CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Security Culture

An Educational Handbook of Nuclear & Non-Nuclear Case Studies

Geoffrey Chapman, Robert Downes, Christopher Eldridge, Christopher Hobbs,
Luca Lentini, Matthew Moran, Alberto Muti & Daniel Salisbury

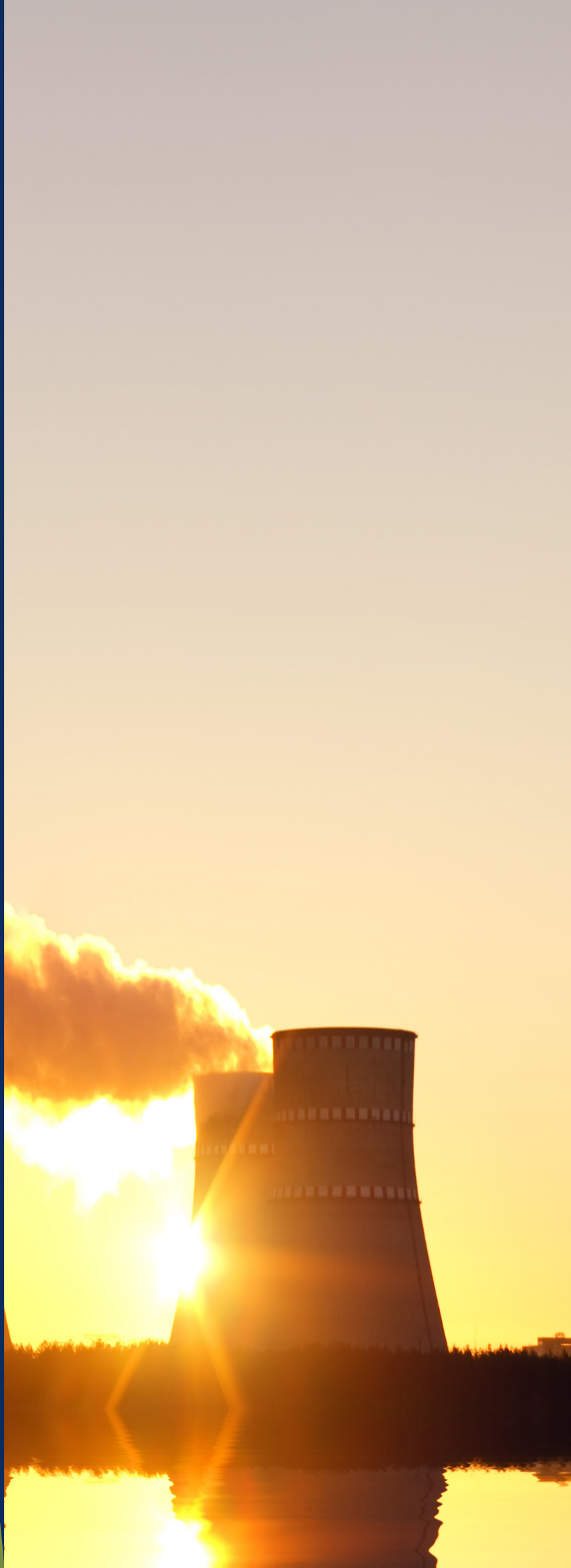
AUGUST 2017

Glossary

CSSS	Centre for Science and Security Studies at King's College London
DOE	US Department of Energy
DPRK	Democratic People's Republic of Korea
FCC	Feed Clarification Cell
HEAT	Head End Accountancy Tank
HEU	Highly Enriched Uranium
HEUMF	Highly Enriched Uranium Materials Facility
HGSD	Hatton Garden Safe Deposit, Ltd.
HMNB	Her Majesty's Naval Base (UK)
IAEA	International Atomoic Energy Agency
INES	International Nuclear Event Scale
NMAC	Nuclear Material Accounting and Control
NNSA	U.S. National Nuclear Security Adminsitration
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSS	Nuclear Security Summit
PID	Perimeter Intruder Detection System (UK)
PIDAS	Perimeter Intrusion Detection and Assessment System (U.S.)
PNS	US State Department's Partnership for Nuclear Security
SCND	Scottish Campaign for Nuclear Disarmament
SO	Security Officer
SOP	Standard Operating Procedure
SSBN	Nuclear Powered, Ballistic Missile, Submarine
THORP	Thermal Oxide Reprocessing Plant
USD	United States Dollars

Table of contents

Introduction



Although nuclear facilities are employing increasingly high-tech and automated security systems, it is widely acknowledged that human beings still have a critical role to play in their design, maintenance, operation and assessment. Here past incidents have shown that the actions of individuals within these systems can have a significant impact on their success or failure. The importance of the 'human dimension of nuclear security' was stressed during the recent high-level Nuclear Security Summit (NSS) process, together with the need for organisations to develop a strong 'security culture', necessary to protect against a range of internal and external threats.[1] Culture is a complex concept, with many different interpretations. For nuclear security culture by far the most widely accepted model is that put forward by the International Atomic Energy Agency (IAEA).[2] Drawing on the work of organizational psychologist Edgar Schein the IAEA model deconstructs nuclear security culture into a series of interlinked levels, which include beliefs and attitudes, behavioural principles, behaviour, leadership and management systems (see Figure 1). For each of these the IAEA's Nuclear Security Series No. 7 'Security Culture' guidance document outlines characteristics reflective of strong security culture and how they might manifest themselves in a generic sense.

FIGURE 1: IAEA MODEL FOR EFFECTIVE NUCLEAR SECURITY CULTURE OUTLINED IN NSS 7.

1 'Workplan of the Washington Nuclear Security Summit', NSS2016, http://www.nss2016.org/document-center-docs/2010-washington-work-plan (12th April 2010).

2 'Nuclear Security Culture', IAEA Nuclear Security Series (NSS) No. 7, www-pub.iaea.org/MTCD/publications/PDF/Pub1347_web.pdf (2008).

The IAEA model provides a useful structure for breaking down and analyzing security culture in different types of organization. This is a necessary step if specific weaknesses are to identified and addressed and it is this model which we use to interrogate the case studies presented within this handbook. However, it should be noted that there are also factors outside of an organization that can influence security culture, for example, its interaction with the regulator. This and other external factors are also examined within the case studies in this handbook, which highlight, for example, how inappropriate oversight and regulatory approaches can weaken security culture at the organizational level.

The Handbook

This handbook is aimed at nuclear security educators and trainers, with the goal of providing them with a set of security culture case studies that can be adapted and used as part of their internal courses. For all the case studies, relevant discussion points and references have been provided, as have corresponding Power Point presentations, for which softcopy is available separately. Educators and trainers should adapt these for use at their specific institutes, as they demonstrate just one way in which the case studies might be presented. In the following section the utility of case studies and the different ways in which they might be integrated into nuclear security courses is discussed. This is the second nuclear security educational case study handbook produced by the Centre for Science and Security Studies (CSSS) at King's College London (KCL). The first focused on insider threats and it should be emphasized that many of the examples outlined there are also relevant from a security culture perspective. Educators and trainers may wish to consider applying the nuclear security culture model outlined above to the cases contained within the preceding handbook. We hope that this will be a useful resource for current and future nuclear security trainers and educators.

Case Studies as a Pedagogical Tool

In the field of education, broadly defined, scholars and practitioners have long sought to identify and implement teaching methods that would engage students and promote what is commonly termed 'deep learning'. As early as 1929, A. N. Whitehead protested 'against dead knowledge, that is to say, against inert ideas'.[3] For Lee Schulman, writing in the early 1990s, this translated as an argument against 'academic programs dominated by the twin demons of lecture and textbook, each a method designed to predigest and deliver a body of key facts and principles through exposition to a rather passive audience of students'.[4]

CASE STUDIES

STORIES THAT PRESENT REALISTIC, COMPLEX, AND CONTEXTUALLY RICH SITUATIONS AND OFTEN INVOLVE A DILEMMA, CONFLICT, OR PROBLEM

The problem, for these and other scholars, was that students were 'mindlessly memorizing and rotely rehearsing. They were surely not learning to connect theory to action, nor were they coming to think analytically or critically'.[5] This perceived gap between theory and practice, in particular, continues to dominate the thinking of academics working in this area. In 2012, for example, Kinsella and Pitman noted 'that the professions and education for the professions are plagued with claims of a theory-practice gap—that the education is too theoretical, or not sufficiently practice focused'.[6]

One of the ways that educators have sought to address the problems mentioned above, and particularly what Gravett *et al.* term the 'theory-practice predicament', is through the case study approach.[7] A range of terms are used to describe this approach in the academic literature – 'case-study methodology', 'case-study pedagogy', 'case-study method', 'case-study instruction', 'case discussion as pedagogical method', and 'case reading and discussion'.[8] Fundamentally , however, all of these terms describe an approach to education and training that offers an alternative pathway to traditional, static pedagogical methods such as lectures, and provides a dynamic means of grounding theory in practice.

What are case studies?

So what are case studies and how can they be effectively integrated into the practice of educators? Well case studies have been described as stories, presenting 'realistic, complex, and contextually rich situations and often involve a dilemma, conflict, or problem'.[9] If utilized correctly they can stimulate students to 'study all of the available information from which decisions must be made' as opposed to just engaging with general theories.[10] Merseth notes that 'the analysis and discussion of individual cases by students in their training to become lawyers' was used by Harvard Law School as early as 1870, but it was the university's Graduate School of Business Administration that pioneered the 'case method of teaching business administration by using systematically arranged problems reported from life instead of lectures'.[11]

3 A. N. Whitehead, The Aims of Education and Other Essays (New York: Macmillan, 1929), p.1.
4 Lee S. Schulman, 'Toward a Pedagogy of Cases', in J. H. Schulman (ed.), Case Methods in Teacher Education (New York: Teachers College Press, 1992), p.1.
5 Ibid.
6 E. A. Kinsella and A. Pitman (eds.) Phronesis as professional knowledge. Practical wisdom in the professions. (Rotterdam: Sense, 2012).
7 Sarah Gravett, Josef de Beer, Rika Odendaal-Kroon and Katherine K. Merseth, 'The affordances of case-based teaching for the professional learning of student-teachers', Journal of Curriculum Studies (2017), Vol.49, No.3, p.370.
8 Ibid., p. 372.
9 'Instructional Strategies', Eberly Centre for Teaching Excellence and Educational Innovation, Carnegie Mellon University, https://www.cmu.edu/teaching/designteach/design/instructionalstrategies/casestudies.html.
10 Edwin C. Leonard Jr. and Roy A. Cook, 'Teaching with Cases', Journal of Teaching in Travel & Tourism (2010), Vol.10, No.1, p.96.
11 Katherine K. Merseth, 'The Early history of Case-Based Instruction: Insights for Teacher Education Today', Journal of Teacher Education (1991), Vol.42, No.4, p.243.

The case study approach is student-centric, allowing participants to explore the 'complex and messy problems of practice' in an artificial environment where flawed decisions have no lasting consequences.[12] This is important, for case studies often contain an element of uncertainty. Indeed, it is for this reason Schulman describes them as accounts 'of an experience in which our intentions have been unexpectedly obstructed, and the surprising event has triggered the need to examine alternative courses of action'.[13] The case study approach allows students to embrace uncertainty and probe the nuances and implications of various courses of action.

In practice, case studies also encourage the development of critical thinking skills and the ability to present evidence as part of a coherent argument. They also typically give students the opportunity to work in a group setting and by doing so improve a variety of interpersonal skills including teamwork, communication, time management and resource allocation. These are qualities sought after by potential future employers.

Certainly, the case study approach poses challenges. The uncertainty and intellectual freedom that accompanies case studies is often an unfamiliar pedagogical setting that can unnerve students. For example, 'students might perceive that the instructor is relinquishing his or her role as instructional leader by not giving them the correct answer to a case problem'.[14] Students may also face other difficulties, such as problems assimilating 'the highly nuanced discussion and debate that case analysis often engenders, resulting in frustration or a growing disinterest with the topic'.[15] Students may also may find it difficult to relate the details of the case study back to theoretical discussions or principles without adequate guidance. This challenge can be compounded by a lack of preparation.

Using case studies can also present a challenge for the educator. For many case studies the outcome of the exercise is not necessarily fixed. Consequently, despite careful planning it is not possible to predict every possible avenue of student enquiry, which will need to be assessed and managed on the fly. Ensuring the exercise stays within the focus of the broader course learning objectives will therefore be a constant challenge and it is for this reason that the case study approach is often described as the 'art of managing uncertainty', with the instructor often serving as 'planner, host, moderator, devil's advocate, fellow student, and judge'.[16]

Ultimately, however, the academic literature recognises the value of this approach for educators seeking to cultivate a dynamic and engaging classroom. It is worth noting that the enthusiasm with which educators have embraced the case study approach as a pedagogical tool is mirrored in the progress and engagement of students. Evidence suggests that 'student evaluations improve when the case study method is used instead of the traditional lecture approach'.[17] Furthermore, studies have demonstrated that 'the use of case studies ranks as the classroom method considered the most effective for developing critical thinking skills'.[18] Ultimately, 'the characteristically complex nature of the case study reflects situations and vectors of influence likely to be found in [...] real-world setting[s]', and students recognise, appreciate and respond to this link to real-life problems.[19]

12 K. Merserth, 'Cases and Case Methods in Teacher Education', in J. Sikula (ed.), Handbook of research on Teacher Education. 2nd ed. (New York: Simon & Schuster, 1996), p.725.
13 J. H. Schulman cited in Gravett et al., 'The affordances of case-based teaching for the professional learning of student-teachers', p.372.
14 Mark P. Mostert, 'Challenges of Case-Based Teaching', The Behavior Analyst Today (2007), Vol.8, No.4, p.437.
15 Ibid.
16 J. K. Satia, Madhavi Misra, Radhika Arora and Sourav Neogi (Eds.), 'Innovations in Maternal Health: Case Studies from India' (Sage Publications, 2014) p. xliii.
17 Leonard and Cook, 'Teaching with Cases', p.96.
18 Leonard and Cook, 'Teaching with Cases', p.96.
19 Mark P. Mostert, 'Challenges of Case-Based Teaching', The Behavior Analyst Today (2007), Vol.8, No.4, p.435.

Approaches to Case Studies

1. The Narrative Approach

In terms of use and implementation, the case study approach offers considerable flexibility. Consider the most common distinction made in the literature between types of case study. The 'retrospective' or 'narrative' approach provides a 'comprehensive history of a problem – complete with multiple actors, contending interests, and the real outcome'.[20] The objective here is for students to analyse how and why events have evolved and suggest if possible, alternative preferential solutions. This type of case study can be deployed at any point in a course – at the beginning to illustrate the benefits or pitfalls of a particular approach, or at the end of a course to compare and contrast lessons learned with the actual outcome of a real-life story – and thus offers the educator flexibility in terms of how it fits with broader learning objectives.

