CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Insider Threats

An Educational Handbook of Nuclear & Non-Nuclear Case Studies

Christopher Hobbs & Matthew Moran

AUGUST 2015

Introduction

Individuals with malicious intent ('insiders') working within nuclear facilities pose arguably the greatest threat to nuclear materials, systems and information. Insiders can exploit their authorised access to bypass multiple layers of security that external adversaries would have to defeat in order to get close to their target. They can also utilise their authority over people and systems, and knowledge of the facility and security systems to both facilitate and mask their actions. When it comes to the theft of the most sensitive types of nuclear material (highly enriched uranium and plutonium) all known incidences, as reported in the open source, have involved insiders. Exploring the nature of the insider threat and their interaction with different security systems through a series of detailed real-life case studies can inform nuclear security planning. Here the effectiveness of different preventative and protective measures can be evaluated, as can the impact of other influencing factors such as security culture. Case studies can also help bring to life the sometimes heavily technical topic of nuclear security, while at the same time highlighting the seriousness of the threat posed to nuclear security facilities.

The Handbook

This handbook is intended to provide nuclear security educators and trainers with a set of insider threat case studies for use in their classes. Due to the relatively small number of available insider incidences within the nuclear enterprise case studies have also been developed from non-nuclear sectors.[1] For these examples the read across to nuclear security has been discussed and should be emphasized by the instructor. For all the case studies relevant discussion points and a detailed reference list 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 institute, as they demonstrate just one way in which the case studies might be presented. A short section outlining in general terms the utility of case studies for engendering student learning has also been prepared in order to help individuals consider how best to utilise this method alongside other forms of instruction.

Acknowledgements

We are grateful to Geoffrey Chapman from the Centre for Science and Security Studies (CSSS) at King's College London for providing research support and, Luca Lentini and Daniel Salisbury for proofreading. We hope that this will be a useful resource for current and future nuclear security educators.

1 Please note that some of the nuclear case studies have previously been presented in a different format by Dr Christopher Hobbs at multiple insider threat workshops.

Glossary

ANC	African National Congress
AQAP	Al-Qaeda in the Arabian Peninsula
BA	British Airways
CSSS	Centre for Science and Security Studies, King's College London
FBI	Federal Investigation Bureau (U.S.)
FDO	Physical Dynamics Research Laboratory (The Netherlands)
FSU	Former Soviet Union
HEU	Highly Enriched Uranium
IAEA	International Atomic Energy Agency
IRS	Internal Review Service (U.S.)
JMB	Jammat al-Mujahideen Bangladesh
LANL	Los Alamos National Laboratory (U.S.)
NMAC	Nuclear Material Accounting and Control
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (U.S.)
PCS	Process Control System
PF-4	Plutonium Facility 4
SCADA	Supervisory Control and Data Acquisition
UCN	Ultra Centrifuge Nederland
USD	United States Dollars
VMF	United Machine Factory (The Netherlands)

Table of contents

Teaching Case Studies

Theory and Practice

In recent years, the theory and practice of teaching in higher education has undergone a profound transformation. Driven by an increased understanding of student learning processes, universities and other providers of higher education have moved away from the 'Instruction Paradigm', the largely passive format of information provision that has traditionally underpinned educational approaches in higher education. Indeed, it is now widely accepted that this out-dated model 'where faculty talk and most students listen, is contrary to almost every principle of optimal settings for student learning'.[2] Instead, higher education institutions now align their educational provision with what is termed the 'Learning Paradigm'.

> **"THE LEARNING PARADIGM HOLDS THAT RESPONSIBILITY FOR PRODUCING LEARNING IS SHARED BETWEEN THE TEACHER AND STUDENT"**

The Learning Paradigm

First proposed by Robert Barr and John Tagg in 1995, the Learning Paradigm places the student at the centre of the process of learning and teaching.[3] Rather than proposing a fixed structure whereby a programme of lectures or instruction is provided and the student assumes complete responsibility for his/her learning, the Learning Paradigm holds that responsibility for producing learning is shared between the teacher and the student. Crucially, in the Learning Paradigm, 'a college's purpose is not to transfer knowledge but to create environments and experiences that bring students to discover and construct knowledge for themselves'.[4] This approach enables students to develop as critical thinkers with the ability to solve problems and make new discoveries.

The 'Learning Paradigm' calls for a more flexible pedagogical approach that is supported by a range of different methods and approaches, all of which support the ultimate goal of engaging students in active learning. A highly useful approach in this context involves the use of case studies.

Case Studies

Pioneered by the Harvard Business School, case studies have long been recognised as a powerful means of promoting active learning.[5] The approach here is student centric and research has shown that 'the use of case studies ranks as the classroom method considered the most effective for developing critical thinking skills'.[6] There is also evidence to suggest that 'student evaluations improve when the case study method is used instead of the traditional lecture approach'.[7]

2 Alan E. Guskin, 'Reducing Student Costs & Enhancing Student Learning Part II: Restructuring The Role Of Faculty', Change: The Magazine of Higher Learning (1994), Vol.26, No.5, pp.16-25

3 Robert B. Barr and John Tagg, 'From Teaching to Learning: A New Paradigm for Undergraduate Education', Change: The Magazine of Higher Learning (1995), Vol.27, No.6, p.13.

4 Ibid.

5 Roland Christensen, Teaching by the Case Method (Boston, MA: Division of Research, Harvard Business School, 1981).

6 Leonard and Cook, 'Teaching with Cases', p.96.

7 Ibid.

The Nature of Case Studies

Case studies are perhaps best described as stories, presenting 'realistic, complex, and contextually rich situations and often involve a dilemma, conflict, or problem'.[8] They help bring the subject to life for the student as when studying a case study, 'students do not just read and discuss general theories; they study all of the available information from which decisions must be made'.[9] With the students experiencing some of the 'complexities, ambiguities, and uncertainties confronted by the original participants' in the case under study.[10] Case studies can also serve to bridge the gap between theoretical concepts and real world problems. Students are invited to analyse a realistic situation, apply prior knowledge and experiences, and arrive at logical conclusions and choices.[11] Simply put, as a pedagogical tool, case studies help to ground theoretical understanding and critical thinking in practice.

In the literature on the subject, a distinction is usually made between two types of case study:

1. The Narrative Approach

The 'retrospective' or 'narrative' case study presents a 'comprehensive history of a problem – complete with multiple actors, contending interests, and the real outcome'.[12] The goal for students here is to analyse the evolution of events, determine the reasoning behind decision-making and, if possible, suggest alternative solutions.

2. The Decision Forcing Approach

In contrast, a 'decision-forcing' case study presents a certain amount of detail but 'stops short of revealing the outcome, thus forcing students to identify and assess the range of possible options for action'.[13] This type of case study typically includes an 'epilogue', presented to students after their analysis is complete. The epilogue sets out the actual progression of events and these are then compared and analysed against the options suggested by the students.

Case Studies as a Pedagogical Tool

There are a number of concrete benefits associated with case studies as a learning tool. When engaged in the analysis of a case, for example, students develop and refine their critical thinking skills and ability to articulate subtle points of analysis as part of a coherent argument. Given that case study analysis usually occurs in a group setting, students are also afforded the opportunity to enhance their communication, teamwork and interpersonal skills, all skills that are highly valued in the professional environment. In addition, the analysis of case studies is usually conducted within a fixed period of time, forcing students to manage their time and critical resources effectively.

