existing security procedures. For example, International Nuclear Services (INS), operate an internal programme known as 'safe-steps' where employees can readily provide anonymous written and electronic feedback on safety and security issues [17].

5. RECOMMENDATIONS FOR INTERNATIONAL COOPERATIVE NUCLEAR SECURITY PROGRAMMES

International cooperative efforts aimed at strengthening the security of nuclear materials, facilities and information date back decades [24]. Initially focused on physical upgrade and infrastructure work these efforts have evolved over time to include a greater focus on strengthening the human dimension of nuclear security in an effort to ensure the effectiveness and sustainability of security improvements. The UK through its NSCP has run more than 30 activities since its inception in 2014 to this end, for a mix of government officials, industry practitioners and academics. Some of the key lessons from activities conducted under this programme are summarised below:

- Engaging current and future nuclear security leaders, with the ability to enact changes at different levels within their respective organisations is key to ensuring the longer-term impact of activities.
- When engaging with industry it is important to explore the threat to nuclear assets in the broadest possible sense, as opposed to limiting discussions to the narrow counter-terrorism perspective that tends to frame debates at the highest political levels. Particularly, given that there exists widely divergent perceptions of the threat posed by nuclear terrorism.
- Nuclear security should be framed as a business enabler with potential benefits when it comes to reducing regulatory and other costs and driving innovation, rather than a drain on the bottom line.
- The fundamental and underpinning nature of nuclear security culture and leadership mean that it can and indeed should be embedded into any nuclear security activity, no matter its primary focus.
- The use of real-life examples and detailed table-top exercises are essential tools for bridging the gap between theory and translating IAEA guidance and nuclear security principles to the operational level.
- Drawing lessons from the UK's and other countries experience in implementing nuclear security can be extremely valuable, but time needs to be allocated so that their application can be considered in different national contexts.

6. SUMMARY

This paper has explored what drives the development and implementation of nuclear security programmes within industry, focusing on financial cost-benefit calculations, the influence of legal and regulatory frameworks and commitments to corporate social responsibility. It has also sought to highlight the importance of engaging senior leadership as part of efforts to develop an effective security culture, discussing a number of strategies that might be taken to that end. Here there are many low cost approaches that organisations could adopt which would significantly strengthen their nuclear security. Finally, drawing on this discussion lessons for how nuclear security should be articulated and promoted through international engagement programmes are outlined.

ACKNOWLEDGEMENTS

The authors are grateful to the UK's Department for Business, Energy and Industrial Strategy (BEIS) for supporting the NSCP workshops and activities discussed in this paper. The authors also appreciate the support provided by the partners and other subject matter experts involved in the programme, including Amport Risk and International Nuclear Services (INS).

REFERENCES

[1] HOLGATE, L., 'Virtuous Circles: Linking Business and Nuclear Security', Paper presented at the High-Level Panel on Nuclear Security, Norwegian Nobel Peace Institute (8-10 June 2017). https://www.nobelpeaceprize.org/content/download/718/11157

[2] Geoffrey Chapman, Robert Downes, Christopher Eldridge, Christopher Hobbs, Luca Lentini, Matthew Moran, Alberto Muti & Daniel Salisbury, 'Security Culture: An Educational Handbook of Nuclear and Non-Nuclear Case Studies', Insider Threats (August 2017) https://www.kcl.ac.uk/csss/assets/security-culture-handbook.pdf

[3] 'Nuclear Security Culture', IAEA Nuclear Security Series No. 7 (2008) https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

[4] 'NDA Value Framework: How we make decisions', Nuclear Decommissioning Authority (1st April 2016) https://www.gov.uk/government/organisations/nuclear-decommissioning-authority/about.

[5] ANON, 'Offline reactor costing EDF $1.2m per day' in Power Engineering International, 22 February 2017. [Online] Available at: https://www.powerengineeringint.com/2017/02/22/offline-reactor-costing-edf-1-2m-per-day/

[6] BOVE, L,. 'Sabotage kerncentrale Doel is vier jaar later nog altijd mysterie [Sabotage nuclear power plant Doel is still a mystery four years later]', *De Tijd*, (9 August 2018,). [online] Available at: https://translate.google.com/translate?hl=en&sl=nl&u=https://www.tijd.be/politiek-economie/belgie/algemeen/sabotage-kerncentrale-doel-is-vier-jaar-later-nog-altijd-mysterie/10038413.html&prev=search (accessed 6 December 2019 via Google Translate).