2. The Decision-Forcing Approach

The other type of case study commonly discussed is a 'decision-forcing' one. Here students are provided with a certain amount of information but the outcome of a particular step. This forces them to 'identify and assess the range of possible options for action'.[21] Typically a case study presented in this way will include an 'epilogue', provided after the students' analysis is complete. This sets out actual events, which can be analysed and contrasted with those put forward by the students. A decision-forcing case study can also benefit the students in different ways according to the point of deployment. Utilised at an early stage, for example, this type of case study could encourage creative thinking ahead of engagement with theory or principles. Students could find themselves aligning with established theories before even encountering them, and this, in turn, could subsequently serve as a source of motivation and engagement for the student as the course progresses. Alternatively, decision-forcing case studies could be utilized towards the end of a course, with the goal of allowing knowledgeable students hone their critical skills on the complexities of some real-world problems.

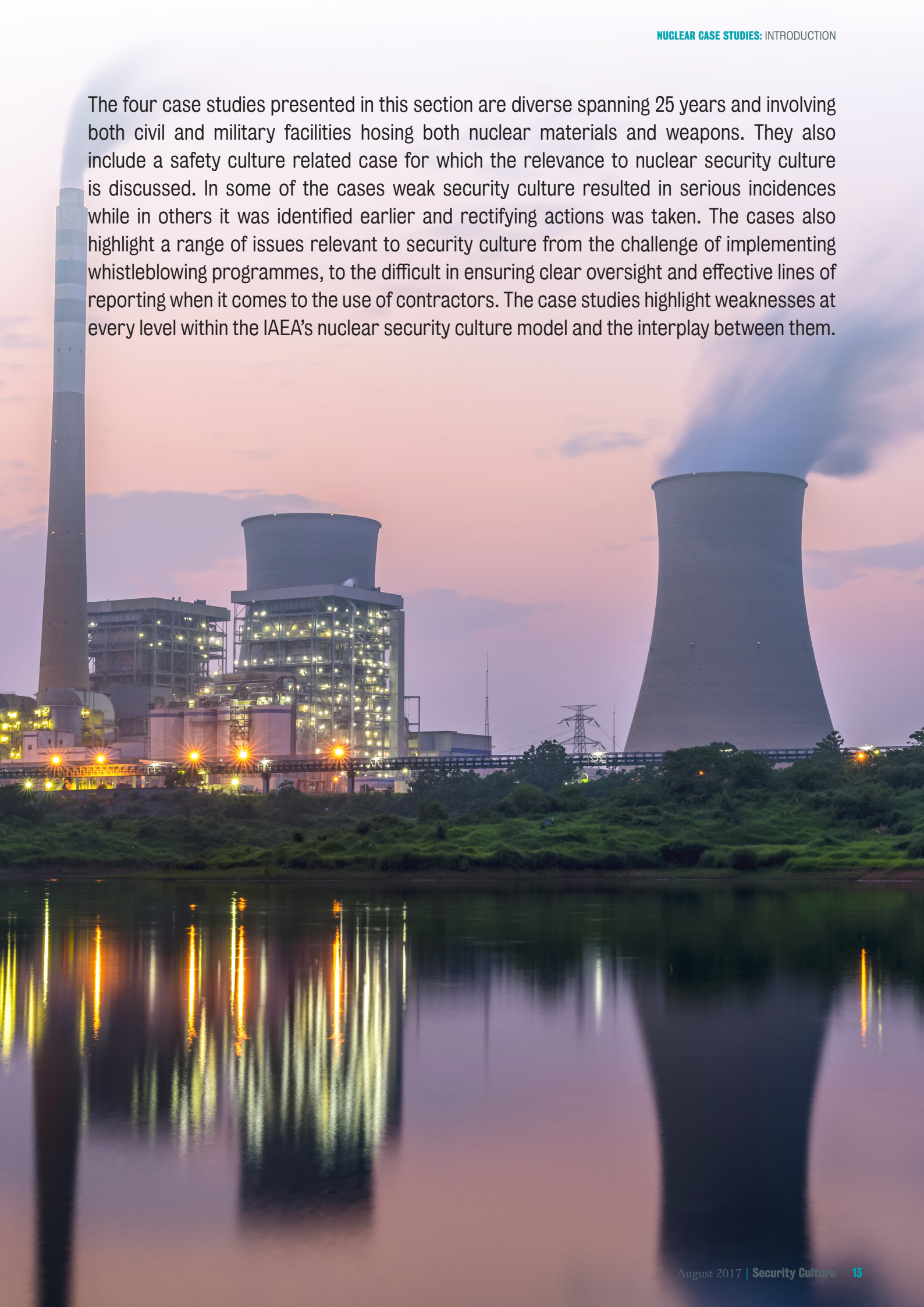
Nuclear Security and Case Studies

The realm of nuclear security, and particularly the complex and multifaceted issue of security culture, is well-suited to the case study approach. Gathered together in this handbook are a range of thought-provoking case studies - some nuclear-specific, others drawn from other sectors - each bringing its own particular set of problems to be analysed and dissected. On one hand, engagement with these cases will allow students to identify the fundamental challenges posed to the cultivation and practice of a strong and robust security culture. On the other hand, the cases all leave room for students to explore the 'what if', the various alternative pathways that lead from each scenario. These will provide much food for thought. Ultimately, if these case studies are analysed, as intended, in the light of the IAEA guidance and the underpinning work by Edgar Schein, students should find a multitude of ways to relate the practicalities of each case back to the broader issues and principles that underpin nuclear security culture.

20 Golich, Boyer, Franko and Lamy, 'The ABCs of Case Teaching', p.1.
21 Ibid.

Nuclear Case Studies

The four case studies presented in this section are diverse spanning 25 years and involving both civil and military facilities hosing both nuclear materials and weapons. They also include a safety culture related case for which the relevance to nuclear security culture is discussed. In some of the cases weak security culture resulted in serious incidences while in others it was identified earlier and rectifying actions was taken. The cases also highlight a range of issues relevant to security culture from the challenge of implementing whistleblowing programmes, to the difficult in ensuring clear oversight and effective lines of reporting when it comes to the use of contractors. The case studies highlight weaknesses at every level within the IAEA's nuclear security culture model and the interplay between them.



Case Study 1: Break in at Y-12 National Security Complex, United States

Background

The Y-12 National Security Complex is a large nuclear facility located in Tennessee in the South Eastern United States, covering over 800 acres and containing more than 500 buildings. The facility has been operating since the Second World War when it produced the High Enriched Uranium (HEU) for the U.S. nuclear weapons programme. It is owned by the National Nuclear Security Administration (NNSA), a government agency under the U.S. Department of Energy and is operated by a number of contractor organisations. Y-12 continues to store a large, yet undisclosed, quantity of HEU, within the High Enriched Uranium Materials Facility (HEUMF) which was completed in 2011. The HEUMF has been described as the "nation's central repository for highly enriched uranium", although the exact quantity stored is classified. The building is located on the north-west facing side of the site, adjacent to the perimeter.

As a purpose built and modern facility, the HEUMF was clearly designed with security in mind, with material moved to it from multiple ageing storage facilities, consolidating much of the HEU into a single location. The HEUMF is alleged to have cost $549 million to construct, and is reportedly designed to be able to withstand various natural and human catastrophes including flooding, lightning strikes, earthquakes, tornados, and the impact of an aircraft crash. The security budget for the broader Y-12 complex is also significant, with reports citing that $150 million was spent securing the facility in 2012. Because of the facility's historic role in the production of material for the bomb dropped on Hiroshima, Y-12 has seen significant anti-nuclear weapons activity. Protests were seen as early as the 1980s, with much of this focused on the anniversary of the bombing of Hiroshima in August.

Security Breach in 2012

In the early hours of the 28th July 2012 three elderly anti-nuclear activists (including an 82-year old Catholic nun) made an incursion into the Y-12 facility. The group accessed the facility from the northwest, crossing a golf course and walking through a wooded area before climbing over the boundary fence. They crossed a patrol road, and then proceeded to cut through three alarmed Perimeter Intrusion Detection and Assessment System (PIDAS) fences, triggering multiple sensors in the process. This gave them access to the protected area surrounding the HEUMF, at which point they proceeded to spray paint the side of the building, cover it in the blood of a fellow deceased activist, hang banners and bang on the side of the building. The protestors remained and roamed around in the protected area for some time, but did not gain access to the building itself.

Weakness in Security Culture?

Weaknesses in security culture played a significant role in enabling the 2012 breach in security at Y-12. This was acknowledged in several official statements after the incursion. For example, in its post incident report, the U.S. Department of Energy (DOE) stated that failures had "contributed to an atmosphere in which the trespassers could gain access to the protected security area". More specifically the report highlighted concerns in several broad areas which feature in the IAEA's nuclear security culture model (in NSS No.7), including "misunderstanding of security protocols, poor communications, and weaknesses in contract and resource management".

In a letter to the security contractor, the NNSA noted that "contributing and direct causes of the security event include an inappropriate Y-12 cultural mindset, as well as a severe lapse of

discipline and performance". Cultural issues are apparent in the inadequate initial response to the incident – showcasing the importance that individuals can play in enhancing or undermining nuclear security. The incident also highlights more broadly how weak security culture can manifest itself in an organisational context – both at Y-12 and at higher levels.

Inadequate Response

The actions of the first responder and officers inside the HEUMF observation towers were heavily criticised. The DOE report found that despite several alarms being triggered, a Protective Force officer "was not promptly dispatched to assess the situation". When the first responder arrived on the scene, his actions were viewed as inadequate: he did not secure the scene, neutralize the protestors or draw his firearm in line with procedures. "Adherence to procedures" is a key element of "personnel behaviors" in the IAEA NSS 7 security culture model. Rather, he remained in his vehicle answering a phone call from a supervisor, and allegedly did not notice the protestors until they approached the vehicle and "surrendered" to him. He had allowed the protestors to roam around the protected area and retrieve items from their backpacks.

The first responder exited the vehicle when his supervisor arrived. Despite his supervisor's greater sense of urgency (he showed belief that "credible threat exists", concerned the incursion was a diversion, and there could be snipers positioned in the hills) the first responder still did not provide cover, continuing to "look away from the trespassers at other areas of the site". Officers in the HEUMF also did not respond in an adequate manner – utilizing an unauthorized technology to assess the scene and silencing an alarm without assessing the situation. The actions of these individuals – and especially the first responder – emphasise the important role that individuals play in ensuring nuclear security. His actions were not in line with procedures, and call into question the beliefs and attitudes at the foundations of the IAEA model, that "credible threat exists" and "nuclear security is important".

Following the incident – after initially being praised by his employer – the first responder was fired, and further sought to justify his actions in a 2014 legal case. He argued:

> *"Like I told the arbitrator… we can sit here and you can scrutinize me all you want, but at the end of the day I stopped their actions, I detained them, I called for backup, we arrested them, I testified against them and they're in prison. How much more picture perfect can it be than that? And I went home to my family, and nobody got killed and nobody got hurt."*

He claimed he was a "scapegoat" for the intrusion. However, his behavior and later attempts to justify it exhibits little regard for the characteristics on the IAEA model listed under "personnel behavior", specifically "personal accountability".

Broader Cultural Issues at Y-12

The enquiry into the incident also called into question security culture at the Y-12 complex more broadly. Significant criticism revolved around the handling of security equipment and technology. The DOE report suggested that repairs of security equipment was "not always treated as a priority at Y-12". Critical items were said to be repaired in five to ten days, rather than the NNSA recommended 24 hours. It also appears that at Y-12 this timeframe was viewed as a goal, not a requirement. Contractors not taking the maintenance of equipment seriously impacted on the events of 28th July 2012 – one fixed camera that would have provided some coverage of the events had been out of service for six months. Also, the manner of testing equipment – just to check that there was a "feed" available from the device – was criticised. One piece of equipment which could have detected the incursion immediately had several features allowing it to do this out of service. This falls directly into the "Operation and maintenance" characteristic within IAEA's culture model under "management systems". Indicators for this characteristic – include that the maintenance of security equipment is performed according to "approved procedures" and

that compensatory measures are used when equipment breaks down. In the Y-12 case, it appears that the procedures for maintenance were not appropriate, and that compensatory measures were both inadequately and over-utilised.

The DOE report also uncovered problematic communication at the facility, which had manifested during the event. "Effective communication" is listed as a key "leadership behaviour" within NSS 7. On 28th July, personnel working inside the HEUMF assumed that the hammering on the side of the building was the actions of maintenance workers, rather than protestors, as they were frequently not informed when such work was taking place. In addition protective force officers were not advised of the equipment outages by their colleagues when they started their shifts.

Cultural Issues at Higher Levels?

The IAEA model places great emphasis on the roles of management and leadership in building a strong nuclear security culture. Some of the issues highlighted by the event of 28th July at Y-12 can be attributed to beliefs, attitudes and approaches at a higher-level. Constrained federal funding was said to have caused decision makers to reduce the "delay" security features surrounding the HEUMF in 2008. Financial pressures also reduced the protective force patrols at the facility. Human resources were also limited, with the same teams responsible for putting in place new security equipment and maintaining existing equipment. These resource cuts are likely to have made it difficult for security personnel to do their job properly.

The way that security contracts were organised at Y-12 also negatively impacted on an integrated approach to security. The maintenance and testing of physical protection systems was conducted by one contractor, while the protective force function was managed through a separate contractor. As the DOE report noted, "The fractured management structure appeared to have led to conflicting priorities". The approach to handling contractors – and particularly limited levels of oversight of contractor activities at the U.S. national labs – was also criticised, with allegations that the DOE had developed a "hands-off-the-contractor culture". In this respect, characteristics of the IAEA model under "leadership behaviors" seem to have been compromised – including "management oversight".

Consequences

The three protestors were jailed for between three and five years in 2014, although they later had their convictions overturned. The first responder was the only person to lose his job because of the event. The contractor who managed the Protective Force lost its contract following the incident and criticism was also leveled at the Department of Energy and the then Energy secretary Steven Chu.

Suggested Discussion Points:

- What does this case tell us about the importance of individuals in ensuring the security of nuclear facilities?
- Why do you think the first responder acted in the way that he did? What does this tell us about the importance – and difficulties – of managing and motivating a guard force?
- What does this case tell us about the importance of the human factor in the design, operation and maintenance of physical protection systems?

Case Study 2: Sleeping Guards at Peach Bottom NPP, United States

Background

Peach Bottom Nuclear Power Plant (NPP) is a large nuclear facility in Pennsylvania in the United States. The facility is owned by Exelon Generation and Public Service and Gas of New Jersey. Since it was inaugurated, the site has hosted three reactor units – two of which are still operating. The facility is in a highly populated area on the East Coast of the United States, with five million people living within a 50-mile radius. The guard force at Peach Bottom at the time of this case was operated by the contractor Wackenhut.

Sleeping on the Job

In September 2007, a series of allegations were made public regarding the guard force at Peach Bottom and other U.S. nuclear power plants. A guard who had seen his colleagues sleeping had previously tried to raise this with his superiors at Wackenhut in spring 2007. He also anonymously (through a friend) raised the issue with a regional office of the Nuclear Regulatory Commission (NRC). Although the NRC let the matter drop when Exelon claimed that there was no evidence of guards sleeping. When no action was taken, the guard made a video on his camera phone, and sent it to CBS News. Some of the allegations made public included:

- Guards routinely sleeping with firearms inside the "ready room" at Peach Bottom, with videos showing his colleagues asleep in March, June and August of 2007;
- Guards sleeping in the "bullet proof watch towers" at the perimeter of the facility;
- Guards sometimes-working 60 or more hours per week.