> From the perspective of assessment and feedback, a core element of the learning process, case studies have the benefit of allowing teachers to provide prompt feedback, often on the spot, and clarify any misunderstandings arising from the subject matter. Furthermore, the fact that case studies are usually constructed around real-life problems and situations means that the impact of feedback provided to the students is greatly increased.
>
> Case studies can serve as the basis for a number of teaching and learning formats, including in-class discussion and debate, small group analysis and individual assignments. In this sense, the case study constitutes a highly flexible pedagogical tool that can be adapted to a variety of teaching situations and needs.

8 'Instructional Strategies', Eberly Centre for Teaching Excellence and Educational Innovation, Carnegie Mellon University, https://www.cmu.edu/teaching/designteach/design/instructionalstrategies/casestudies.html.
9 Edwin C. Leonard Jr. and Roy A. Cook, 'Teaching with Cases', Journal of Teaching in Travel & Tourism (2010), Vol.10, No.1, p.96.
10 Vicki Golich, Mark Boyer, Patrice Franko and Steve Lamy, 'The ABCs of Case Teaching', Institute for the Study of Diplomacy, Georgetown University, 2000, p.1.
11 Leonard and Cook, 'Teaching with Cases', p.96.
12 Golich, Boyer, Franko and Lamy, 'The ABCs of Case Teaching', p.1.
13 Ibid.

> **THE CASE STUDY CONSTITUTES A HIGHLY FLEXIBLE PEDAGOGICAL TOOL THAT CAN BE ADAPTED TO A VARIETY OF TEACHING SITUATIONS AND NEEDS**

Of course, while case studies offer a number of pedagogical benefits, this approach also brings some important challenges that must be navigated by teacher and student alike. From the teacher's perspective, case studies require a significant amount of planning and background research. A successful case study is one that is rich in details usually drawn from a range of sources that can take time to gather and collate.

The use of case studies in the classroom also places considerable pressure on the teacher. For while case studies require considerable planning, the outcome of the exercise is not necessarily fixed. When asked to analyse a case study from a particular perspective, the teacher cannot anticipate every possible route the student thought process might take. Consequently, ensuring that the focus of the exercise is constantly in line with broader course learning objectives remains a constant challenge. It is for this reason that the case study approach is often described as the 'art of managing uncertainty', a process where the teacher serves as 'planner, host, moderator, devil's advocate, fellow student, and judge' all at the same time.[14]

From the student's perspective, analysis of a case study usually requires a base level of knowledge that is then applied and tested in new ways. If this base level is absent, perhaps through a lack of engagement with other aspects of a course, the case study approach loses value. Another challenge lies in the attention and focus usually demanded by the case study approach. Comprehensive analysis of a case study requires a good working knowledge of its constituent parts and details. On the whole, however, the benefits of the case study outweigh any challenges or drawbacks. This approach holds enormous potential as a means of promoting active learning and student engagement with key issues.

Case Studies in Nuclear Security

The nuclear security context is well-suited to the case study approach. While security incidents are thankfully relatively rare compared to other industries, there exist a number of real-life cases that highlight different facets of nuclear security, both in terms of the threat and the response. This handbook is focused on the issue of insider threats and the preventative and protective measures that can be taken to mitigate against this risk. Here cases may be presented in a 'retrospective' manner where the specific incident is described in detail before students are asked to critique insider motivations and characteristics and the adequacy of the security measures in place at the specific facility. Alternatively a 'decision forcing' approach might be utilised, here instructors could pause at each stage of the insider interaction with different security measures and pose the question of the probability of insider detection at this stage. This may be an effective way to explore relatively abstract concepts such as security culture and how this can impact on the effectiveness of security systems.

Top Tips for the Preparation and Use of Case Studies:

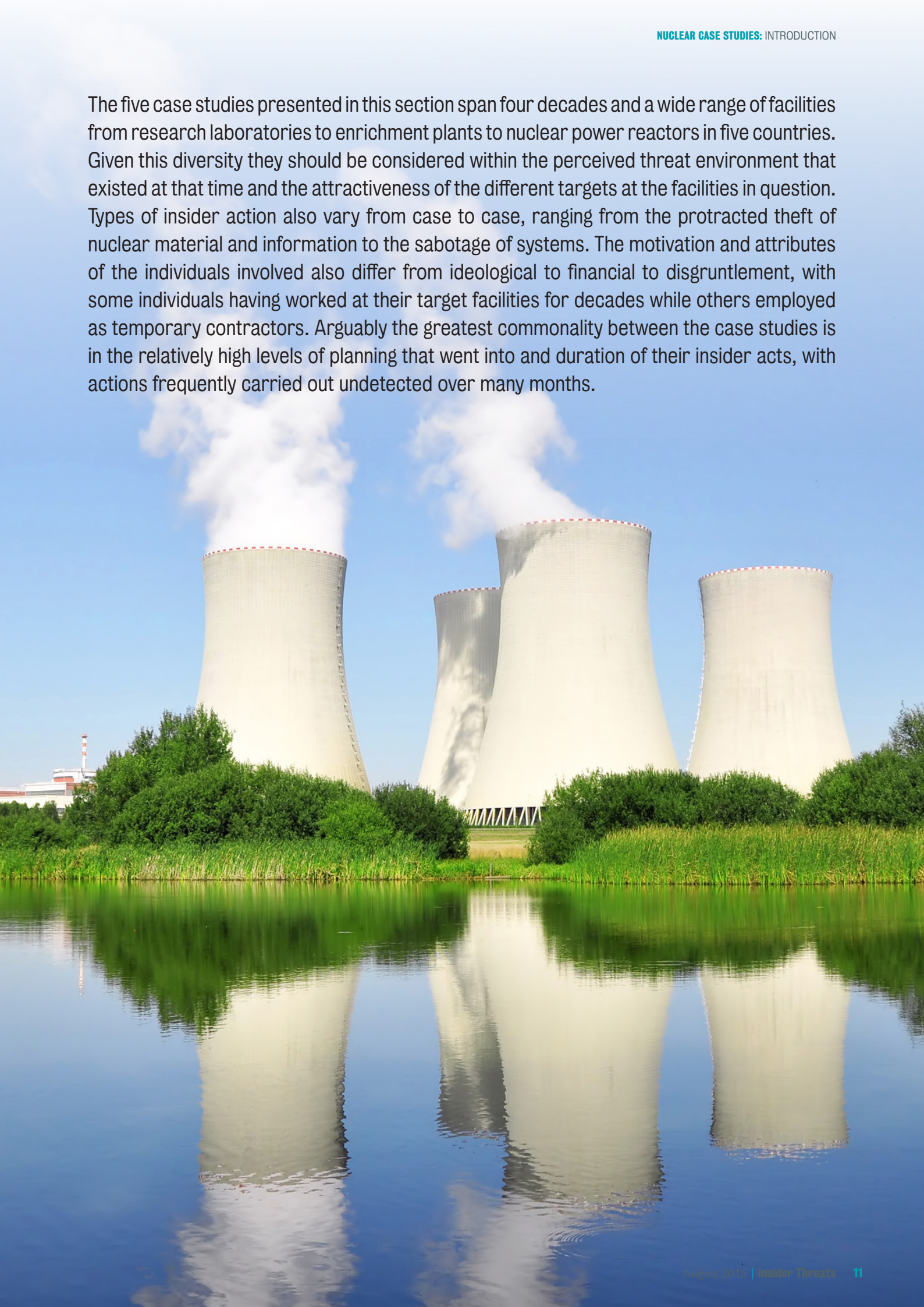
There are a number of guiding principles that can be adopted by teachers to ensure that their use of case studies brings value to the student learning experience:

- Identify learning objectives and clearly set out how the case study in question will help you meet them.
- Formulate a 'discussion path' – what type of broad, guiding questions should you posed to generate the discussion you desire?
- Stress to students the importance of preparation and active engagement with the exercise.
- Present the case study in a structured and accessible format
- Provide the students with adequate source materials to support their discussion and analysis.
- Be prepared to 'steer' the discussion if students lose focus during the exercise.

14 J. K. Satia, Madhavi Misra, Radhika Arora and Sourav Neogi (Eds.), 'Innovations in Maternal Health: Case Studies from India' (Sage Publications, 2014) p. xliii.

Nuclear Case Studies

The five case studies presented in this section span four decades and a wide range of facilities from research laboratories to enrichment plants to nuclear power reactors in five countries. Given this diversity they should be considered within the perceived threat environment that existed at that time and the attractiveness of the different targets at the facilities in question. Types of insider action also vary from case to case, ranging from the protracted theft of nuclear material and information to the sabotage of systems. The motivation and attributes of the individuals involved also differ from ideological to financial to disgruntlement, with some individuals having worked at their target facilities for decades while others employed as temporary contractors. Arguably the greatest commonality between the case studies is in the relatively high levels of planning that went into and duration of their insider acts, with actions frequently carried out undetected over many months.



Case Study 1: Luch Scientific Production Association – Leonid Smirnov

Perpetrator Profile

Leonid Smirnov worked at Luch Scientific Production Association in Podolsk, Russia for over 25 years, having joined in the mid-1970s. Employed as an engineer he was responsible for weighing, account and dispensing highly enriched uranium (HEU), weapons grade – 90% ^{235}U, to different research teams. In 1992 he carried out the protracted theft of 1.5 kg of HEU, over a period of several months, with the intention of selling the material to a buyer in Moscow. While he succeeded in removing the material from his facility without detection he didn't locate a buyer. Smirnov was eventually apprehended at Podolsk railway station with the HEU in his possession, while in the process of transferring it to a baggage locker for storage. He was later found guilty of stealing and storing nuclear material and sentenced to three years probation. The theft was financially motivated, brought about due to the worsening economic situation in Russia following the dissolution of the Soviet Union. Hyperinflation and a reduction in wages for nuclear workers meant that Smirnov was undergoing significant financial struggles. After reading an article in a local paper about the insider theft of 1200 grams of uranium from another facility he decided to do the same. While Smirnov was successful in removing uranium from his facility without detection it is unclear how successful he would have been at selling this material as he simply assumed this would be possible by approaching 'foreign firms in Moscow'. Following his conviction he later became somewhat of a champion of nuclear security, giving a number of interviews about his crime, to raise awareness of the threat posed by insiders.

Facility and Security Systems

Luch Scientific Production Association was a state owned nuclear research and development institute in Poldosk, an industrial town, 40 km South West of Moscow. Scientists and engineers at the institute carried out nuclear related work on experimental reactors utilising HEU fuel. While detailed information is not available on the security measures in place at Luch it is clear that there were minimal systems in place for detecting insiders. It would appear there was no remote surveillance or two person rule within Smirnov's laboratory, where significant quantities of Category I nuclear material was routinely handled. While there was an accounting system in place to track the flow of nuclear material the 'irretrievable loss limit' for the laboratory was high, around 3 percent. Through careful processing it was possible for Smirnov to siphon off 1 percent of the material a month and stay under this limit, meaning his theft did not show up on the material balance books. At the time there were no radiation monitoring or contraband checking at the entry and exist points to the facility. The only radiation detection devices in use were hand held systems that workers could use on themselves to check if they were contaminated.

Incident Summary

In May 1992 Leonid Smirnov started to steal HEU from his laboratory. Waiting until he was alone in the room, he would transfer a small amount of uranium from the storage box into a 50-gram glass vial, which was routinely used for transferring samples. After sealing and wiping the vial with a special chemical solution, he would check it with a Geiger counter for contamination before rolling it up in paper and placing it in his bag. At the end of his shift he would take the bag and walk out of the facility. Once home he would transfer the uranium to a jar on his balcony, before taking the vial back into the facility the next day and disposing of it with other laboratory waste. Smirnov utilised this method an estimated 25-30 times over the next three and a half months, taking one or two vials at a time, with each vial holding up

to 60 grams of HEU. Having accumulated approximately 1.5 kg, 300 grams more than his original target he decided to transfer the jar from his balcony to a baggage locker at a nearby train station, where it could be stored until he found a buyer. He placed the uranium in three metal containers, surrounded by sheets of lead and within a plastic bag, before placing them in a travel case and heading to Poldolsk railway station. There he bumped into three neighbours who were being tailed by the police, having been suspected of stealing batteries from a local factory. Smirnov was arrested with them by mistake and taken to the local police station where they searched his bag and discovered the containers. Faced with the prospect of the police opening the containers and contaminating the interrogation room, he decided to inform them that they contained uranium.

Suggested Discussion Points:

The case study is significant in that it is one of the first officially acknowledged cases of nuclear material theft by the Russian authorities. It offers a number of possibilities for in-class debate. Key questions for discussion with students might include:

- Based on the classification within the IAEA's Nuclear Security Series No. 8 how would you assess Smirnov's level of access, authority and knowledge?
- What were the security weaknesses at the facility? How has the security at Russian nuclear facilities changed over the past two decades?
- What role can nuclear material accounting and control (NMAC) play in detecting insider actions? What were the weaknesses in the NMAC system at the Luch Scientific Production Association?
- Explain why there were a number of nuclear insider incidents in Russia and other Former Soviet Union (FSU) countries in the early to mid 1990s.

Case Study 2: Wilmington Nuclear Plant – David Learned Dale

Perpetrator Profile

David Learned Dale was employed as a temporary contractor at the General Electric nuclear plant in Wilmington, United States where he worked day shifts in the Chem Tech Laboratory. Using his insider access on 26th January 1979 he stole two canisters of low enriched uranium powder, which were later recovered following a failed blackmail attempt. According to behavioural analysis by the authorities, based on the letter Dale wrote to extort money from General Electric, his motivation for stealing the uranium was purely financial. Even though the letter mentioned sending samples of the material to anti-nuclear groups, it does not appear that he was ever a member of such an organisation. His brother claimed at the time that Dale was suffering from depression, as his temporary job at the plant was due to finish in the next few months. He was found guilty of stealing nuclear material and attempting extortion and sentenced to fifteen years in prison.