[7] DE CLERCQ, G., "UPDATE 2-Belgian Doel 4 nuclear reactor closed till year-end", Reuters, (14 August 2014), [online] Available at: https://uk.reuters.com/article/belgium-nuclear-doel-idUKL6N0QK43R20140814

[8] "Tokyo Electric Power Company Holdings, Incorporated (TKECY)", Yahoo Finance, https://finance.yahoo.com/quote/tkecy?ltr=1 (accessed 6 December 2019).

[9] 'INDEPENDENT SAFETY REVIEW OF THE ANSTO HEALTH APPROACH TO OCCUPATIONAL RADIATION SAFETY AND OPERATIONAL PROCEDURES (AS001-REP002)' - OCTOBER 2018. Available at: https://www.arpansa.gov.au/sites/default/files/independent_review_of_ansto_health.pdf?acsf_files_redirect

[10] US Department of Energy Office of Inspector General, "Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex", DOE/IG-0868, August 2012, p.1.

[11] GARDNER, T., "Nuclear site ends security contract following nun's break-in", Reuters, 29 September 2012, [online] Available at: https://www.reuters.com/article/us-usa-nuclear-gaf/nuclear-site-ends-security-contract-following-nuns-break-in-idUSBRE88S0F320120929; HUOTARI, J. "After 13 years guarding federal facilities, WSI leaves Oak Ridge", Oak Ridge Today, 25 March 2013, [Online]. Available at: https://oakridgetoday.com/2013/03/25/y-12-security-breach-wsi-leaves-oak-ridge/

[12] See for example PHAM, S., "How much has the US lost from China's IP theft?", CNN Business, (23 March 2018) [Online] Available at https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html

[13] Office for Nuclear Regulation, "Events reported to the Nuclear Safety Regulator in the period of 1 April 2001 to 31 March 2015", (4 February 2016), [Online] available at: http://news.onr.org.uk/2016/02/events-reported-to-nuclear-safety-regulator-2001-15/

[14] Associated Press, "Sleeping Guards Lead to $65G Fine for Nuclear Plant Operator", Fox News, 2 January 2009, https://www.foxnews.com/story/sleeping-guards-lead-to-65g-fine-for-nuclear-plant-operator.amp; "Guards Found Sleeping at Another Power Plant", Global Security Newswire, 11 April 2008, https://www.nti.org/gsn/article/guards-found-sleeping-at-another-power-plant/

[15] Office for Nuclear Regulation, 'Security Assessment Principles for the Civil Nuclear Industry', 2017 Edition, Version 0. [Online] Available at: http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

[16] Office for Nuclear Regulation, 'A guide to Nuclear Regulation in the UK' 2016 update. [Online] available at http://www.onr.org.uk/documents/a-guide-to-nuclear-regulation-in-the-uk.pdf

[17] Interview with staff member at the International Nuclear Services, December 2019.

[18] FINANCIAL TIMES, 'Ethical investing has reached a tipping point' (18 June 2019). https://www.ft.com/content/7d64d1d8-91a6-11e9-b7ea-60e35ef678d2

[19] PEHUET LUCET, F. 'Conditions and possibilities for financing new nuclear power plants', *Journal of World Energy Law & Business*, Vol.12, No.1, pp.21-35 (22 December 2018).

[20] 'Nuclear Power Plant Exporters' Principles of Conduct', Carnegie Endowment for International Peace https://carnegieendowment.org/publications/special/misc/nppe/

[21] WINS, Corporate Governance Arrangements for Nuclear Security: Analysis of Annual Reports from Companies and Regulators, (1 March 2014) https://wins.org/document/corporate-governance-arrangements-for-nuclear-security-analysis-of-annual-reports-from-companies-and-regulators/

[22] FINANCIAL TIMES, 'UK can emulate key accounting reforms of Sarbanes-Oxley Act' (28 Feb 2019) https://www.ft.com/content/86b6d8a2-3aa9-11e9-b72b-2c7f526ca5d0

[23] Centre for the Protection of National Infrastructure, https://www.cpni.gov.uk/; Nuclear Decommissioning Authority https://www.gov.uk/government/organisations/nuclear-decommissioning-authority.

[24] Alan Heyes, Wyn Q. Bowen and Hugh Chalmers, 'The Global Partnership against WMD: Success and Shortcomings of G8 Threat Reduction (19th October 2011) https://rusi.org/publication/whitehall-papers/global-partnership-against-wmd-success-and-shortcomings-g8-threat