In total, the guard believed that he had seen around 20 of his colleagues sleeping at various points at Peach Bottom. It should be noted that these allegations are not unique to Peach Bottom. The U.S. Nuclear Regulatory Commission has also investigated sleeping guards at another U.S. NPP – Turkey Point in Florida between 2004 and 2006. Ensuring that a guard force remains motivated and believes "credible threat exists" when security incidents are relatively infrequent is a challenging task.

Was this a Problem?

The true severity of the problem in this case – the guards sleeping on the job – is arguably ambiguous. Some jobs permit sleeping in certain circumstances, even when a certain level of "readiness" is required. For example, firefighters can often be on shift for 48 hours, ready to deploy at a moment's notice, but are permitted to sleep. Soldiers can also sleep when under a certain level of readiness. A full judgment cannot be made in the Peach Bottom case without knowing the exact location, time and existing procedures. That guards were sleeping in the "watch towers" is far more concerning than in the "ready room", where the level of readiness is more ambiguous.

The response – although only occurring after the guard leaked the story to the media – does suggest that what was happening was considered highly problematic. Exelon, the operator, terminated its Peach Bottom contract with Wackenhut in December 2007. Wackenhut also lost the contracts for guarding another nine of Exelon's nuclear plants – one-third of its total business in relation to NPPs. In 2008, Wackenhut's CEO resigned, and a hearing was

held in a U.S. House of Representatives Committee into why the claim wasn't taken more seriously by the NRC. At the hearing, the NRC Chairman noted:

> *"I want to make it very clear that this behaviour is unacceptable. The NRC requires that security personnel, along with other personnel, be attentive at all times."*

In 2009 Exelon was be fined $65,000, over the Peach Bottom case but continued to maintain that "at no time was security compromised".

Whistleblowing

The case also highlights the issue of "whistleblowing", and ensuring that there are appropriate and confidential avenues where employees can raise security related issues and when issues are raised, they are subject to an independent and unbiased investigation. In this case, the guard's concerns not being taken seriously led him to leak details to the press. It would appear that he did so because he was concerned about compromised security, and because he had no other options.

Whistleblowing and whistle-blowers can be controversial. As noted below, the guard's supervisor suggested that raising the issue could compromise relationships with his team. Mechanisms for whistleblowing need to be adequately thought-out, and have appropriate checks and balances. It is possible that they might be used by employees to pursue personal vendettas. The NRC Chairman noted that only one in ten "allegations" are "substantiated and warrant enforcement action". Furthermore, apparently 80 percent of allegations received by the NRC are referred back to the operator for investigation.

The way that the whistleblowing guard was treated after he took the story to the media is also worthy of note. After Wackenhut lost the contract, a number of the guards were re-hired for a revamped security force. The guard who blew the whistle was not one of these, and was allegedly told that he didn't "meet the criteria for the job".

Cultural Dimensions?

Statements from different parties – the whistleblowing guard, within the operator and the regulator – suggest a cultural dimension to this case. Allegedly when the guard spoke to his supervisor about the sleeping guards, his supervisor said: "don't talk about that, focus on being a team player". The guard believed that this attitude showed that sleeping on the job was "socially acceptable", and that "it was a culture that it was OK to do it". The conditions in the ready room, and the situation that the guards found themselves in during their daily activities were highlighted as problematic and according to the NRC were said to be:

> *"not conducive to attentiveness and station management... failed to address these known adverse conditions. The 'ready room' had high background noise, was dimly lit and was poorly ventilated".*

This suggests that issues with work environment had undermined security culture – this is reflected in the IAEA's model under management systems. This was exacerbated by the management's failure to recognise the lack of activity undertaken by guards during long shifts. The NRC noted, Exelon:

> *"Failed to identify human factor issues related to 12-hour shifts spent, in part, at the 'ready room' post with low physical activity. For some SOs [security officers], a significant portion of the shift could be spent sitting in the ready room when not on patrol or performing other duties."*

This evidence raises questions regarding other elements of the IAEA's nuclear security culture model – including "improving performance" and "motivation" under leadership

behaviour. A former Security Force manager at Wackenhut has suggested that the contractor management was aware that guards were frequently sleeping on the job and did nothing to remedy this. Another individual who used to run training courses for the guards, noted more broadly that "attitudes towards security" were "problematic". A further Wackenhut employee had previously noted that operators had been pressing for lower costs, suggesting they were "down to the bone".

At a higher-level, an Exelon CEO would later acknowledge that it was "disturbing" to realise "that a 'subculture' existed where this behaviour was tolerated and accepted among certain members of the security guard force". A representative of the Nuclear Regulatory Commission also suggested that the NRC's response had been inadequate – "more than anything else, we have to change the way the NRC responds to these allegations". Furthermore, the NRC Chairman testified that the Peach Bottom incident suggested "that there may be a disconnect between safety and security culture". Following this case, the NRC "decided to expand its policy on safety culture to explicitly address security".

Several characteristics of a strong nuclear security culture – as set out in the IAEA model – appear to have been compromised in this case. The guards do not seem to have internalised the fundamental belief that "credible threat exists". Other characteristics can also be observed as problematic – including all the "principles for guiding decisions and behaviour" – particularly, "motivation" and "professionalism". The case also reflects weaknesses with regards to many of the characteristics listed under management systems and leadership and personnel behaviour – notable examples being "self-assessment", "interface with the regulator", "management oversight", and "vigilance".

Suggested Discussion Points:

- What do you believe was the key cause for guards sleeping on the job? Can you link these to the IAEA nuclear security culture model?
- What does the initial response of the operator and the NRC tell you about attitudes to nuclear security?
- What role do "whistleblowing" mechanisms play in ensuring a strong nuclear security culture?
- In your opinion, was the treatment of the whistle-blower appropriate?

Case Study 3: Protestor Incursion at HMNB Clyde, United Kingdom

Background

Her Majesty's Naval Base (HMNB) Clyde is home to the United Kingdom's Submarine Service. The site was selected in the early 1960s following an extensive search for a suitable location for the UK's Polaris nuclear submarines (SSBNs). HMNB Clyde, which is also known as Faslane, was thought to provide the Royal Navy with the best overall balance of operational, safety, and cost considerations compared with alternative locations. Following construction, the base was commissioned in 1967. Since then, HMNB Clyde has been the home base for both generations of the UK's SSBN fleet, the Resolution and Vanguard class submarines, and will continue to play this role for Vanguard's replacement, the Dreadnought class submarine.

Following the 1982 decision to replace the ageing Polaris missile system, a major programme of work was undertaken at Faslane. The new Vanguard class submarines that would carry the new Trident missiles required enhanced and modernised facilities. Dubbed the Trident Works Programme, the renovation was one of the largest and most complex construction programmes undertaken by the UK's Ministry of Defense. The portion of the Programme carried out at Faslane and the nearby Coulport armoury began in 1985 and finished in 1991, with a total cost of £1.9bn. At the Faslane site, the programme consisted of over one hundred separate projects, including an eleven-story ship lift and a new power generating facility.

Physical protection systems at the site were upgraded as part of the programme. They included "seemingly endless" lines of perimeter fences and razor wire, security patrols with dogs, CCTV cameras, infrared sensors, observation towers, and modification of the surrounding landscape and waterways for enhanced site security. An un-climbable and un-cuttable "super-fence" equipped with a Perimeter Intruder Detection System (PIDS) was central to the upgrade. With a concept of operations stressing the importance of defense-in-depth, these measures were fully integrated into the complex naval base.

Faslane was therefore one of the most heavily fortified facilities against external intrusion in the UK in the late 1980s. Despite this, in 1988 three anti-nuclear protestors gained access to the facility's vital Green area which contained HMS Repulse, a Polaris submarine. The protestors managed to gain entry to the submarine's control room before they were apprehended. Weaknesses in security culture were crucial in the protestors' success.

Protest at HMNB Clyde: A Brief History

Faslane's role as the UK's major submarine base has engendered many acts of protest dating from the early 1960s. Actions have been carried out by a range of civil society groups as well as the broader disarmament movement. Various combinations of Christian organisations, students, trade unions, and local authorities worked with independent anti-nuclear organisations such as Greenpeace UK, Trident Ploughshares, and the Scottish Campaign for Nuclear Disarmament (SCND) to organise protest and civil disobedience. In an early example, on 4th March 1961 the SCND and the Direct Action Committee Against Nuclear Weapons organised a 1,000-person march against Faslane in opposition to American submarines at the base.

In 1982 the Faslane Peace Camp was founded as a permanent presence outside the HMNB Clyde with the support of Strathclyde Regional Council. Typical actions by protestors included "spontaneous presentations, bonfires, premeditated interruption of submarines while navigating through Scottish lochs and the blockading of Faslane itself or warhead

transports...spray painting slogans...[Attempting] physically to disrupt the patrols of massive boats while they traversed the Clyde also became a featured item for the movement as countless numbers of activists, with little regard for their own personal safety, attempted to swim into the path of these boats...Furthermore, the blockading of Faslane had been accompanied by a multitude of operations that included activists chaining themselves to rails, damaging fences that surrounded shore facilities and frequent incidents of illegal trespass."

The Faslane naval base was therefore subject to regular protest over many years. By the late 1980s, security forces at the facility had been regularly contending with well-resourced and inventive protestors for thirty years. A permanent protest camp had been established for a decade. From 1985, with the inception of the Trident Works Programme, physical security measures at the facility were upgraded and the guard force expanded. Security should have been a priority at Faslane given its highly sensitive nature and routine acts of protest.

The Incident: 1988 Protestor Incursion

In the early hours of 10th October 1988, four protestors decided to undertake a non-violent protest action. A permanent resident of the Faslane Peace Camp planned to swim into a dock where Polaris submarines moored in-between patrols. At the time, only one submarine, HMS Repulse, was berthed at the base: the swimmer planned to spray-paint the submarine with anti-nuclear slogans. Three other activists would assist the protest by acting as a decoy, drawing attention from the swimmer by climbing the new super-fence and attempting to gain access to the site. All had a past history of incursion at the facility.

At 1:30 am the protestors breached perimeter fences at a location where razor wire had been removed by construction crews. Using a pair of heavy bolt cutters, the three protestors cut the super-fence so that the gap was "invisible to close scrutiny" by roving guards. Much to the protestors' surprise, the PIDS fence failed to initiate an alarm. After following a drunken sailor into the heart of the base the protestors gained access to the Red Area, the second most vital area of the base, using a construction worker's ladder. They immediately went on to access the Green area, the most sensitive area of the base where the Polaris submarines docked, by climbing onto dustbins tied to the fence. Both areas were cluttered due to ongoing construction work, which offered many places for the protestors to hide. Taking advantage of a startled guard at the gangway to HMS Repulse, the three protestors ran aboard the submarine and entered the nearest available hatch. They then gained access to the submarine's control room, announcing to the assembled crew "We're from the peace camp and we're hijacking this submarine. Take us to Cuba" before being arrested.

The protestors were far more successful than they had hoped. The swimmer was found in the Green Area (and was, in fact, the first of the four protestors to be discovered) while the remaining three protestors gained access to the control room of one of the UK's SSBNs without any forward planning or specialist equipment. Newly installed security systems and a highly trained and equipped guard force failed to halt the incursion. What went wrong?

Weaknesses in Security Culture

Weaknesses in security culture at Faslane can be gathered into three key areas. Firstly, ongoing upheaval caused by construction work at Faslane undoubtedly assisted the protestors in their incursion. Site security arrangements dictated that several lines of razor wire should have been present both inside and outside perimeter fencing. However, these had been removed "to enable engineering work within the [base] perimeter to proceed." Parts of the base surrounding the sensitive Red and Green Areas were cluttered with construction materials and cabins used by workers. Dustbins attached to the Green Area's fence were used by protestors as a makeshift ladder to gain access to submarine jetties, while ladders left by workmen were used to overcome the Red Area's fence. Construction clutter was also spread on the jetties immediately adjacent to the submarine berths: one officer on the nearby submarine HMS Trafalgar was unable to observe the area due to this impedimenta, which assisted the protestors in approaching HMS Repulse unnoticed. Most importantly, the newly installed PIDS-enabled super-fence had been deactivated for maintenance but had not been subsequently reactivated.

Failure to address the security implications of ongoing construction work is an indicator of poor security culture. Managers must ensure that events affecting security are analysed and appropriate mitigation measures are implemented in such a way that the integrity of the security system is maintained at all times. At Faslane, long-term site renovation was foreseeable and, as such, regularly assessed and updated contingency planning should have been undertaken by site security managers. Of particular importance to the incursion, measures to compensate for the removal or maintenance of security equipment should be instituted. The removal of razor wire and deactivation of the PIDS-enabled super-fence could have been compensated for by increasing the number of guard patrols both inside and outside the base, for example. Furthermore, the large number of contractors working on the complex construction project should have been taken into account in forward planning. Good security culture is characterised by teamwork and cooperation across organisational and bureaucratic boundaries: this includes ensuring roles and responsibilities are adequately explained to new site personnel (including temporary contractors) at initial briefings and further training sessions, and that the needs of external contractors (including the storing of building materials within the site's security perimeter) are factored into security planning.

Secondly, guard patrol arrangements were a problem at the base. The protective security forces inside the super-fence in the region of the base penetrated by the protestors were on a tea-break as the breach occurred. In theory, security forces assigned to another region of the base should have provided coverage during this period. In practice, however, this meant the active guard force was undermanned and located in the wrong part of the site to maintain consistent coverage of the super-fence. When gaining access to the Red Area, the protestors reported standing in direct view of roving guards on two occasions, and were saved only by the guards' lack of vigilance. In the Green Area, there were fewer guards than required by Standard Operating Procedures (SOPs) and those available were also taking refreshment. The personnel near the submarines failed to challenge the protestors, later claiming they had mistaken them for naval officers or a construction crew. However, this seems unlikely as it was "the middle of the night and [one protestor] had a 12 inch mohawk, [another protestor] was wearing a rainbow sweater and donkey jacket, and [the third] had hair down to [his] shoulders."

Poor arrangement and scheduling of security forces is an indicator of weak security culture. Site security managers should work across bureaucratic and organisational boundaries (between different teams and at different areas of the base) to ensure that security coverage is adequately maintained as dictated by the site security plan. Managers should seek to observe the operational performance of security staff to confirm that expectations are being met. In the case of Faslane, the fact that many guard team's tea breaks coincided left the site under-prepared to deal with intruders and undermined the consistent implementation of security measures. While it appears that senior managers and leaders were unable to recognise the degradation of security conditions due to construction work, it is also concerning that SOPs were in place that left the base security force unmanned due to tea breaks. Managers failed to demonstrate good knowledge of security system vulnerabilities and, hence, were unable to use their authority to take remedial action. This implies a concerning lack of management oversight at Faslane. In addition, security personnel failed both to adhere to procedures

and to exercise adequate vigilance in the course of their duties: on several occasions, the intruders were visible but were not seen, and personnel in the Green Area failed to observe basic security protocol in checking identification. This suggests that security personnel were not motivated, another indicator of weak security culture. For security personnel, effective security culture is characterised by compliance with rules, regulations and procedures, and also constant vigilance and a proactive questioning attitude. Managers should seek to keep staff highly motivated, and should ensure appropriate SOPs are adhered to through regular observation and training.