Facility and Security Systems

At the time the Wilmington Nuclear Plant was a large nuclear site, which produced low enriched uranium fuel rods. It had a site area of approximately 800,000 square feet, employed a staff of approximately 1,600 and operated 24 hours a day. While precise details about the security systems employed at the facility are not readily available, it would appear that a number of measures were employed at the site during the time of the incident. These include access control, with checkpoints employed to ensure that only authorised personnel were onsite. Once past the perimeter personal vehicle access was only permitted to designated parking areas, which were separated from the buildings where nuclear material processing occurred. Within these buildings additional security measures such as locks were in place to limit access to areas that contained nuclear material.

Incident Summary

At 10.50pm on Friday 26th January 1979 Dale drove to the plant, having previous left following the completion of his day shift. In order to gain admittance he used his Florida driving license, which had the same blue background colour of a permanent staff members ID badge. Only permanent staff members had access to the site outside of the regular working day. He was confident this technique would work having used his driving license to gain access to the facility on multiple previous occasions. After gaining access to the facility, rather than follow the fences to the parking area, he took advantage of a gate that had been removed for maintenance to drive and park his car next to the Chem Tech Laboratory. After entering this building using his key card, he gathered the necessary protective clothing, a cart used to transport material and a container for shipping chemicals. He then headed to the radiation-controlled area of the building, passing through a door that although normally locked, was currently ajar due to a malfunction of the locking mechanism. Once inside, Dale accessed the materials store and removed two 5-gallon cans of uranium dioxide, placed them in the shipping container and transported them back to his laboratory. There he removed some of the material and placed it in a vial for use in his subsequent blackmail attempt. He then sealed the cans and utilising the cart wheeled them outside to his car, where he placed them in the trunk. He then followed his entry route back to the main gate where he left the plant just before midnight. If he had left after midnight he would have been required to sign out.

On Monday 29th January the plant manager found, slipped under his office door, a letter and vial containing a sample of the removed uranium. The six-page letter, which had been hand written by Dale, demanded 100,000 USD in exchange for the stolen uranium; to prove the authenticity of his action Dale provided serial numbers for the removed cans. If these demands were not met the letter threatened that similar vials of material would be sent to a mix of anti-nuclear groups, the US Nuclear Regulatory Commission (NRC), a mix of government and non-governmental organisations and major US newspapers. According to Dale this would turn the public against nuclear power and force the NRC to immediately 'shut down your plant'. If the plant contacted the authorities, the contents of one of the cans would be spread through the downtown area of a major city and the price of the remaining can would rise to $200,000. This was ignored by the plant manager who, after checking the cans were indeed missing, contacted the NRC and the US Federal Bureau of Investigation (FBI). The investigation that was subsequently launched compared the handwriting in the letter to employee notes written to management at the plant. The FBI also contacted Murray Miron, a behavioural psychologist, who based on the contents of the letter constructed a behavioural profile of the perpetrator. This profile suggested that the authorities were looking for a 25-30 year old Caucasian male, who still worked at the facility and whose actions were likely solely financially motivated. This combined with other analyses allowed the FBI to quickly narrow the list of suspects down to Dale, whose handwriting was also judged to match that of the letter and he was arrested on Tuesday 1st February. He swiftly admitted his guilt and pointed the authorities to the missing cans, which were just three miles from the plant in a nearby field. In terms of impact it was claimed by papers at the time that the incident cost General Electric $1 million, as the plant was closed for two days in order to search for the missing cans of uranium.

Suggested Discussion Points:

The case study is particularly interesting from the perspective of nuclear security culture, given the number of security systems that were in place at the facility at the time of the incident. Key questions for discussion with students might include:

- What role does nuclear security culture play in strengthening or weakening the effectiveness of security systems at a nuclear facility?
- Discuss how access control if properly enforced can help minimise the risk posed by insiders.
- Following an incident what types of actions can be taken by the operator, regulator and authorities to identify the perpetrator and recover the stolen material or information?

Case Study 3: Koeberg Nuclear Power Plant – Rodney Wilkinson

Perpetrator Profile

Rodney Wilkinson was employed for two periods at Koeberg Nuclear Power Plant in the early 1980s, initially as a labourer before being rehired as a safety officer. A former national fencing champion, Wilkinson was also an anti-apartheid activist, a university dropout and a former military deserter, having served during South Africa's intervention in the Angolan civil war. He claims to have been motivated to act by the arrest of Renfrew Christie, a member of the African National Congress (ANC) who had previously spied on South Africa's nuclear programme. Wilkinson stole site plans from Koeberg towards the end of his first stint of employment, before smuggling them to Zimbabwe and passing them to members of the ANC. He was later convinced by the ANC to use his insider access to Koeberg to sabotage the nuclear facility. Following the successful attack he fled South Africa with his girlfriend, Heather Gray, eventually settling in the United Kingdom. Wilkinson and his girlfriend, who were never tried for their acts, were later granted amnesty by the South African Truth and Reconciliation Commission in 1999.

Facility and Security Systems

The Koeberg Nuclear Power Plant, 20 km outside of Cape Town in South Africa, was under construction at the time of the attack, with nuclear fuel yet to be loaded into the two reactors. Precise details on the security systems in place are not readily available, although from reports it would appear that there were several layers of security. These included a perimeter fence and checkpoint to ensure only authorised personnel were allowed onsite. There was also a second layer of security that employees would have to pass through on foot in order to gain access to the main reactor building. It would appear that there was no vetting or behavioural monitoring of personnel.

Incident Summary

Encouraged by his girlfriend, Heather Gray, Wilkinson stole blueprints for the Koeberg Nuclear Power Plant towards the end of his first period of employment at the facility in the early 1980s. He took these to Zimbabwe and passed them to the ANC, thinking they could be used to plan an attack on the facility. Initially suspicious of the white South African claiming to have sensitive information from what was considered the most secure installation in South Africa, the ANC carefully authenticated the plans and vetted Wilkinson. Realising his access to Koeberg provided an opportunity to strike at the heart of the plant, Sathyandranath 'Mac' Maharajto, the ANC leader in Zimbabwe asked Wilkinson to carry out the sabotage attack. Initially hesitant Wilkinson was convinced and started, under the direction of an ANC handler, to plan an attack that would cause significant damage, while minimising loss of life or any radiological release. In order to achieve this 16th December 1982 was chosen as the attack date, several weeks before nuclear fuel was scheduled to be loaded into the reactors. This date also had broader significance, as the anniversary of both the foundation of Umkhonto weSizwe, the ANC's guerrilla army and the Battle of Blood River in 1838, where the Boers defeated the Zulu's. Interestingly the leadership at Koeberg had pinpointed mid-December as a likely date for an ANC attack on the facility. Paul Semark a senior manager was quoted as saying, 'we knew the ANC would not target Koeberg once nuclear fuel was there... We even pinpointed 16 December 1982, which was a public holiday, as the likely date.' Four targets for detonating explosives were selected within the facility: the two reactor heads; the containment building; and a concentration of electric cables under the control room. To prepare for the attack Wilkinson practiced smuggling bomb sized objects, typically bottles of whisky or vodka, past the security systems at Koeberg. According to

reports he was caught in the act at least once by a security guard, but escaped with only a warning about bringing contraband into the facility. In the lead up to the attack a cable fire at Koeberg led the ANC President Oliver Tambo to mistakenly claim credit for the incident. This was investigated by the authorities before being confirmed as an accident.