Thirdly, critical security equipment was both inadequately operated and broken at Faslane. The most important piece of physical protection, the PIDS-enabled super-fence, was deactivated during the site breach. Extensive investigations were unable to determine why this was the case, although operator error was strongly believed to be the cause. This meant that secondary equipment such as CCTV cameras and infrared detectors could not focus on the area of concern. In addition, defective floodlighting facilitated the protestors' access to the Green Area and their entry to the submarine was made easier as the gangway gates were broken and awaiting maintenance. Poor lighting in the jetty area made it hard for security personnel to identify the swimming activist who, as a result, was able to roam the jetty area for over an hour before being apprehended.

At a facility with good security culture, personnel understand how their roles contribute to maintaining security. While the maintenance of floodlighting may not appear to be a security critical task, security is a concern for everyone at a sensitive facility. Maintenance should be performed according to approved procedures to ensure that design requirements and site security as a whole are not compromised. Furthermore, when systems are defective, compensatory measures should be put in place. In the case of the broken gangway gates, an enhanced security presence on the jetty could have made up for this short-term weakness. While the work environment at Faslane was not conducive to high standards of performance due to construction clutter (an issue dealt with above), security staff failed to take personal responsibility for system operation: the inadequate operation of the PIDS-enabled fence highlights this lack of personal commitment and responsibility.

Ultimately, weaknesses in security were a major contributory factor in the intrusion. It is apparent that neither security managers nor security personnel believed that a credible threat existed and, hence, that security was important. This is a fundamental requirement for good security culture. Furthermore, staff at all levels, from senior managers to maintenance staff, did not demonstrate the high levels of professional conduct required at such a sensitive nuclear facility. While the activists were intent only on protesting, "if [they] had been an armed group – which [they] could easily have been – [they] would have been in control of British nuclear weapons" by blockading themselves in the submarine. Perhaps more importantly, lessons were learnt slowly following the incident. According to one of the protestors, security forces "built a £10 million fence around the base but it didn't work. For me, the most serious aspect of the story was that two weeks later peace campers broke into the Coulport nuclear weapons store and managed to get up to the fourth level fence around the warhead stores." This occurred despite immediate remedial measures implemented to strengthen base security on the order of UK's Secretary of State for Defence.

Consequences

The incident was a major security lapse at one of the UK's most sensitive military facilities. The UK's Prime Minister Margaret Thatcher wrote that she was "utterly horrified" by the incident which had "all the hallmarks of slackness in protecting sensitive defence installations." Had the perpetrators been armed, wrote her Private Secretary, "the consequences would have been incalculable." Ten members of the Royal Navy were found to have shown "degrees of negligence in the performance of their duties" alongside three police officers. This included the Commodore commanding HMNB Clyde and the commander of the squadron of Marines charged with guarding the submarine. A specially formed Board of Inquiry put forward a report containing 42 remedial actions, which included a renewed focus on maintenance of security equipment and wide cooperation between the different organisations charged with protecting the base.

Despite efforts to keep the story quiet, the incident was a minor public relations disaster. Reports concerning weaknesses at the base appeared in a number of newspapers, including on the front page of the Daily Express. The protestors were charged with a number of offenses, but were ultimately released without any punitive actions being taken.

Suggested Discussion Points:

- What were the indicators of weak security culture shown by the 1988 incursion?
- How could managers have fostered better security culture at HMNB Clyde?
- Why is motivation an important characteristic of good security culture?

Case Study 4: Leak at THORP Facility, United Kingdom

Background

The Thermal Oxide Reprocessing Plant (THORP) is located at Sellafield, the United Kingdom's primary nuclear reprocessing site. The facility reprocesses spent oxide fuel from advanced gas-cooled and light water reactors for domestic and international customers, 97% of this spent fuel is useful and can be reprocessed to produce new mixed oxide fuels. The remaining 3% is not useful and is disposed of as waste after extraction.

The decision to build THORP stemmed from expected growth in the oxide fuel reprocessing market in late 1960s. Early forays into oxide reprocessing were carried out at an older Sellafield facility designed to reprocess Magnox fuels. However, a combination of accidents, increasing international safeguard requirements, and expected market growth led to the realisation that a dedicated oxide fuel facility was required. Initial parliamentary approval for THORP was given in 1978, planning permission was gained in 1983, and construction was completed in 1991. The plant began its fitful operational life amid significant controversy in 1994 and is scheduled for closure and decommissioning starting in 2018. By 2012, the facility had processed over 7,000 tonnes of spent fuel assemblies during its 20-year lifetime.

In April 2005, a substantial leak was discovered at the THORP facility. Investigators determined the leak had taken place over a 9 month period. However, leak detection systems and procedures at the facility failed to identify this incident due to poorly maintained equipment, a lack of adherence to procedure, and limited management oversight. These weaknesses in safety culture were identified as a crucial contributory factor in the failure to stop the leak.

The Reprocessing Process at THORP

At the time of its construction, THORP was one of the world's most complex civil engineering projects. While complicated, the industrial process at THORP can be broken down into four key stages. Firstly, upon arrival at THORP spent fuel assemblies are removed from transport flasks and placed into cooling ponds in the Receipt and Storage Area. This provides time for both cooling and the decay of highly radioactive elements in the fuel assemblies before reprocessing begins. Secondly, cooled fuel assemblies are moved into the Head End Plant Area where they are sheared (broken into small pieces), dissolved in hot nitric acid to form "dissolver product liquor", and centrifuged to remove solid impurities such as pieces of fuel cladding. Outputs of centrifuging then undergo Nuclear Material Accounting and Control (NMAC) processes to satisfy international safeguard requirements and to determine how much material is being processed for each customer. Thirdly, the centrifuged liquor is fed into the Chemical Separation Area where it is divided into uranium, plutonium, and highly radioactive liquid waste effluent streams. Finally, in the Finishing Line Area, the uranium and plutonium are processed into dried powdered form, stored and shipped to customers.

The Feed Clarification Cell

The radio-toxic nature of the dissolver product liquor required the THORP facility to be built to robust specifications. In the Head End Plant Area, the Feed Clarification Cell (FCC) is used for NMAC processes before liquor is passed downstream for chemical separation. The FCC is typically robust: the 36.5m long, 14.5m wide cell has deep 1.5m thick walls constructed from barytes concrete designed to maximise radiation shielding for plant

workers. The 21m tall walls are lined with stainless steel, as is the floor of the whole cell. The thick steel-lined walls and floor form a secondary containment structure that protects workers and the environment from leaks. These could emanate from the tanks, pipework, and other apparatus in the FCC.

The key equipment in the FCC includes a centrifuge feed tank (which accepts unclarified dissolver product liquor after shearing but before centrifuging), two centrifuges, and two diverters, which feed centrifuged liquor into either of two head end accountancy tanks (HEATs). The HEATs are large vessels suspended from the ceiling of the FCC: this allows their contents to be weighed for NMAC. All tanks and pipework are constructed from Nitric Acid Grade stainless steel, which is impervious to the corrosive effects of the liquor.

Incident: the 2005 Leak

On the 20th April 2005, the THORP operators discovered a leak in the FCC. The source of the leak was a pipe that supplied liquor to one of the HEATs. A total of 83,000 litres of highly radioactive dissolver product liquor containing 22,000 kilograms of nuclear fuel (and 160 kilograms of plutonium) leaked onto the floor of the cell. The leak started before August 2004 and remained undetected until April 2005. The source of the leak was a sheared pipe above one of the HEATs. This was likely due to agitation of the tanks during operation.

Why wasn't the leak detected sooner?

Two means of leak detection were in operation in the FCC. The first was a mechanical fluid depth-measuring device called a pneumercator installed in the sump, a trench in the floor of the FCC. A leak from any tanks or pipework in the FCC would lead to a change in the depth of fluid in the sump: this would be measured by the pneumercator and would, under certain circumstances, lead to the initiation of an alarm in the THORP control room. Secondly, although not required under UK regulation, the FCC's Standard Operating Procedures (SOPs) required routine sampling from the sump at three-month intervals (additional sampling was also required in response to pneumercator alarms). Samples of liquid from the sump were analysed and tested for uranium content: any uranium appearing in a sample would be a strong indication that a leak had occurred somewhere in the FCC.

However, both means of leak detection failed. In the end, erroneous NMAC information caused concern amongst THORP personnel who placed cameras in the FCC. The leak was visually identified along with its cause, a broken pipe above a HEAT. The crucial information that led to the visual inspection was collected as part of THORP's NMAC procedures, not as a result of installed safety equipment or safety procedures. What went wrong?

The pneumercator

Following the discovery of the leak, a mechanic was dispatched to investigate why the pneumercator did not record an increase in the depth of fluid in the sump despite a leak of 83,000 litres of liquor into the FCC. Subsequent investigation showed that the pneumercator was not working and, furthermore, had been producing erratic and unreliable output for at least five years (to January 2000). This problem was not confined to any single worker or team, but was a systemic issue affecting the maintenance staff as a whole.

Further investigation revealed that maintenance requests (and other similar activities) were delivered verbally between maintenance staff rather than using standardised paperwork and involving more senior managers, as was required under SOPs. This lack of adherence to procedure was a major factor in the failure to identify the leak. Historical instrument trend data was also not interrogated despite its ready availability: both maintenance and operational personnel therefore failed to exercise appropriate vigilance when carrying out

their duties. Finally, maintenance staff and plant operators did not engage in effective cooperation or teamwork during equipment testing, leaving several safety-critical systems effectively out of order.

A partial explanation of this issue is that maintaining and calibrating the pneumercator and the fiducial level of fluid in the sump was known to be a difficult task. This affected staff motivation in dealing with the problem over an extended period of time. Further, the equipment was allowed to operate in 'low alarm' mode, whereby there was insufficient fluid in the sump for the pneumercator to produce reliable output. Managers generally accorded less importance to indications of 'low alarms' compared with 'high alarms' (which suggested a leak had occurred) and, as a result, pneumercator maintenance was not accorded appropriate priority. Management behaviour thus affected the expectations and motivation of staff in relation to the importance of maintaining safety-critical equipment.

In its investigation into the leak, the UK's Health and Safety Executive found that "there was no assurance that the instrument would do what was intended to fulfill its safety function, i.e. detect leaks from primary containment to the sump" as a result of this situation.

The sump samples

THORP's SOPs required sump samples to be taken both when pneumercators registered an increase in fluid level and on a routine three-monthly basis. The detection of uranium in any sample would be cause for concern as this would indicate that a leak had occurred in the FCC.

There were two crucial problems with sump sampling arrangements. Firstly, samples testing positive for uranium were ignored despite the potentially serious safety situation they suggested. Three such positive samples were recorded in the year leading up to the discovery of the leak but no remedial actions were taken. This indicates a lack of adherence to procedures at the THORP facility. Secondly, despite regular requests from staff responsible for analysis, Head End Plant operators often did not provide sump samples. Managers accorded limited priority to sump sampling, indicating a lack of personal accountability and effective management oversight. The incident investigators found evidence that this had been an issue since 1995 and was again related to the difficulty in taking samples. For one sump, no samples were successfully taken from mid-November 2003 until mid-August 2004, from mid-August 2004 until April 2005 in direct contravention of SOPs. (Only a single sample had been successfully taken during 2004.)

According to the investigating team, a "lack of management oversight and consequent lack of proper ongoing proactive monitoring and audit" of sump sampling "was one of the principal reasons why this event proceeded for as long as it did."

Consequences

As a result of the leak and the investigation into safety failings at the facility, THORP's operators were charged under the UK's Nuclear Installations Act (1965) with three offenses:

1. A failure to ensure all safety-critical operations related to the FCC sump were carried out in accordance with SOPs;
2. A failure to ensure that appropriate safety mechanisms and equipment (namely, pneumercators) were in good working order;
3. A failure to ensure that leaks of radioactive material could be detected in a timely manner.

The regulatory body ordered production at the facility halted until a long list of requirements arising from the investigation were met: this took the plant operator three years to achieve, with significant economic and reputational impacts. The operator was also fined £500,000 in a bruising public trial. The leak was a public relations disaster. The incident was classified as Level 3 on the International Atomic Energy Agency (IAEA) International Nuclear Event Scale (INES), which invited public comparison with Three Mile Island and the Chernobyl

disaster. Finally, the THORP workforce were placed under intense scrutiny and the entire senior operational team was removed. This left many plant operational staff without clear direction or leadership following the incident, adding further stress to an already demoralised workforce. Senior Sellafield managers were personally financially penalised for failings at the facility, and Government Ministers were reportedly "furious" about the leak, which dented public confidence in the nuclear industry.

Relevance to Nuclear Security Culture

Weaknesses in safety culture were a major contributory factor in the failure to identify the THORP leak in a timely manner. The official investigation into the incident found that THORP had "a culture that seemed to allow instruments to operate in alarm mode rather than questioning the alarm and rectifying the relevant fault [and] alarm response instructions were not being followed, leading to the conclusion that the culture also condones non-compliance with" SOPs. Furthermore, the fact that THORP had been deliberately operated without adherence to SOPs for so long raised "concerns about control and supervision as well as the effectiveness of the safety management system and safety culture existing in the plant at the time of the leak."

Personnel at THORP regularly failed to adhere to procedure. According to the report, "the culture within the plant...condoned the ignoring of alarms, the non-compliance with some key operating instructions, and safety related equipment [was] not kept in effective working order for some time, so this became the norm." Personnel failed to demonstrate appropriate vigilance: there was "an absence of a questioning attitude...even when the evidence from the [available data] was indicating something untoward" had occurred at THORP. Managers failed to effectively communicate the importance of safety procedures to staff, indicating a lack of management oversight and a failure to lead by example.

Ultimately, personnel, managers, and leaders all failed to believe that a leak was a credible possibility at THORP. This shortcoming in fundamental attitudes concerning nuclear safety stemmed from the belief that THORP was a "new" facility and was therefore immune to accidents (at the time of the leak, the plant had been operating for over twenty years). Managers also failed to learn the lessons from earlier incidents – two months before the leak was identified, three personnel were contaminated during routine maintenance. The workers checked their clothing on three separate radiation monitors, preferring to believe that the monitors were broken rather than that they were contaminated. This event suggested that safety failures at THORP could occur, but managers failed to appreciate the seriousness of the situation and effected no remedial actions.

The importance of adherence to SOPs, appropriate vigilance, a questioning attitude, effective management and leadership (through leading by example, learning from past mistakes, and communicating effectively with personnel), and the belief that a credible threat exists are all critical for nuclear safety. All of these factors are also crucial for nuclear security: they play a key role in the IAEA's model of nuclear security culture. Although the THORP incident is a nuclear safety case there is clear read across to nuclear security.

Suggested Discussion Points:

- What does this case show us about the importance of adherence to procedure at nuclear facilities?
- What can we learn from the THORP leak about the role of managers in setting expectations and motivating personnel?
- What are the differences and similarities between safety and security culture?