With the attack date set Wilkinson and his girlfriend obtained four limpet mines from an ANC arms cache in a remote area of South Africa, hiding them in empty wine boxes in their car and transporting them back home. He then smuggled them individually, within a hidden compartment in his car, onto the nuclear site through the perimeter security fence, placing them in a desk draw in his office. Once there he carried them under his clothes through another security gate and into the main building. In order to place the mines on the reactor heads he had to navigate a 'clean' area, which required him to undress and put on protective clothing. In order to minimise his risk of detection he took advantage of the plastic diaphragms used to keep the air clean, passing the mine through and picking it up on the other side. Although successful in planting the mines Wilkinson did not make the target date and instead set the fuses on Friday 17th December, with a 24-hour delay so the mines would detonate on the weekend when few people would be onsite. The mines exploded the next day over a period of several hours causing massive damage, delaying the commissioning of the plant by eighteen months and causing an estimated 50 million USD of damage.

Suggested Discussion Points:

This case study vividly highlights the threat of insider sabotage at a nuclear facilities and the need to provide rigorous security systems at every stage of a plants construction. Key questions for discussion with students might include:

- How can security systems testing be utilised by insiders to help facilitate a malicious act?
- What role can vetting and continuous behavioural observation plan in help minimising the risk posed by insiders?
- How did weak security culture play a role in facilitating Rodney Wilkinson's actions in the aforementioned case study?
- How can nuclear facilities handle temporarily increased threat levels? In this case around a historically significant date.

Case Study 4: Almelo Enrichment Facility (URENCO) – Abdul Qadeer Khan

Perpetrator Profile

A.Q. Khan was born in Bhopal in 1937 but moved from India to Pakistan in 1952 after witnessing the bloody turmoil resulting from the partition of the two countries. After completing his physics degree in Pakistan, Khan moved to Europe where he studied in Germany before transferring to the Delft University of Technology where he obtained a Ph.D. in engineering in 1972. On the strength of his recommendation from his doctoral supervisor, Khan obtained a job at the FDO (Physical Dynamics Research Laboratory) in the Netherlands. At the time, the FDO was a subsidiary of the VMF (United Machine Factory) and a major subcontractor for work conducted on centrifuges by the UCN (Ultra Centrifuge Nederland), the Dutch partner in the URENCO consortium. Despite being a foreign national, Khan received security clearance to work on commercially sensitive projects as he came with good references and it was assumed he desired to become a naturalised citizen. However, this was never checked: while Khan may not have initially intended to conduct espionage, he had become increasingly politicised by world events, including the 1965 and 1971 Indo-Pakistani Wars. The Indian nuclear test in 1974 prompted Khan to write a letter directly to Prime Minister Bhutto, offering his services to the Pakistani nuclear weapons programme. Despite only being cleared for restricted projects, Khan was seconded by the UCN to work on translating secret technical documents on the German G2 centrifuge for 16 days in 1974. This work gave Khan direct access to the operations at Almelo enrichment facility. With information acquired from Almelo, the FDO and many of the VMF subsidiaries, Khan left the Netherlands in December 1975. Khan would use the information he gained to assist the Pakistani nuclear weapons programme, which successfully conducted its first nuclear test in 1988. Khan would also establish a proliferation network based on the contacts and information he initially gained in the Netherlands to supply URENCO based centrifuge technology to multiple countries including Libya, North Korea and Iran.

Facility and Security Systems

Khan's activities were conducted across a range of sites run by different contractors but the main sensitive site that he had access to was the Almelo enrichment facility. The plant housed a major gas centrifuge cascade that provided enriched uranium for URENCO operations. To gain access to the site, Khan should have required the approval by the URENCO Joint Committee and notification be given to the Dutch Ministry of Economic Affairs, but it appears that the FDO deliberately ignored this procedure, such was the demand for Khan's translation skills. Evidently, he was allowed on-site despite his improper authorisation. While the established security practices at the plant may yet have proven sufficient, they were poorly implemented. While Khan should have been restricted to the 'brainbox' (a temporary office used for the translation of documents) outside of the plants security perimeter, the building had no sanitary or canteen facilities and thus its workers were allowed inside the security cordon of the plant. While inside the plant's security perimeter, workers from the 'brainbox' should have been escorted at all times; it appears however that this procedure was routinely ignored. It has been alleged that even basic practices like wearing ID tags were overlooked. Security within the 'brainbox' was also weak: while secret documents were meant to be kept in locked cabinets and shared only on a need to know basis, there was an 'open atmosphere' where colleagues shared classified information with each other. The physical security of these documents was further compromised by there only being a single typist in the 'brainbox' so translators were allowed to take notes and even original documents away to be finished elsewhere.

Incident Summary

After having made the conscious decision to assist the Pakistani nuclear weapons programme some time in 1974, Khan took every opportunity in the next two years to acquire as much information, samples and contacts as possible that he thought may be useful to his future work. The most serious incident was when he was sent to the Almelo 'brainbox' facility for sixteen days in October 1974. While working on translations for the G2 German Centrifuge designs, Khan was seen taking notes in Urdu but explained that he was writing a personal letter. Khan also took advantage of the lax security for classified documents by taking original copies home, explaining that he needed time to make a better translation. In addition, staff claim to have seen Khan within the highly restricted enrichment areas of the plant making notes. While the exact quantity of information that Khan was able to obtain is unknown, it is believed that he had access to all of relevant information kept by VMF's subsidiaries. While the Dutch government claimed in 1979 that Khan had only a 'limited opportunity' to steal information from the UCN given his short time at the facility, Khan left the Netherlands with 'the designs for almost every [URENCO] centrifuge on the drawing board'.

Despite one of Khan's colleagues at the FDO reporting him for holding restricted information at his house three times, no official investigation was launched. It was only after enquiries were made that were sourced back to the Pakistani embassy about specific frequency converters used in URENCO centrifuges, that suspicions were aroused. Even after Khan was directly implicated and later observed asking suspicious questions at a nuclear trade show, the Dutch Minister for Economic Affairs believed that he was involved in industrial espionage rather than proliferation activity. Therefore, rather than being arrested, Khan was 'promoted' away from access to sensitive information while further investigations were conducted to build a case against him. However, this signaled to Khan that he was now a suspect, prompting him to return to Pakistan in December 1975, claiming to be ill. The Dutch government was only prompted to publicly acknowledge the incident after the airing of a German documentary on the subject in 1979, which led to pressure for further action from fellow URENCO Partners. However, by this stage, Khan had established himself in Pakistan and was working, with the assistance of the stolen information, to assist the Pakistani nuclear programme. While Khan was convicted of espionage in the Netherlands in absentia in 1983, the case was later dismissed on a technicality, leaving him free to establish an international nuclear proliferation network.