Key Sources for Nuclear Case Studies

Case Study 1

- U.S. Department of Energy, "Special Report Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex", DOE/IG-0868, https://energy.gov/sites/prod/files/IG-0868_0.pdf (August 2012)
- Eric Schlosser, "Break-in at Y-12", The New Yorker http://www.newyorker.com/magazine/2015/03/09/break-in-at-y-12 (9th March 2015)
- Frank Munger's "Atomic City" Blog, http://knoxblogs.com/atomiccity (accessed June 2017)

Case Study 2

- "Sleeping on the Job", CBS News Segment, https://www.youtube.com/watch?v=x2o0Wh8dVZY&t=105s (January 2008)
- Steven Mufson, "Video of Sleeping Guards Shakes Nuclear Industry", Washington Post, , http://www.washingtonpost.com/wp-dyn/content/article/2008/01/03/AR2008010304442.html (4th January 2008)
- Congressional testimony hosted at this link: "B&W Defend Peach Bottom Nuclear Power Plant Whistleblower", http://bernabeipllc.com/2008/03/bw-defend-peach-bottom-nuclear-power-plant-whistleblower/(21st March 2008)

Case Study 3

- Peter Burt, Case Study 6 in "Playing with fire: nuclear weapons incidents and accidents in the United Kingdom," Nuclear Information Service, https://www.nuclearinfo.org/article/nis-reports/playing-fire-nuclear-weapons-incidents-and-accidents-united-kingdom (2017)
- Prime Ministerial Office Files, "Policing of demonstrations at military bases: activities by anti-nuclear demonstrators," UK National Archives, http://discovery.nationalarchives.gov.uk/details/r/C16328924 (2016)
- Brian Jamieson, "Scotland and the Trident System, 1979-1999," University of Glasgow PhD thesis, http://theses.gla.ac.uk/6551/1/2004JamisonPhd.pdf (2004)

Case Study 4

- United Kingdom Health and Safety Executive, "Report of the investigation into the leak of dissolver product liquor at the Thermal Oxide Reprocessing Plant (THORP), Sellafield, notified to HSE", http://www.onr.org.uk/periodic-safety-review/thorpreport.pdf (20th April 2005).
- Keith Hemming, "The human elements of a nuclear incident," Hazards, https://www.icheme.org/~/media/Documents/Subject%20Groups/Safety_Loss_Prevention/Hazards%20Archive/XXI/XXI-Paper-075.pdf (2009) Sellafield, "In focus: The Thermal Oxide Reprocessing Plant," Sellafield Magazine, Issue 6, https://www.gov.uk/government/publications/sellafield-magazine-issue-6 (2017)

Non-Nuclear Case Studies

The four case studies presented in this section are drawn from the diamond, jewellery and entertainment industries, and the prison sector. They are all based around serious incidences where weaknesses in security culture were only identified after the event. For each case study its relevance to nuclear security culture is discussed.

Case Study 5: Antwerp Diamond Heist, Belgium

Background and Perpetrator Profile

Leonardo Notarbartolo, a formidable Italian career thief with an extensive criminal record, carried out with a number of associates a major diamond heist in 2003 in Antwerp, Belgium. He had started his criminal career from a young age with petty thefts, short prison sentences allowing him to generate wide ranging criminal contacts and helping him develop his illicit skills. Driven by ambition, Notarbartolo would eventually specialise in highly complex jewellery thefts, which employed subterfuge rather than violence. Jewellers would find that their stock had been stolen without any alarms being triggered and that multiple layers of physical security had been bypassed. He became a member of the 'School of Turin', due to the city's benign environment to low level criminality due to the police prioritising mafia related violent crime. While no such formal organisation existed, the loosely affiliated group of jewellery thieves operating out of Turin shared their expertise, intelligence and frequently worked with one another. The information that Notarbartolo received that inspired him to rob the Antwerp Diamond Center came from one such colleague. Ferdinando Finotto had been in Antwerp's diamond district plotting thefts when an abortive robbery forced him to flee the country. However, while in Antwerp, Ferdinando had discovered that an office could be rented in the Antwerp Diamond Center without a background check. Ferdinando informed Notarbartolo about this oversight and encouraged him to conduct his own reconnaissance.

In autumn 2000, Notarbartolo moved to Antwerp and rented a small flat near the diamond district. He was subsequently able to secure an office in the Antwerp Diamond Center with the on the pretext that he ran a small jewellery business. If the Diamond Center had performed even a cursory check to gauge Notarbartolo's trustworthiness or the licencing of his business, it would have immediately triggered warnings of his ill intent.

Facility and Security Systems

Even with considerable access and inside information, the Antwerp Diamond Center was by no means easy to rob. The Diamond Center was located within Antwerp's diamond district, which itself was heavily protected. Armed police were always present and located within minutes of the facility. Access to the main street level entry to the facility was also guarded by a set of retractable bollards which were manned by police and would hold a suspect car in check while it was examined. Once at the front door, entrance to the building was controlled by a computerised access card system that logged incoming and outgoing visitors. A network of CCTV cameras and two guards on day shifts monitored movement within the building. The facility also housed two concierges who alternately lived within the building 24/7, to provide both additional security and to facilitate out-of-hours access.

To access the vault, a customer would have to pass the ground level reception and then descend two flights of stairs to enter the vault atrium. During the day, the main vault door would be open but a barred 'day' door would be closed. Known clients would present themselves to a nearby CCTV camera before the door was unlocked by reception. At nights and over the weekends, the vault door was closed and the alarms activated. The vault door itself was 30cm of steel and secured by a custom 100 million combination key lock. The key consisted of two parts – a 1-foot long arm and separate teeth component. For additional security, these parts were intended to be kept separately and only assembled when needed. The vault door also had an electromagnetic system that would detect if the door had been opened out of hours. The signal created by separating the magnets was sent to a remote monitoring station and if the opening was unauthorised, the authorities would be called to investigate.

To prevent attempts at bypassing the vault door, there was a seismic sensor, which made undetected tunneling into the vault a near impossibility. Inside the vault, additional sensors included a dual infra-red and microwave radar motion sensor. There was also a light sensor, so even if the vault door was opened, thieves would have to operate in darkness. All the alarms were silent, so if triggered, potential thieves would only know of their failure when armed police descended on the building. Even if the alarms were successfully bypassed, the Diamond Centre's client's valuables in the vault were contained within individual safety deposit boxes. Each of these boxes had a combined lock and combination dial mechanism and would have to be broken into one at a time. This was potentially a time-consuming task and would have to be done without triggering any of the alarms.

If an assessment was made purely based on the array of physical security systems in place at the Antwerp Diamond Center, it may have appeared impregnable. Counterintuitively, this may have weakened security at the centre, as this case study will show staff became complacent due to their reliance on their sophisticated physical security systems. Most notably they failed to be vigilant of Notarbartolo's suspicious behaviour and routinely compromised the facility by failing to adhere to set procedures.

Incident Description

After Notarbartolo had secured an office within the Antwerp Diamond Centre, he was free to conduct a meticulous reconnaissance of the premises over the course of two years. Notarbartolo made extensive notes on the security features, how staff implemented them and made sure that no upgrades went unnoticed. Notarbartolo also brought in a concealed camera contained within his bag to record footage to help plan the heist: the models of the security systems present were researched and the means to defeat them was acquired. Notarbartolo was also able to secure a copy of the building's blueprints simply by asking the building manager to provide additional information on security, suggesting he was thinking of renting more offices.

The provision of this information was not the only lapse in security culture. Perhaps the most fatal security flaw present was that there was a side-garage meant for employees, whose entrance was outside of the secure diamond district. This meant that after Notarbartolo and his associates had cloned the wireless fob used for opening its gate, they had a discrete means to approach the vault entry room. Furthermore, Notarbartolo became aware that the security cameras inside the building were only monitored during the day and their tapes were stored on site. If the heist took place and night and the tapes were stolen, these cameras would be rendered useless. During his time observing staff procedures, Notarbartolo realised that staff kept the custom two-part key fully assembled in a utility room adjacent to the vault entry room. Notarbartolo was also aware that at night, the two live in concierges, who were meant to provide additional security, rarely ventured from their apartments on the higher levels. Here it is clear that staff members were not adhering to a number of essential security procedures and management had not implemented either sufficient training to stress the importance of their staff's responsibilities or any quality assurance mechanisms.

Notarbartolo's reconnaissance also revealed complacency by the building's management with regards to new physical security systems. Rather than install the electromagnetic sensor on the inside of the vault door where it would be tamper proof, it was installed on the outside for presumably cost saving reasons. The motion-detector also had no anti masking feature so if it could be blinded without initially being activated. Additionally, the individual safety deposit boxes had a plastic rather than metal front plate, making them easier to penetrate. The building's management's knowledge of these subtle security weaknesses was potentially the reason why they refused to allow for an insurance evaluation inspection of their premises. Whatever the motivation, no inspection occurred, so no upgrade requirements for insurance coverage were ever issued. For the diamond business, insurance organisations effectively act as a prescriptive regulator and in this case, they were ignored. In addition, the building's owner was largely absent, so decisions on the building's security were left to the

building's manager, who as discussed above prioritised commercial interests above security responsibilities. In summary there was no effective leadership commitment to security.

With an awareness of these faults, sufficient intelligence and now adequately prepared, Notarbartolo decided upon the weekend of 15th-16th February 2003 as the ideal time to raid the vault. This date was chosen as activity in the diamond district would be at a minimum due to it being the Valentine's Day weekend. The heist was set in motion on 10th February. One of Notarbartolo's associates, D'Onorio, entered the building using Notarbartolo's access card. D'Onorio hid in Notarbartolo's office during the day and managed to swipe his borrowed card to leave the building in the evening without being challenged by a guard, before retreating back to Notarbartolo's office. After waiting for nightfall, D'Onorio descended to the vault level. With the help of a custom tool, D'Onorio disarmed the electromagnetic vault door alarm, painstakingly removed the bolts that connected it to the door and then stuck it back in place. While it would superficially appear that nothing had changed, his work meant that the electromagnetic alarm could be rapidly disarmed by allowing it to be moved out of the way. D'Onorio then exited the facility through the garage door without being noticed. During the week, Notarbartolo also disarmed another layer of security. When inside of the vault during one of his trips to his safety deposit box, Notarbartolo sprayed the motion detector with a layer of hairspray to effectively blind them. He was confident that he would not be observed as guards never entered the vault with clients and there were no CCTV cameras inside the vault either.

On the night of 15th, Notarbartolo, Finotto and D'Onorio entered the diamond centre through the garage door using a cloned electronic fob. They quickly reached the vault foyer, removed the tampered electromagnetic alarm and retrieved the complete two-part key from the adjacent utility room, before proceeding to open the vault door. How they bypassed the vault combination mechanism is unknown – two commonly offered explanations are that they were either able to film the code being inputted with a hidden camera, or the concierge who last closed the vault never cleared the combination. To avoid triggering the light sensor, the thieves used night vision goggles when entering the vault. They broke down the day gate with a crowbar and placed tape over the light senor. The thieves then placed a premade Styrofoam shield in front of the already masked motion detector to ensure it was inoperable.

From then on, the thieves could freely operate within the vault. Using a custom-made drill tool, the gang proceeded to break into individual safety deposit boxes. While a few boxes with metal faceplates proved impregnable, the vast majority were plastic and their contents were sorted and then packed into bags. It was only when the gang had as much jewellery, diamonds, and currency as they could carry (an estimated worth of between 100-400 million USD) that they started leaving. The limitations on what they could carry out of the vault meant they discarded 'semi' precious stones such as rubies and emeralds. On their way out, the gang removed the CCTV tapes of the previous several weeks and then left via the staff garage door before being picked up by a waiting driver. At no time did the thieves encounter any guards – the live in concierge who was meant to be in the building during the robbery had in fact been out drinking with his brother-in-law. While the concierge returned at 2 AM, he didn't notice anything untoward on his way back to his apartment. The theft was only noticed when he went into the vault atrium on Monday morning to open it for business.

Ultimately, Notarbartolo would not get away with the heist. While the thieves had meticulously planned the break in, they abandoned incriminating evidence on private property. While they had intended to burn their rubbish in a secluded wooded area, the gang were spooked by the approach of an unknown individual and left hurriedly before they had completed this task. By chance, the person who nearly encountered the thieves was the land's owner, who reported this fly-tipping to the police. When the police inspected the refuse, receipts within the rubbish connected Notarbartolo to the theft. From there, the investigation rapidly collected additional evidence against Notarbartolo, for example, a raid on his apartment found loose diamonds from the centre were scattered on his floor. Notarbartolo was sentenced to 10 years and his associates 5 years each. Despite none of the stolen valuables ever being recovered, these were the maximum sentences for non-violent theft allowed under Belgian law. Notarbartolo was sentenced to 10 years as he was successfully prosecuted as the heist's instigator.

Relevance to Nuclear Security Culture

There are a number of parallels between the 2003 Antwerp Diamond Center heist and potential threats to nuclear facilities. At both diamond centres and at nuclear facilities, material is held onsite within secure conditions to mitigate the risk of its diversion. However, as observed within this case, reliance on even seemingly impressive physical security measures is not sufficient to ensure reliable security. The actions of Notarbartolo and his associates demonstrates how a skilled adversary, with careful planning can overcome multiple physical protection systems if security culture within a facility is weak. In this case there were cultural weaknesses at multiple levels which he exploited. At the management level, poor security planning led to the installation of obsolete systems for which relatively straightforward countermeasures existed. At the personnel level, there was poor adherence to security procedures and a lack of vigilance. The combination of these weaknesses was first observed and then exploited by Notarbartolo, if a strong security culture had been in place the robbery may have been impossible and Notarbartolo may well have been deterred from initiating such an attempt in the first place.

Suggested Discussion Points:

Although the Diamond Center may have only employed a few security relevant people in comparison to a nuclear facility, this case raises several relevant discussion points to security culture at nuclear facilities.

- Can an overabundance of technologically advanced security systems encourage complacency? What can be done to overcome this?
- What measures can be introduced to prevent an insider from collecting information that could facilitate an external attack?
- Does the two and a half years Notarbartolo spent observing the centre suggest that potential adversaries to nuclear facilities could be equally well prepared?
- What was the interplay between weaknesses in physical security and security culture?

Case Study 6: Cyber Hack of Sony Pictures

Background and Perpetrator Profile

On 24th November 2014, the operations of Sony Pictures Entertainment were brought to a halt by a massive cyber-attack, which crippled the company's IT infrastructure. In the following weeks, the perpetrators divulged online more than 200 gigabytes of documents they had stolen from Sony Pictures' computer systems, including sensitive personal data of thousands of employees, private emails from Sony Pictures executives, and then-unreleased films. Speculations on the perpetrators' identity quickly focused on the Democratic People's Republic of Korea (DPRK), which had previously threatened Sony Pictures Entertainment in order to stop the release of "The Interview", a comedy movie featuring the assassination of DPRK supreme leader Kim Jong Un. In an unprecedented move, the US Government took a stance on the matter, officially accusing the DPRK of the attack. Most cybersecurity experts seem to agree with this analysis, and a following investigation by a consortium of top cybersecurity firms found that the software used in hacking Sony Pictures was also connected to previous cyber-attacks attributed to the DPRK, that had targeted South Korean banks and media companies.