Suggested Discussion Points:

This case study serves to highlight the threat posed by insiders to sensitive nuclear information at facilities. Key questions for discussion with students might include:

- How are the key topics of nuclear security culture and information security related? What is the interplay between them?
- How might sensitive nuclear information help facilitate an act of nuclear terrorism?
- What were the weaknesses in the security systems at URENCO that enabled A.Q. Khan to steal copious amounts of sensitive nuclear information?

Case Study 5: Los Alamos National Laboratory – Alex Maestas

Perpetrator Profile

There is relatively minimal information available about Alex Maestas, a technician who had worked at Los Alamos National Laboratory (LANL), U.S. for over ten years. According to reports until his attempted theft of gold (worth an estimated 2,000 USD) contaminated with plutonium he had no criminal record. For his actions Maestas was convicted of theft and engaging in an unauthorised transaction involving nuclear material and sentenced to one year in prison and three years of supervised release.

Facility and Security Systems

LANL is a major U.S. research laboratory, focused on supporting the United States' nuclear weapons enterprise. Approximately 9,000 employees and a smaller number of contractors work on the LANL site. Within Room 401 at the Plutonium Facility Four (PF-4) at LANL plutonium is extracted from waste material produced during the production of nuclear weapons. The room contains a series of interconnected glove boxes within which the processing is carried out in order to reduce the risk of radioactive contamination.

Incident Summary

At lunchtime on 24th March 2009 Maestas attempted to leave his working area (Room 401) at Plutonium Facility Four (PF-4) with a small amount of gold, contaminated with plutonium. The gold was a piece of solder that has been used to repair an area used for the melting of materials containing plutonium. While it is unclear how Maestas removed the solder from the glovebox it was deduced from the subsequent investigation that he attempted a decontamination process, either on the gold itself, the packaging, or the gloves he used to handle the waste. While leaving the area he set off a personnel contamination monitor, this prompted Maestas to inform the radiation control technician that he was carrying material that should have undergone a separate screening. After an assessment it was determined by the technician to be radioactive. Maestas then attempted to explain his action by claiming that he was asked to bring the material into a separate area, the machine shop, and suggested he return it back to the glove box in room 401. However, his explanation was not perceived to be credible as the machine shop was a cold 'radiation free' area, to which radioactive material would never be transferred. He also could not remember why he was transferring it or who he was transferring it too. During the subsequent investigation Maestas admitted that he had scanned the material with a hand and foot monitor prior to leaving room 401 and that it did not trigger an alarm. This monitor only detects alpha radiation, which although emitted from plutonium was likely shielded by the gold in the sample. In contrast the personnel contamination monitor also detects beta and gamma radiation and was able to detect the beta particles emitted from the solder. It subsequently emerged that Maestas did not know that this detection system was sensitive to beta radiation. At trial, as part of a plea bargain, Maestas pleaded guilty to the theft of both government property and nuclear material.

Suggested Discussion Points:

In contrast to the other incidents presented in this handbook, this case study provides an example of where an insider was caught in the act, as opposed to his or her actions being uncovered after the event. Consequently, it directly highlights the effectiveness of protective measures when applied correctly. Key questions for discussion with students might include:

- What role did security culture play in successfully determining that Maestas actions were malicious in nature?
- What were the potential health risks posed by the solder? What if the solder had been melted down and made into jewellery?
- Why did Maestas scan the solder with the hand and foot monitor before leaving room 401?

Key Sources for Nuclear Case Studies

Case Study 1

- Transcript of interview with Leonid Smirnov, Public Broadcasting Service, http://www.pbs.org/wgbh/pages/frontline/shows/nukes/stuff/script.html (November 1996)
- Potter, William C. (1996), 'Nuclear Leakage from the Post-Soviet Nuclear States,' Oral Presentation before the Permanent Subcommittee on Investigations US Senate Committee on Governmental Affairs, available via **http://www.bu.edu/globalbeat/pubs/papers/w_potter.html** (13th March 1996)
- Sam Roe, 'Trafficking in stolen nuclear material on the rise', Chicago Tribune, **http://articles.chicagotribune.com/2002-01-31/news/0201310215_1_nuclear-materials-nuclear-device-nuclear-weapon** (31st January 2002)

Case Study 2

- E. Morris Howard, 'Attempted Extortion – Low Enriched Uranium', NRC Information Notice No. 79-02, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1979/in79002.html (2nd February 1979)
- E. Morris Howard, 'Attempted Extortion – Low Enriched Uranium', NRC IE Circular No. 79-08, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/circulars/1979/cr79008.html (2nd February 1979)
- "Dale gets 15 years for uranium plot", Wilmington Morning Star, 9th May 1979
- Jeffrey T. Richelson, 'Defusing Armageddon: Inside NEST, America's Secret Nuclear Bomb Squad', (W. W. Norton & Company, February 2009), pp. 37-42

Case Study 3

- David Beresford, 'Truth is a Strange Fruit: A Personal Journey Through the Apartheid War', Jacana Media (Pty) Ltd (1st July 2010)
- Mohtadi, Hamid and Antu Murshid, 'A Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks: 1950-2005', p. 17, (7th July 2006)
- "South African who attacked a nuclear plant is a hero to his government and fellow citizens", http://www.publicintegrity.org/2015/03/17/16895/south-african-who-attacked-nuclear-plant-hero-his-government-and-fellow-citizens, (March 2015)
- 'How we blew up Koeberg (... and escaped on a bicycle)', Mail and Guardian, http://mg.co.za/article/1995-12-15-how-we-blew-up-koeberg-and-escaped-on-a-bicycle, (15th December 1995)

Case Study 4

- Albright, David, 'Peddling Peril', (New York: Free Press, 2010)
- Corera, Gordon, 'Shopping For Bombs. (Oxford: Oxford University Press, 2006)
- Dutch Government Working Group, 'The Case Khan', Amsterdam (1979) Orginal Language: Dutch, Translation: Frank Hemmes
- Khan, Feroz Hassan, 'Eating Grass' (Stanford: Stanford University Press, 2012)
- Nuclear Threat Initiative (NTI), 'Pakistan Nuclear Chronology'. Nti.Org http://www.nti.org/media/pdfs/pakistan_nuclear.pdf?_=1316466791 (2011)

Case Study 5

- 'United States v. Maestas', United States Court of Appeals, No. 10–2204, accessed via http://caselaw.findlaw.com/us-10th-circuit/1572680.html (28th June 2011)
- 'Former LANL Employee Sentenced for Stealing Irradiated Gold', FBI Albuquerque Division, http://www.fbi.gov/albuquerque/press-releases/2010/aq083110.htm (31st August 2010)
- 'Former Los Alamos lab worker accused of theft', The Seattle Times, http://seattletimes.com/html/nationworld/2010034663_apuslabtheftcharge.html?syndication=rss (9th October 2009)

Non-Nuclear Case Studies

The five case studies presented in this section are drawn from a diverse range of industries including aviation, gaming, waste-treatment, mining and finance. They include examples of insiders including with external adversaries, coercion through the threat of physical violence and in several cases significant financial losses to the businesses under attack. Although exhibiting certain differences with the nuclear industry there are a number of commonalities, particularly when it comes to the flow of valuable items/materials, security systems employed and insider motivations. With insider incidences arguably more common in non-nuclear industries they serve as examples of what could potential happen within the nuclear context.