It is unclear exactly how and when the perpetrators, who acted under the moniker 'Guardians of Peace', gained access to Sony Pictures' computer systems, but most experts have indicated that they might have worked for months within the network, slowly exfiltrating internal documents, before executing the final stage of their plan. When this happened, more than 3000 personal computers and 800 servers - roughly half of Sony Pictures' global IT network – had their entire content, including the operating systems and startup code, wiped out in a way that made data recovery difficult or impossible. Coverage of the Sony Pictures hack largely focused on the business consequences faced by Sony and on technical analyses of the hackers' methodologies and Sony Pictures' cyber defences. However, the inadequate cyber security practices within Sony Pictures, especially when it came to the protection of sensitive information, and the poor understanding of security risks by Sony Pictures executives, also provide interesting insights on the importance of security culture.

Cybersecurity Practices at Sony Pictures

Despite Sony Pictures' claims to the contrary, most experts agree that the 2014 attack, while unprecedented in terms of the amount of documents that was stolen, was not particularly sophisticated, and that its success was largely due to the fact that Sony Pictures' cybersecurity practices were insufficient. Notably, several of the issues that made Sony so vulnerable can be attributed to failures of human behaviour.

Once the attackers managed to penetrate within Sony Pictures' corporate IT networks, they easily gained access to sensitive documents and information, due to very weak standards of access control. The company did not use multi-factor authentication, meaning that a username and password were enough to obtain access to email accounts and document folders. This potential vulnerability was greatly amplified by the fact that password practices in the company were extremely poor, as many users used insecure passwords such as "Password1", "abc1234" and similarly common combinations that hackers can easily crack. In a 2007 interview, Sony Pictures' chief cybersecurity officer Jason Spaltro had mentioned poor password practices as a key example of poor security behavior, but one that he thought was not worth the effort of improving.

Another crucial failure in this case was a lack of vigilance. This was well documented in a security audit that global consulting firm PricewaterhouseCooper carried out for the company. The audit's final report, dated September 2014, was one of the many internal documents leaked by the attackers. Auditors found that Sony Pictures' IT network was not properly monitored for signs of intrusions or attacks, with different sections of the network assigned to different internal groups and serious inconsistencies in the level of rigour applied to monitoring different devices. The report concludes that "Security incidents (...) may not be detected or resolved timely"; after the attack, several industry experts commented that Sony Pictures' information security team should have been able to detect the stolen documents being copied and transferred to servers outside the corporate network, which would have allowed the company to respond to the cyber attack and mitigate damage. The gaps in Sony Pictures' security found by the auditors were largely due to a lack of oversight on the company's security. Most notably entire sectors of the network had gone unmonitored for a year, since Sony Pictures had stopped using third-party services as coverage in September 2013, and no process was in place to make sure that all security-relevant hardware was being monitored. Speaking after the incident, former Sony Pictures employees said that the company repeatedly failed to address security vulnerabilities and violations that were brought up by staff members, and that while it regularly carried out risk assessments, the resulting recommendations were not acted upon. To quote a former employee "there was no real investment in or real understanding of what information security is".

Handling of Sensitive Information

One of the attack's most serious consequences was the large amount of sensitive information leaked online. In addition to information on Sony Pictures' business endeavours, the leaked files contained personal information on thousands of current and former employees, including names, addresses and dates of birth, salary information, tax records, social security numbers, background check results, and information on health insurance and health savings. The affected individuals suffered a severe violation of their privacy and were exposed to the risk of identity theft, while Sony itself risked severe damage to its business and reputation. This was, in large part, made possible because of inadequate protection of sensitive information by the company and by its employees.

At the organisational level, it is important to note that no systematic effort was made by Sony Pictures to identify sensitive information handled by its employees and stored in its IT systems, and to provide adequate protection. No additional layers of defence or dedicated secure storage were used for sensitive data, and individual folder and files were not password-protected or encrypted. Had these measures been taken, the hackers would not have been able to see the contents of the stolen files without spending significant time and resources in trying to crack each document's protection. Experts noted that even the standard document encryption offered by Microsoft software could have greatly mitigated the damage. When documents were password-protected, the passwords were often stored unencrypted in a text file in the same folder as the documents themselves. Similarly, passwords providing access to corporate accounts and computers in the corporate network, as well as external web-based services and corporate social media profiles, were stored in unencrypted form, and many were kept in a dedicated folder called "Passwords".

Individual employees also showed a very poor understanding of how to handle and protect sensitive information. Many employees used their email accounts as a repository of important documents such as business records and contracts, without realising that if their emails were hacked, these documents would be stolen. Furthermore, employees used their corporate emails to discuss matters that should have carried out offline. The leaks exposed credit card login information that had been carelessly copied into an email's text, contacts with doctors to procure mental health medication, fertility treatments and gossip on co-workers and business partners. Top Sony Pictures executives engaged in this, too, and remarks they made about Hollywood insiders, movie stars and even then-U.S. President Barack Obama were widely reported by the press, damaging the company's reputation.

Attitude Towards Risk by Sony Pictures' Executives

The lack of security awareness at Sony Pictures is very apparent when looking at the behaviour and statements of its top executives. In June 2014, when the movie The Interview was first announced, the DPRK had claimed that releasing the movie would constitute "an act of terrorism and war", and had threatened "a merciless counter-measure" against both the U.S. and Sony Pictures. Sony Pictures' parent company, Sony Entertainment, also urged caution as the history of tensions between Japan and the DPRK was keenly felt in the Tokyo headquarters. While the DPRK is known for its harsh and often overblown rhetoric, it has also displayed real capabilities in the realm of cyber attacks in the past, including against media companies that criticised it in South Korea. Despite this, the possibility of a cyber attack against the company did not seem to be taken seriously, and no precautionary measures were taken to improve the defences and resilience of its IT systems.

Sony Pictures' CEO Michael Lynton claimed that experts hired by the company to conduct a risk assessment did not highlight cyber attacks as a possible threat. However, at least two experts who later spoke with the media claim that they had warned Sony Pictures against this possibility. Leaked emails show that in the months preceding the movie's release, The Interview was the subject of heated discussions, but these always framed the issue in terms of potential controversy and public relations, with a lot of time devoted to debating whether to tone down the scene depicting Kim Jong Un's extremely graphic and grotesque on-screen death. The company's studio executive never really seemed to consider that there might be a real threat to the security of the company.

Even Sony Pictures' top cybersecurity officer seemingly shared this scarce awareness of potential threats. In a 2007 interview, Sony's Senior Vice President for Information Security Jason Spaltro acknowledged that he knew of widespread poor cybersecurity practices, like the use of weak passwords, but that he chose to overlook some of those and only focus on the ones "absolutely required by law". He claimed it was "a valid business decision to accept the risk" of being hacked, and added that he would not "invest $10 million to avoid a possible $1 million loss". When he talked about the hypotetical $10 million upgrade compared to a $1 million projected loss, Spaltro mentioned as an example the systems that Sony uses to track credit card payments across the world, including those used for its online videogames platform PlayStation Network. In 2011, PlayStation Network was hacked, and personal information and credit card numbers for 77 million users were leaked. The incident cost Sony Pictures' parent company Sony Entertainment upwards of $170 million. As a consequence, Sony Entertainment announced a plan to drastically improve its cybersecurity capabilities, spearheaded by a new Senior Vice President and Chief Information Security Office, Philip R. Reitinger, who had previously served in top cybersecurity positions at Microsoft and at the U.S. Department of Homeland Security. Despite this strong change of direction in the parent company, practices at Sony Pictures apparently remained unchanged, and Spaltro was still in charge of Sony Pictures' information security in 2014.

Consequences of the Attack

The consequences for Sony Pictures were far-reaching: the company suffered severe internal disruption due to the loss of records and infrastructure, which lasted into the beginning of 2015. In addition, as mentioned above, thousands of Sony employees and former employees had sensitive personal data published online. After initial complaints, Sony Pictures provided identity theft insurance and protection services to its employees and ex-employees, and also faced class action lawsuits for failing to protect sensitive personal data. Five Sony Picture films, four of which had not been released yet, were leaked on the internet, and distribution plans for The Interview suffered: a large-scale opening on Christmas day, involving major theatre chains across the United States, was cancelled after the threat of further attacks. The film eventually received an online streaming release, followed by a limited release in theatres, significantly damaging the movie's box office intake. By the end of March 2015, the company estimated that the total cost of the incident so far had been roughly $41 million, with the bill likely to increase because of further work on establishing a more secure IT network, the aforementioned lawsuits, and damage to the company's reputation.

In the early months of 2015, Sony announced a new IT infrastructure plan, to rebuild its capabilities after the catastrophic damage caused by the attack and protect itself from future danger. This includes new hardware and infrastructure, but also new and very stringent procedures for access and storage of information that all staff members are expected to follow. While improving the company's procedures is certainly a step in the right direction, it is unknown whether Sony Pictures also provided security awareness training to its employees in order to ensure that procedures are respected.

It is more difficult to gauge whether the behaviour of individuals has changed as a consequence of the incident. Given the glaring security problems that have been discovered, there are many lessons that Sony Pictures should be keen to learn for its future. However, several employees complained that in the weeks following the attack, the company's chief executives seemed to focus more on avoiding legal responsibilities for the company than in being frank and transparent about the situation. Sony Pictures' stance on the incident, refuted almost unanimously by top cybersecurity experts, was that the attack was unprecedented in skill and power, and that there was nothing the company could have done to stop it. Further interviews with Sony Pictures staff, held a year after the attack, show a mixed picture. Some employees stated that they and their colleagues are now more careful about the content of their digital communications, and that many discussions have been taken offline. However, other staff members and business partners claim that they still received emails with sensitive or personal contents from corporate email addresses. CEO Michael Lynton said "people are still sending me emails that they would very much not like to see show up in another venue".

Relevance to Nuclear Security Culture

While this case focuses on the theft of information, rather than material, it still presents a score of valid lessons on the importance of a strong security culture. The key failures that allowed the attackers to inflict so much damage were rooted in human behaviour, and many of these highlight aspects of poor security practices that are also relevant for nuclear facilities.

At outlined in NSS 7, the core belief underlying a strong security culture is an understanding that threats are real, and security is important. While managers and company leaders should provide an example to their employees, and respond to their security concerns, Sony Pictures' top managers ignored the potential of a cyber attack against the company, even after receiving threats. It is also important that companies put in place measures to continuously review and improve their security arrangements, and that managers' support these measures. Employees must be empowered to report on security concerns, and these reports must be followed up. Instead, potential vulnerabilities highlighted both by formal review processes and by concerned employees had not been addressed and the poor oversight Sony Pictures exerted over its IT systems further degraded the company's security. Instead of practicing good security behaviour and encouraging it in others, Sony Pictures displayed a great degree of acceptance of poor security practices and poor vigilance, which further degraded the effectiveness of the company's defences. Finally, if Sony Pictures had understood the need to classify and protect information according to its sensitiveness, a great deal of damage to the company and its employees could have been avoided.

Suggested Discussion Points

- What do you think of the attitude of Sony Pictures' chief cybersecurity officer? Can we assume that members of the security team will automatically have a good security culture?
- Why do you think that no measures were taken to improve Sony Pictures' cyber defences after the threats by DPRK? What are the limits of focusing on "business as usual"?
- Obviously, companies need to focus on their bottom line, and there are trade-offs to be made between security and production, what are the limits to these trade-offs? Did Sony Pictures compromise too much?
- Is all the information you handle daily classified and protected appropriately? Is there sensitive information you work with that may not be recognised as such and exposed to danger?

Case Study 7: Hatton Garden Jewellery Raid, United Kingdom

Background and Perpetrator Profile

Over Easter weekend 2015, a group of thieves broke into the vault at Hatton Garden Safe Deposit Ltd. in an area of London known for dealers in jewellery and precious stones. The thieves stole millions of pounds' worth of expensive items and cash. They broke into the building twice. Their first attempt, on the night of 2nd-3rd April, was unsuccessful due to an equipment failure. But their second attempt on the night of 4th-5th April was a success. The exact value of the stolen goods and cash remains unknown, but the current estimate is approximately £30 million.

There has been considerable public interest in this case (a movie was released in April 2017), stemming in part due to the advanced ages of the burglars, who were mostly in their 60s and 70s. The mystery and intrigue are further heightened by the fact that one of the members "Basil" has apparently not yet been apprehended by the police. Furthermore, only a fraction of the stolen goods and cash have been recovered. It is possible that Basil absconded with the bulk of the spoils, or that it has been hidden in the countryside outside London, or that it was shipped out of the UK within days or weeks of the raid.

Due to the technical difficulty and scale of the burglary, a sizeable team of experienced criminals was assembled to carry it out. Brian Reader, "The Master," or "The Governor," reportedly the leader of the ground, was 76 at the time of the burglary. His criminal career began early in life, as he was arrested at the age of 11 for breaking and entering. Later, he was allegedly part of the "Millionaire Moles" gang that tunnelled underground to rob safe deposit boxes in a Lloyds bank vault in Baker Street, London in 1971. In 1983, he was connected to the robbery of the highly-secure "Brinks Mat" warehouse at Heathrow airport, in which £26 million worth of gold bullion was stolen and for which he was incarcerated for eight years.

John "Kenny" Collins, 74, was the lookout and driver. His list of previous convictions goes back to the 1950s and 1960s and he had already been in jail multiple times, including for armed robbery. Collins was involved in planning the Hatton Garden raid and visited the area numerous times prior to the break-in. Daniel Jones, 60, the youngest of the core group, participated in planning and vault access. Referred to as a "fitness fanatic," he runs marathons when he is not in jail. Like the others, Jones had several previous convictions and had been to prison more than once. Previous offences included a burglary in 1982. He and "Basil" were the thinnest and fittest of the group, and thus were assigned the activities where that was an advantage, most importantly crawling into the vault, breaking open the security deposit boxes, and handing out the contents. Terence Perkins, 67, participated in planning and carrying out the raid, including drilling the holes in the vault wall and receiving the stolen goods handed out from the vault. Prior to this break-in, he had already been convicted of armed robbery in 1985 and sentenced to 22 years in prison. Basil, age and real name unknown, is still at large. He had "insider" access, including keys to the front door of the building and possibly one or more of the codes needed to open interior doors. Exactly what inside information he received and how he received it is not publicly known. He was responsible for disabling alarms and CCTV cameras and for joining Jones on the more athletic parts of the heist, including crawling through the hole into the vault, breaking into the security deposit boxes, and handing the contents out. At least one source maintains that Basil rather than Reader was the mastermind behind the burglary.

Carl Wood, 58, was not involved in planning the burglary. He was present at both break-ins but decided not to enter the building on the second night. Like the others, he already had a list of previous convictions. He was a friend of Jones, who recruited him "as someone who

would be a useful additional pair of hands." William "Billy the Fish" Lincoln, 59, had a family connection with Collins, who recruited Lincoln to assist with selling the stolen goods. He was not involved in planning the heist, nor was he present at the break-ins. He had also served time in jail in the past. Hugh Doyle, 48, was a long-time friend of Collins and others in the group. Doyle was not involved in planning or carrying out the robbery, but played an ancillary role in providing a place where stolen property could be transferred. The fact that this "safe" place was covered by CCTV gave police the final proof they needed to arrest the gang. Doyle had previously spent some time in prison on a drugs charge.