Case Study 6: Maroochy Shire Sewage Treatment Plant - Vitek Boden

Perpetrator Profile

Vitek Boden was 48 years old at the time of the incident in 2000. An information technology professional he was employed from 1997 to 1999 by Hunter Watertech, a small Australian firm that supply supervisory control and data acquisition (SCADA) and telemetry systems for industrial facilities and public utilities. During this period of employment he was responsible as site supervisor for installing SCADA radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia. In December 1999 Boden resigned from Hunter Watertech due to a 'strained' relationship with the company. Boden then immediately applied for a job at Maroochy Shire Council but was not hired. This motivated Boden to seek revenge on both his former employer and the council. In early 2000 he intentionally manipulated the SCADA systems at the council to cause a release of sewage. He was apprehended in April 2000, tried and found guilty in October 2001 of 26 counts of wilfully using a computer to cause damage and one count of causing environmental harm, and was sentenced to two years in prison.

Facility and Security Systems

The Maroochy Shire SCADA controlled sewage system had 142 pumping stations spanning more than 1157 km^2. SCADA systems are used to gather real-time data, monitor equipment and control processes within industrial facilities. This specific system included special purpose control computers at the pumping stations linked to valves and alarms at each specific site. These computers were controlled from a central station with communications relayed via a radio (as opposed to a wired network). There were no cybersecurity procedures or systems at the facility, with unsecure radio links used to communicate between the control room and the pumping stations. Hunter Watertech, the contractor, didn't have personnel reliability programmes in place and consequently Boden was never vetted or his behaviour monitored.

Incident Summary

In late 1999, shortly before resigning, Boden stole a SCADA configuration programme, two-way radio equipment and a PDS Compact 500 computer control device that could be used to impersonate a genuine machine from Hunter Watertech. From January and April 2000 he used this equipment and his knowledge of the council's SCADA controlled sewage system to generate spoof signals, which stopped pumps, prevented alarms being reported to the central control station and caused loss of communication between the pumping stations and central control. During this time he issued radio commands at least 46 times to the sewage system. As a result of these actions 800,000 litres of raw sewage was released into the surrounding area causing significant ecological damage. Initially his actions were attributed to the newly installed system malfunctioning and Hunter Watertech was asked to investigate the source of the problem. This investigation involved monitoring all signals transmitted on the sewage systems radio network. A detailed analysis identified that bogus signals were being purposefully sent over the network. Boden, due to his role in installing the system, was identified as a potential suspect and placed under police surveillance. On 23rd April 2000 Boden's vehicle was pulled over by police with a search finding the stolen Hunter Watertech equipment. This was examined and it was found that the computer control device was programmed to simulate a specific pump station on the network. Although this was denied by Boden, who instead claimed that the computer was used for his business and personnel correspondence, he was convicted and sentenced to two years in jail.

Relevance to Nuclear Security

This case study is highly significant as it is one of the first known examples of an insider intentionally manipulating a process control system (PCS), resulting in both its disruption and subsequent negative impact on the local environment. This is of direct relevance to the nuclear industry where SCADA systems are routinely used to control and relay information on a variety of processes at a facility. SCADA systems were traditionally perceived to be immune from cyber attack due to historically being completely isolated from the Internet and operated by proprietary protocols and specialist hardware. However, this analysis was done from the perspective of external adversaries not insiders as this case study graphically illustrates. In presenting this case study a link could be made to Project Aurora, an example from 2007, where scientists from Idaho National Laboratory demonstrated how a staged cyber attack could be used to cause an electric generator to self-destruct.

Interestingly, over the past fifteen years nuclear operators have been moving to 'open protocols and off-the-shelf hardware' for PCS at nuclear power plants and also in some case connecting them (indirectly) to the Internet. This has served to increase the relevance of external threats as specialist knowledge, software and hardware may no longer be needed to access these systems. This was highlighted by the infection of process control network at the David Besse Nuclear Power Plant (NPP) in France in 2003 by the slammer worm. Although a firewall was in place to protect these systems from the wider Internet this was bypassed by a contractor who logged on the corporate network of his company from within the NPP. This is also a highly relevant example, which could be linked to this case study.

More generally this case study demonstrates that insider threats to nuclear facilities are not just posed by permanent staff but by also temporary contractors who have specialist narrow knowledge of certain key systems. It also highlights how disgruntlement, in this case of a former employer, can motivate an individual to undertake a malicious act for the purpose of revenge. Finally, and perhaps most surprisingly it shows that certain individuals can present a threat even after leaving an organisation, in the information security context organisations should therefore consider the regular changing of procedures, protocols and passwords.

Suggested Discussion Points:

The case study also offers a number of possibilities for in-class debate. Key questions for discussion with students might include:

- What is a SCADA system and how is it typically employed at nuclear facilities?
- What are the security vulnerabilities of SCADA systems and PCS more generally and how have these changed/evolved over time? What are the potential future cyber threats to nuclear facilities?
- Based on the classification within the IAEA's Nuclear Security Series No. 8, how would you assess Boden's level of access, authority and knowledge?
- Can you highlight other examples where insiders or external adversaries have attempted (failed or successful) to take control of PCS systems at industrial facilities?

Case Study 7: British Airways Attack - Rajib Karim

Perpetrator Profile

The individual in question, Rajib Karim, was employed as a software engineer at a British Airways (BA) IT centre in Newcastle from the mid-2000s. Originally from Bangladesh, Rajib studied electronics at Manchester University from 1998-2002 before returning to Bangladesh where, influenced by his brother Tehzeeb, he became a supporter of extremist organisation Jammat-ul Mujahideen Bangladesh (JMB). In 2006, Rajib returned to the UK with his family and obtained a job as a graduate at BA in 2007.

The process of radicalisation that began in Bangladesh continued in the United Kingdom. In December 2009, Tehzeeb travelled to Yemen where he made contact with radical cleric Anwar al-Awlaqi and the new division of Al-Qaeda that had established itself there, Al-Qaeda in the Arabian Peninsular (AQAP). Tehzeeb put al-Awlaqi in touch with his brother Rajib prompting a frank exchange of messages between the radical cleric and the BA worker, as they contemplated how they could exploit Rajib's position within the airline company to launch a terrorist attack. Rajib's motivation was wholly ideological and he aspired to martyrdom. In February 2011, Rajib Karim was convicted of five counts of engaging in conduct in preparation of acts of terrorism, contrary to section 5 of the UK Terrorism Act, following a trial at Woolwich Crown Court.

Facility and Security Systems

BA is the national flag carrier airline of the United Kingdom. Flying to over 400 destinations and carrying some 40 million passengers, the company has a strong global presence and operates almost 300 aircraft (2013 figures). Yet while BA continues to be a lucrative business (total revenue in 2013 exceeded £11 billion) the airline (along with others) continues face significant challenges in its efforts to prevent terrorism.

Rajib Karim was employed as a software engineer at a BA IT centre in Newcastle. All BA employees are subject to a screening process, which usually includes a five-year personal history check and right to work check. Prospective employees are usually required to provide the employment dates, company names and addresses of all previous employers (including recruitment agencies). Details regarding educational background are also required.