Facility and Security Systems

The vault at Hatton Garden Safe Deposit, Ltd. (HGSD) contained 996 safe deposit boxes that were mainly used by local dealers to store valuables such as jewellery, precious stones, gold, and cash. When jewellers would close up shop at the end of the work day or before the weekend, for example, they would bring their most valuable items to HGSD and deposit them in their boxes in the belief that they would be safer there than in their shops.

To access the vault normally, one would enter the front doors of 88-90 Hatton Garden. During the work day, these doors were open; for other times, all tenants had their own keys. The next step was to pass through a glass door immediately behind the front door. This door was left open during business hours and could be opened at other times using a four-digit code that all the tenants knew. Behind the glass doors was an unstaffed lobby with a lift. The lift could not be used to access the vault level, following a modification in the 1970s. Instead the basement could be accessed via stairs controlled by a door, this should have been locked outside of business hours but apparently was always open.

At the bottom of the stairs, was a second wooden door, which was also left unlocked during business hours. At other times, only the security guards or the manager could open it. Immediately behind the wooden door was an iron gate that could be opened using a four-digit code. Once past the wooden door and iron gate, you were in the "air lock" and had 60 seconds to deactivate the intruder alarm using a five-digit code; this alarm was connected to a monitoring company. During business hours, the "air lock" was monitored by a security guard who would then let you through the second iron gate. At this point, an adversary would be standing in front of the vault door. This was two feet wide, "bomb- and burglar-proof," and could only be opened with the relevant combinations. The walls, which were 0.5 metres thick, were made of reinforced concrete. Inside the vault, the safe deposit boxes were mounted in steel cabinets that were bolted to the floor and ceiling. There were also apparently motion sensors inside the vault. The building had a CCTV system, linked to a data storage system in a basement office. In addition, HGSD had its own CCTV system connected to a hard drive in an office in the airlock area.

In addition, the basement could also be accessed via a fire exit door, which opened on a courtyard leading via a set of stairs to an adjacent street. Very few people had the keys to this door, but it could of course be opened by anyone from the inside. Apparently, it was not connected to a fire alarm. Also, inside the air lock were locked, unalarmed shutters, behind which were the old, now unused, lift doors, these were used to access the shaft to conduct maintenance work.

Incident Summary

Given the aforementioned security measures that would need to be bypassed, the group spent significant time planning their raid. Reader supposedly began planning in 2012 and in the months leading up to April 2015, the group met many times at a pub in north London to make their plans over a beer. In preparation, Basil collected considerable "insider information" and access that apparently involved not only keys to the front doors of the building and the codes for internal doors, but also detailed knowledge of the building's interior layout, the alarm systems and motion sensors, and the locations of surveillance cameras and the hard drives to which they were connected. Preparation also included multiple scouting trips by Collins and a visit on 31st March to HGSD itself by Terry Perkins, who posed as a workman and was seen in the lift, surrounded by tools. Collins also managed to acquire a key to 25 Hatton Garden, the building across the street.

At 6pm on Thursday 2nd April, the HGSD security guard set the alarm and locked up as usual, heading home for the long holiday weekend. Neither he nor any other HGSD personnel anticipated returning to the premises until the following Tuesday. By the time Collins and others from the group pulled up in a white van at 8.20pm, Reader had also arrived via public transport. All the robbers were dressed as gas company workmen. At 9:21pm, Lionel Wiffen, a jeweller who was working late in his office in the building that housed HGSD, left the premises via the fire escape door; this was normal practice as his back office was accessible via the building's courtyard. Basil, who had apparently already entered the HGSD building from the street using a key, had hid inside the building, waiting for Wiffen to depart. Now that he was gone, at 9:22pm, Basil opened the fire escape door to allow the rest of the group inside the building. Collins drove the van up and they unloaded tools and wheelie bins, taking them inside. At this point the group inside the HGSD building comprised Reader, Jones, Perkins, Wood, and Basil. As he moved through the building, Basil disabled alarm systems, motion sensors inside the vault, and the CCTV camera systems. The latter included removing the relevant storage devices from the control equipment, however, he missed (or could not disable) two cameras. Collins parked the van around the corner again and then at 9:30pm, using a key, he entered 25 Hatton Garden—which stands diagonally opposite the HGSD building—to take up his watch post.

Inside the HGSD building, the burglars called the lift to the second floor. They disabled the lift door sensors so that the doors wouldn't close, thereby keeping the lift at the second floor. Returning down the stairs to the ground level, they hung an "out of order" sign on the lift, then forced the lift doors open. Basil and Jones climbed into the shaft and dropped down to the basement level. The rest of the gang waited for them by the wooden door at the bottom of the stairs in the basement. Once Basil and Jones were at the bottom of the lift shaft, they forced open the old lift doors, broke the lock on the shutters, lifted them up, and found themselves inside the "air lock." They cut a telephone line and snapped off the aerial on the intruder alarm, attempting to disable it. They then cut the power to the first iron gate in the "air lock," enabling them to slide it across and access the wooden door. This they forced open, finding the rest of the group waiting for them. With the entire group now in the air lock, they cut through the second iron gate and finally stood in front of the vault door.

Meanwhile, just after midnight on the 3rd April, the intruder alarm, despite being damaged, managed to send an SMS to its control centre. The monitoring company called the building manager, telling him that there was an intruder alarm and that the police had been notified and were responding. The building manager called the HGSD security guard and they both headed for the building. The guard arrived first, about an hour after the SMS was sent. He look through the mail slot into the courtyard, checked the front doors of the building, and, seeing nothing amiss, called to tell the manager to turn around and head back home as it was a false alarm. Despite what the monitoring company told the building manager, the police did not respond to the alarm. Subsequent investigations revealed that the alarm message had been incorrectly "graded," i.e. given a low priority indicating that no response was necessary.

Back at the HGSD vault, the burglars were busy setting up their key piece of equipment, a Hilti DD 350 diamond-tipped coring drill. They used it to bore three large overlapping holes through the concrete next to the vault door. This created an opening, 45 cm wide by 25 cm high, that went clear through the concrete, leaving the robbers looking at the solid

steel rear wall of the cabinet in which the safe deposit boxes were housed. This is where the thieves' luck ran out: their 10-ton hydraulic ram failed to force the cabinet away from the wall, apparently because of a faulty pump. They had no choice but to leave the way they came, departing at just before 8am on Friday the 3rd. They left the fire exit door propped open.

After catching up on sleep on Friday, most of the group broke the cardinal rule of thieving – agreeing to return to the scene of the crime on Saturday night. Brian Reader, however, bowed out, believing the risk of capture if they returned was too great. Undaunted, Jones and Collins procured a replacement pump for the hydraulic ram, assembled the team and returned to Hatton Garden. When they arrived, they discovered that someone had closed the fire exit door. This was Mr. Wiffen, who had been surprised to find the door ajar when he arrived to clean his office on Saturday evening. So Basil went in through the front door as on the first night, but while the group waited for him at the fire exit, Carl Wood lost his nerve and decided to leave. Basil appeared, letting in Jones and Perkins, and Collins resumed his watch. This time, the hydraulic ram worked, forcing the steel cabinet inside the vault away from the vault wall. Basil and Jones, both being relatively slim, crawled through the hole and went to work on the safe deposit boxes. They forced the boxes open, handing the contents out to Perkins, who was waiting on the other side of the access hole. Of the nearly 1,000 safe boxes, they opened "only" 73; 40 of which contained valuables. They appeared to have advance knowledge of the general area of the vault that contained the boxes holding the most valuable items. This was taken up the fire escape stairs and out to a waiting van. The burglary was not discovered until the Tuesday after the long Easter weekend when the security staff arrived as usual for work.

During and after the raid, the burglars made a number of mistakes that eventually enabled the police to identify them as the perpetrators. The most important of these was probably their use of Collins' personal automobile on the second night. It was a distinctive white Mercedes, and once the police identified it using CCTV footage and linked it to Collins, they began to piece together the evidence to build a very strong case against the group. Approximately six weeks after the heist, the police raided 12 locations around London simultaneously, arresting all of the individuals listed above except Basil. Reader, Collins, Jones, and Perkins were presented with such overwhelming evidence against them that they all decided to plead guilty; they later received relatively lenient sentences of seven years in prison. Lincoln, Wood and Doyle pled "not guilty." Lincoln was given seven years, Wood was given six, and Doyle was released with a suspended sentence based on time he spent in jail awaiting trial. During the trial, the value of the stolen goods was estimated at £14 million. However, subsequent claims by HGSD tenants has since raised this figure to £29 million. Only £4 million pounds' worth of items has been recovered, leaving the whereabouts of not only Basil but also £25 million pounds' worth of stolen property a mystery.

Relevance to Nuclear Security Culture

Even though this case does not involve a nuclear facility, the IAEA's NSS 7 can be helpful in elucidating a number of the weaknesses in security culture that enabled the thieves to steal so many valuables from the HGSD vault. It is clear that the police response to the alarm message sent out by the damaged alarm system at HGSD was insufficient. The alarm received was not given the proper priority in their system, with the result that no police arrived on the scene on the first night. There are also a number of weaknesses in the security culture at HGSD that can be identified. Arguably the most important is the apparent lack of resources committed to security. Outside of business hours, there was neither on-site security nor live monitoring of the CCTV system by an outside organisation. It is remarkable that a burglary of this scale in central London could go unnoticed for such an extended period of time. The failure of the HGSD manager to embody, set and maintain strong security practices was also a problem. Weaknesses included allowing multiple people to have keys to the front door of the building and the combination to the ground-level glass door. A lack of enforcement when it came to the policy of locking the door at the top of the stairs on the ground level outside of business hours. The security guard's response to the intruder alarm

was also inappropriate, he should have entered the premises.

It is clear that there was a relatively "relaxed" approach to security at the site. The commitment of both the manager and the guard to security was arguably weak. Professionalism and competence with regard to the facility's physical layout, characteristics, and equipment, as well as policies in place, was also lacking. Information security was also apparently problematic, as someone shared critical "insider knowledge" with Basil, while storing the CCTV data on site was also inappropriate. There were also weaknesses in the operations and maintenance of security equipment. For example, the air lock could be relatively easily accessed via the locked but not alarmed shutters between the room and the old lift doors. Contingency plans and drills had apparently not been thought through, if merely ensuring that the front doors were locked and looking through the mail slot into the courtyard constituted a good response to an intruder alarm. Security could also clearly have been improved if someone off site was monitoring the CCTV cameras. There were also weaknesses in terms of professional conduct and personal accountability, by other non-security people working in the building. Mostly notably by the jeweller Lionel Wiffen, who found the fire exit door propped open twice during the weekend—once after each visit by the burglars—and did not immediately report this to HGSD management, security, or the police.

Suggested Discussion Points

- What were the most important failures of the security system and HGSD management and staff?
- How might HGSD management and staff and/or the police have acted differently to hinder the burglary? Both prior to and during the event?

Case Study 8: Mecklenburg Prison Break, United States

Background and Perpetrator's Profiles

The two leading instigators of the 1984 Mecklenburg prison break were brothers – James and Linwood Briley. Although growing up in a stable family environment, the two brothers had a long history of violent crimes. Linwood committed his first murder at the age of 16 in 1971 when he shot and killed an elderly neighbour. He only received a year-long sentence due to being convicted of manslaughter as a legal minor. James would receive his first criminal conviction shortly after when he became involved in a gun fight with police officers. James and Linwood would continue to pass in and out of prison for a range of violent criminal offences. The Briley brothers would reach the peak of their notoriety in 1979 when they perpetrated a vicious serious of killings, rapes and robberies in Richmond, Virginia. Their spree, which involved the assistance of their third brother, Anthony Briley and another conspirator, Duncan Meekins, resulted in the deaths of 11 people. They were eventually caught as police officers heard gunshots when the brothers were committing their final murders. Duncan Meekins agreed to testify against the Briley brothers and as a result, Linwood and James were successfully convicted for their murders and received the death sentence.

As the chance for the Briley brothers having their death sentences commuted was minimal, escape was always on their mind. This task was complicated by the two brothers being moved to Mecklenburg in 1980, Virginia's premier high security prison. Nevertheless, the Briley brothers quickly gained notoriety for their extreme violence, being key actors in the prison's drug trade and controlling their fellow inmates. James' first abortive escape attempt occurred in October 1981 and although unsuccessful, the brothers continued to search for a new method to break out of prison. By October 1983, the Briley brothers were holding wider discussions with other inmates about escape plans. Rapid progress was made as the Briley brothers were under pressure to act because Linwood's appeal process was coming to an end. The prisoners collectively decided upon their final approach in March 1984. In their plan to escape, the brothers were joined by four fellow murderers: Earl Clanton, Derick Peterson, Willie Jones and Lem Tuggle. More prisoners were involved in the plot but some did not participate in the final escape as they thought it wouldn't succeed – among these was Dennis Stockton, who actively warned the prison authorities that an escape attempt was imminent. The Briley brother's need to escape was pressing as Linwood had received the date for his execution by early May 1984.

Facility and Security Systems

Mecklenburg Prison was constructed incrementally between 1974 and 1982 at the cost of $20 million, and had been designed with maximum security in mind to house the very worst offenders. The site contained five prison block buildings and was surrounded by a double barbed wire fence which was lined by watch towers that housed armed guards. There was only one external exit gate from the site, which was an 'air-lock' double gate, so passing vehicles would be checked before entering or exiting. Prison block building one housed the prisoners on death row, including the Briley brothers. Each prison building could only be accessed through another 'air-lock' gate system, where the inner and outer gates had to be opened separately from a secure booth. Building one's ground floor was occupied with workrooms, while prisoners were kept on the upper floors in three separate 'pods'. Death row inmates were held in 'C' pod, which contained 24 cells with single occupancy. The pod was separated in half by a dividing wall, with each half having its own entrance gate. In each half of the pod, there were six cells on the upper row and six on the lower row. Each pod

had a single central control room, where prison staff could electronically open both entrance gates to the pod as well as lock individual cell doors. To prevent prisoners from breaking into the control room during a riot, the only access point was behind the entrance gates to the pod and the door itself was meant to be kept locked.

During the day, prisoners on death row could congregate in the central area between their cells and the dividing wall, called the 'day room'. In the 'day room', prisoners were constantly overseen by a guard in the room itself. All staff in the prison building were meant to be armed with stun guns. In the event of a riot, the contingency procedure was that staff in the inaccessible control room would be able to radio for reinforcements. Even if the inmates could escape their pod, prisoners would be unlikely to open the prison block building's doors or then escape the perimeter without alerting the authorities. While some prisoners had suggested trying to break out just with holding hostages and force alone, this had quickly been dismissed as unfeasible.

While the physical security systems seemed daunting, the prisoners observed two potential weaknesses. One physical security weakness that the prisoners routinely exploited were the blind spots from the central control room. Prison guards were unable to observe the bottom half of the six cells on the lower row in each half of the pod. This meant that these cells proved ideal for storing contraband and weapons. A further flaw was the number of potential hiding spots immediately before entering the pod, including a staff toilet opposite the control room access door, which was routinely left unlocked. During the day, prisoners worked in the classrooms on the lower floor. Upon returning to their pod, a prisoner had the opportunity to leave their group and hide. If the guards didn't notice his absence, he would be beyond the pod entry gates and only have a single locked door separating him from the control room.

Perhaps more detrimental to security was the low morale among staff. Considering the constant risk of assault and abuse faced by the guards, they received minimal pay. A full-time guard received just $13,000 per year, which compared unfavourably with all other police work in America at the time. This left staff susceptible to bribes as they could more than double their income by participating in the prison's drug trade. As a result, the drug trade within the prison flourished – one of the Briley brothers was found to have 63 marijuana cigarettes in his cell in 1983. In May 1984, one Mecklenburg guard was arrested for supplying drugs to death row inmates.

One unforeseen consequence of the use of the keyless entry system was that it changed the relationship between inmate and guard. Guards became passive observers from their control rooms rather than having to actively engage with inmates to open their cells. This factor has been credited with why Mecklenburg had an abnormally high rate of assaults compared to other high security prisons. These attacks could prove deadly as prisoners fashioned knives from scrap metal that was smuggled from the workshops on the lower floor. This further degraded security as even incorruptible guards faced constant intimidation. Staff often valued their personal safety above their responsibilities. These two factors help explain why sweeps conducted on 19th April and 17th May failed to recover any contraband, despite its abundance within death row.

These problems were further compounded by a lack of training among staff and a reliance on overtime to cover for staff shortages. As was later revealed in reports commissioned after the escape attempt, the prison's management had been maintaining staff at insufficient levels. In combination with the poor working conditions and insufficient pay, staff turnover was high and the levels of training among incoming guards was often insufficient. To maintain acceptable coverage, staff members were pressed into taking excessive overtime. This vicious cycle's effects were manifested in staff failing to properly conform to proscribed procedure.

These shortcomings proved disastrous as the Briley brother's and their associates were constantly observing the guards and learning how weaknesses could be exploited. While not a traditional 'insider threat' as their authorised access was strictly limited and their relationship with the prison was always openly adversarial, their intimacy with the facility and proximity to the staff had many of the same characteristics. The Briley brothers built

up a sufficient pool of knowledge on the layout of the facility, learned of opportunities for gaining access to areas of the prison and how the hierarchy of authority among prison staff could be exploited in the event of an escape. Key faults that were noted included how that staff did not carry their stun guns while on duty, instead opting for nightsticks – this left them more susceptible to being overpowered. Whether staff did this of their own volition, were never issued or were never trained to use them has not been satisfactorily explained. Secondly and entirely against procedure, staff would sometimes temporarily leave the locked control room if a prisoner asked for an item to be passed from one half of the pod to another. Additionally, the prisoners had noted that staff were not identifying themselves over the radio when communicating amongst each other. Therefore, if the prisoners could gain access to the control room, they could potentially impersonate guards.

As later audits would reveal, attempts at rectifying or highlighting these problems to decision makers were severely undermined by weak 'institutional security management and practices'. In what would now be termed weak security culture, several key elements were missing. Due to being understaffed and overworked, the supervisory role of senior guard employees was neglected. In 1984, Mecklenburg had the worst guard to officer ratio at any Virginian prison. In combination with their responsibilities for overseeing large numbers of inmates, these senior officers had little time to check that their staff were performing their roles as per protocol. Even then, these issues might have been addressed had there been an effective regulatory body that could provide external oversight. However, the Virginian Department of Correction's recently established Regional Offices proved insufficient – they were unsure of their institutional role and their inspections were improvised and failed to collect any usable data. Due to a lack of quality assurance and despite valuing security, Virginian legislators were unaware of the potential problems at Mecklenburg. Instead, they placed their faith in the modernity of the facility to prevent escapes.

Incident Description

With a date set for Linwood's execution, the Briley brothers had to act swiftly. They had spent the last four years observing the behaviour of their guards, storing sufficient contraband and gathering a cohort of fellow prisoners willing to participate in the escape attempt. By the end of May 1984, their plan was ready. While relatively simple and requiring a significant amount of luck, it proved highly successful. The first stage of the plan was the most well formulated as it required the escapees taking over the entirety of 'C' pod without the guards calling for reinforcements. On the morning of 31st May, the six prisoners set to escape cut their hair and shaved off their beards. This collective and unusual change of appearance went unnoticed. When the prisoners returned to C pod from outside recreation in the evening, Earl Clanton ducked out of the group and hid inside the unlocked staff bathroom opposite the entrance to the control room. The remaining prisoners were moved back into the day room and the gates closed, at this point, Earl Clanton's absence wasn't noticed as the guards had failed to conduct a head count.

One hour after returning to the day room, James Briley asked the guard in the control room if he could pass a book from one half of the pod to the other. Against protocol, the guard left the control room. With the door open and unlocked, Earl Clanton ran into the control room from the bathroom and opened all the doors in C pod. With the help of fellow prisoners and crude knives, the guards in the pod were overpowered and tied up. Their uniforms were taken and the escapees put them on. The escapees subsequently captured the other guards in prison block one by one using the control room radio to lure them into C block to help deal with a supposedly injured prisoner. Through this method, the prisoners captured Larry Hawkins, the senior officer on duty. He was forced to call the guard on the perimeter fence gate to get a van ready and through the double gates to help deal with an unspecified emergency. A further call was put through to the guard in charge of the booth in control of the 'air lock' exit doors of prison block one. She was told that she was being relieved by a fellow guard coming from inside the building. While this was against protocol, she opened the door and was overpowered by Derick Peterson. After being forced to open both sets of doors, the prisoners had access to the prison yard. Before leaving, the prisoners donned riot

gear and made Hawkins make a final call explaining that there was a bomb in building one and that it had to be evacuated immediately. To further this ruse, a 'bomb' was created by placing a television covered with a sheet on a stretcher and having it periodically sprayed with a fire extinguisher.

With their appearances masked by the riot gear and with their 'bomb', the prisoners rushed through the yard to the now waiting van at the perimeter fence. Overcome by this apparent crisis, the officer in charge of the gate opened both sections of the gate at once to allow them to leave as quickly as possible without any inspection. The guard who had brought the still running van to the fence ran away immediately, not wanting to be caught in a sudden detonation. After all the escapees boarded the van, the 'Mecklenburg Six' sped through the open double gate and out of the prison and across the state border into North Carolina.

While the prisoners had carefully orchestrated their escape to get out of the prison, the next part of their plan was not so well considered. While the escapees had a vague idea to cross into Canada, they split up and were progressively tracked down and arrested by the authorities. Peterson and Clanton were caught the day after the escape as a call to Peterson's mother was traced to their location. Tuggle was apprehended next after a woman he robbed reported the licence plate number of the car he was using to the police. Jones, who had been travelling with Tuggle, turned himself in shortly after Tuggle's arrest. The Briley brothers were caught 19 days after the escape, working in their uncle's garage. The FBI had discerned their location after being informed by Tuggle that the pair had been dropped off in Philadelphia and then placing the Briley's uncle under surveillance.

While all the prisoners were recaptured, the incident created a political scandal in Virginia. There had been fears that the Briley brothers would resume their murderous rampage. Due to the escape, the director of the Virginian department of corrections resigned, the chief warden of the prison and the ranking security officer were moved to other positions and two guards were fired. Mecklenburg received urgent technical upgrades such as the installation of security cameras, more walls, mirrors to eliminate blind spots and extra locking doors. Death row was made more secure by confining prisoners to their cells for a greater proportion of the day. In addition, more guards were hired and more training was provided. Their pay was progressively increased to place it in line with other policing work. Consultants were brought in to assess the failings of Mecklenburg and a new post of inspector general was created to ensure effective continuous assessment of prisons in the state of Virginia. Despite these reforms, Mecklenburg was eventually downgraded to a medium security prison in 1995 and Virginia's death row was moved to another facility in 1998. Unable to repeat their feat, all the 'Mecklenburg Six' were executed between 1984 and 1996.

Relevance to Nuclear Security Culture

While there is the obvious dissimilarity between a prison keeping people in and a nuclear facility wanting to keep intruders out, the 1984 Mecklenburg prison escape highlights relevant lessons for both when the IAEA's model for security culture is applied. When this case is examined, the ability of the 'Mecklenburg Six' to escape was the result of a series of human errors in failing to conform to procedure. As observed, the low standards for compliance in the prison can be partly attributed to poor pay among guards, which can also be a problem at nuclear facilities. Overworked and often inexperienced staff on low wages and in a hostile work environment left them unmotivated and susceptible to corruption. As adherence to procedures and robust professional conduct are central aspects of the correct staff behaviour for maintaining a strong security culture, it is evident that there was a problem.

However, as the audits that would be conducted after the escape would reveal, the key institutional failing at Mecklenburg was the inability of any party to effectively communicate potential security lapses, such as those resulting from poor staff morale and practices, to decision makers. While the IAEA stresses the necessity for effective communication to be facilitated by leaders, in this case, both the regulator and officers at the prison failed to do so. The personnel issues led prison officers to abandon their supervisory roles to engage

in normal operations to the detriment of conducting quality assurance. Thus, faults in the staff's adherence to procedures went routinely unaddressed and unnoticed. In addition, the Virginian Department of Corrections regional offices were failing to provide meaningful oversight despite their role as a de facto regulator. Thus, systemic problems with security culture went unaddressed as no effective quality assurance or performance measurement was taking place. Comforted by the modernity of the prison and therefore a lack of a belief in a credible threat, decision makers were therefore unaware of the potential problems at Mecklenburg. When confronted by an adversary that had observed numerous lapses in protocol and knew that guards would be unready to adapt to an unexpected scenario, the Mecklenburg staff were overwhelmed with embarrassing results.

Suggested Discussion Points:

While the aims of security at prisons and nuclear sites invariably differ, this case raises several discussion points on the role of nuclear security culture:

- How can security staff be equipped to deal with an unexpected scenario?
- How can decision makers ensure that sufficient quality assurance and performance measurement is taking place?
- Does this case reveal the potential problems of neglecting staff morale? How can economic considerations and minimising the threat of corruption be balanced?
- How can overconfidence in physical security systems be avoided?

Key Sources for Non-Nuclear Case Studies

Case Study 5

- Davis, Joshua, "The Untold Story Of The World'S Biggest Diamond Heist". WIRED. https://www.wired.com/2009/03/ff-diamonds-2/ (2009)
- Dell'Arti, Giorgio, "Biografia Di Leonardo Notarbartolo". Cinquantamila.Corriere.It. http://cinquantamila.corriere.it/storyTellerThread.php?threadId=NOTARBARTOLO+Leonardo (2014)
- Even-Zohar, Chaim, "Gangster Viciously Implicates Antwerp Diamond Dealers". Idexonline.Com. http://www.idexonline.com/Memo?id=32091 (2009)
- Lafleur, Jarret M., Liston K. Purvis, and Alex W. Roesler, "The Perfect Heist: Recipes From Around The World", http://prod.sandia.gov/techlib/access-control.cgi/2014/141790.pdf (2015)
- Selby, Scott Andrew, and Greg Campbell, Flawless: Inside The Largest Diamond Heist In History. 1st ed. New York: Sterling (2012)

Case Study 6

- Elkind, Peter, "Inside the Hack of the Century", Fortune, http://fortune.com/sony-hack-part-1/ (2015)
- Schneier, Bruce, "Lessons from the Sony Hack", Schneier on Security, https://www.schneier.com/blog/archives/2014/12/lessons_from_th_4.html (2014)
- Franceschi-Bicchierai, Lorenzo, "Sony Pictures leak shows employees used worst passwords ever", MashableUK, http://mashable.com/2014/12/02/sony-hack-passwords/#jkr2Q6l3I5qo (2014)
- Chmielewski, Dawn, and Hesseldahl, Arik, "Sony Pictures Knew of Gaps in Computer Network Before Hack Attack", Recode, https://www.recode.net/2014/12/12/11633774/sony-pictures-knew-of-gaps-in-computer-network-before-hack-attack (2014)
- Hill, Kashmir, "Sony Pictures Hack was a long time coming, say former employees". Fusion, http://fusion.net/sony-pictures-hack-was-a-long-time-coming-say-former-e-1793844351 (2014)
- Barrett, Brian, "The Sony Hacks are Goddamn Terrifying". Gizmodo. http://gizmodo.com/the-sony-hacks-are-goddamn-terrifying-1668911102 (2014)

Case Study 7

- F. Hamilton, "Hatton Raiders Forgot to Shut the Fire Door," The Times, (2nd December 2015)
- 3D simulation of raid, Sky News, https://www.youtube.com/watch?v=AD1Gta-J-mM&list=PLG8IrydigQfcxV9FjXInKa0Liomsq3Epq (13th January 2016)
- "One Last Job: The Unlikely Story Behind the Hatton Garden Heist," Sky documentary, https://www.youtube.com/watch?v=rIqZCNzt00A (14th January 2016)
- "Who are the Hatton Garden Heist Gang? Meet The Master, Billy the Fish and Basil," Express, http://www.express.co.uk/news/uk/634714/Hatton-Garden-heist-gang (14th January 2016)
- "Bad Dads Army: The Hatton Garden Heist," BBC documentary, https://www.youtube.com/watch?v=ipH15WOhP7U (15th January 2016)
- Sentencing Remarks of HHJ Kinch, Woolwich Court, https://www.judiciary.gov.uk/judgments/sentencing-remarks-r-v-collins-others-hatton-garden-robbery/ (9th March 2016)
- "Hatton Garden Heist Gang 'Stole Extra 10m of Pearls and Gems", Guardian, https://www.theguardian.com/uk-news/2017/feb/03/hatton-garden-heist-gang-stole-extra-10m-of-pearls-and-gems (3rd February 2017)

Case Study 8

- Daryl Cumber Dance, Long Gone, Knoxville: University of Tennessee Press (1987)
- Joint Legislative Audit and Review Commission, "The Capital Outlay Planning Process and Prison Design In The Department Of Corrections. Richmond", http://jlarc.virginia.gov/pdfs/reports/Rpt87.pdf (1987)
- Joint Legislative Audit and Review Commission, "Security Staffing and Procedures In Virginia's Prisons", Richmond, http://leg2.state.va.us/dls/h&sdocs.nsf/fc86c2b17a1cf388852570f9006f1299/202336ff893e03b785255fda0075061d/$FILE/HD3_1986.pdf (1986)
- Bill McKelway, "Jailbreak: Briley Brothers Busted Out of Death Row". Richmond Times-Dispatch. http://www.richmond.com/news/jailbreak-briley-brothers-busted-out-of-death-row/article_68778648-a61d-500c-9dfc-38cb20878a15.html (2009)
- Tom Sherwood, "Guards Cite Security Lapses", Washington Post. https://www.washingtonpost.com/archive/politics/1984/06/18/guards-cite-security-lapses/20203fc5-e17f-4eff-ae8c-b5350f899aeb/ (1984)

Centre for Science and Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

www.kcl.ac.uk/csss
@KCL_CSSS