To comply with Department for Transport regulations, BA may ask prospective employees to complete a criminal record and counter terrorism check, although these are normally only for persons accessing sensitive areas. Rajib, for example, would not have been subject to this level of scrutiny.

The screening process for Rajib Karim did not raise any red flags or concerns. Rajib had no prior criminal convictions in the United Kingdom and was not on any government watchlists. Moreover, in his role at the IT Centre in Newcastle, Rajib was not in a position to interfere with aircraft held no real responsibility on this front. Rajib's behaviour and Internet activity were thus never monitored.

Incident Summary

In 2011, UK police intercepted a series of encrypted messages sent between a British Airways employee, Rajib Karim, and then senior Al-Qaida figure Anwar al-Awlaqi. As police deciphered over 300 of the intercepted messages, they began to build a profile of a radicalised and dangerous individual with a strong desire to play a role in religious Jihad against Western nations.

In 2010, Rajib began corresponding with Anwar al-Awlaqi, a senior figure in Al-Qaeda in the Arabian Peninsula (AQAP). In a series of heavily encrypted exchanges, Rajib volunteered information on how he could cause disruption to BA both operationally and financially, by attacking their computer servers. He claimed that he could, at the least, cause BA significant financial damage and perhaps even ground its entire fleet. Karim also offered to begin recruiting other people.

During a 2009 industrial strike, Rajib also applied for a position as cabin crew in response to a request from managers. His application was rejected only because he had not been at the company long enough to earn a transfer. Normally lateral movement is accommodated within the company.

As Rajib grew impatient for martyrdom, Al-Awlaqi urged him to bide his time and to stay in the UK while applying for his UK passport, avoiding any activity that would expose him to scrutiny. Rajib was well-educated, mild-mannered and respectful and this helped him to avoid suspicion. He also described to al-Awlaqi how he had engaged with Western practices such as going to the gym and playing football with a local team to avoid scrutiny.

BA had no idea of Rajib's religious tendencies or his involvement in terrorism until the company was informed by police. The Metropolitan police said that the incident prompted 'the most sophisticated decryption task of its kind ever undertaken by the Met's Counter Terrorism Command'.

Relevance to Nuclear Security

The case of Rajib Karim is highly relevant to the nuclear sector, relating as it does to human reliability and the extent to which employees can and should be vetted and monitored. Of particular interest is the combination of Rajib's skill set - his IT background equipped him to apply sophisticated levels of encryption to his communications and would, no doubt have helped him cover his tracks online - and his recognition of the need to appear 'normal' - engaging in social activities etc so as to avoid raising suspicion.

Suggested Discussion Points:

The case study also offers a number of possibilities for in-class debate and discussion. Key questions for discussion with students might include:

- What do you see as the most striking feature of this case study? Why?
- What weaknesses can you identify in the British Airways screening process?
- What changes or measures could British Airways introduce to mitigate the risk of a similar situation occurring again?
- Would the evolution of this case study have been different if Rajib Karim was working at a nuclear facility? If so, how?
- What parallels can be drawn with the nuclear industry?

Case Study 8: Argyle Diamond Mine – Barry Crimmins

Perpetrator Profile

The Argyle Mine diamond theft constitutes a particularly complex incident, whereby a lucrative and long-running case of insider theft was compounded by a sophisticated external support network. In this case, the perpetrator, Barry Crimmins, was a former police officer in Victoria, Australia who was employed as security manager at the Argyle Diamond Mine in the late 1980s and early 1990s. Crimmins was recruited by an external actor who paid him to steal rough diamonds from the mine and served as 'handler' for the stolen goods. It seems that the motivation was largely financial; during the court case, Crimmins claimed that his wife was 'a "greedy" woman who had driven him to commit the thefts'. Over a period of five years, diamonds with an estimated trade value of some USD 30 million were stolen and sold on the black market.

Facility and Security Systems

The Argyle diamond mine is located in the East Kimberley region of Western Australia. It is the largest single source of diamond production in the world by volume. The Argyle mine is particularly renowned for its rare pink diamonds. Indeed the mine is responsible for approximately 90 per cent of the global supply of pink diamonds. To give a sense of the current value attached to these rare diamonds, it is worth noting that in November 2013 a vivid pink diamond became the world's most expensive diamond when it was sold for GBP 51 million at auction. The commercial enterprise that has built up around the Argyle mine is clearly an extremely lucrative one with high value materials to be protected.

The nature of the product mined at Argyle means that security has always been a priority at the facility. At the time of this incident, for example, security measures included perimeter fences, a guard force and extensive video surveillance. This said, there were a number of important weaknesses in the system. A number of surveillance cameras, for example, were not functioning. In addition, while employee handling of the diamonds commenced at the mining and sorting stage, no official record of the diamonds was made until they were weighed and registered on the company books.

Incident Summary

The case study of this mine dates to the period 1988-1993 when experts associated with the Argyle mine noticed that pink diamonds of the sort mined at Argyle were turning up on the international market with no accountable background. In November 1989, the mine informed West Australian Police of its suspicion that a significant amount of diamonds was being stolen from the mine. Police embarked upon the first of three separate enquiries into the alleged theft.

It was not until late 1993, however, that the source of the theft was uncovered. It transpired that a Security Manager at the Argyle mine, Barry Crimmins, was responsible for a series of thefts in the period in question. As a Security Manager, Crimmins had access to most areas of the facility. His role meant that he also had a detailed knowledge of the security measures in place at the mine and was in a position to exploit weaknesses in the system. Crimmins knew, for example, that there was a gap between the time when the diamonds were sorted at the mine and the point when they were weighed and registered. He was also aware of the positioning, range and periods of activity of CCTV cameras and frequently conducted inspections alone and at irregular hours.

Crimmins had been recruited by a corrupt businessman, Lindsay Roddan, and was paid for a supply of rough diamonds that he stole at the sorting stage and transported from the facility in plastic film cannisters. Roddan then sold the diamonds on the black market. It is worth noting that it was not the police investigation that exposed Crimmins, rather it was his wife Lynette Crimmins who informed police. Lynette had become romantically involved with Lindsay Roddan and revealed the details of the crime when the affair soured.

Yet this was only part of the story. The Argyle thefts had been the subject of two unsuccessful police investigations. It has been suggested that high-ranking police officers frustrated and limited those investigations in order to protect Roddan. With regard to the second investigation in particular, it was alleged that the Senior Sergeant in charge, Senior Sergeant Jeffrey Noye, formed a corrupt relationship with Roddan, pursuant to which he concluded that investigation by exculpating Roddan of any involvement in the theft of diamonds.[15]

In any case, Lynette Crimmins' confession triggered a third investigation led by different detectives. This third investigation found evidence to suggest that Roddan had paid corrupt police officers to abandon the first two investigations, thus ensuring the continuation of his operation. The third investigation resulted in the prosecution of Barry Crimmins, Lynette Crimmins and Lyndsey Roddan.

Relevance to Nuclear Security

The case of Barry Crimmins touches on a number of issues of significance in the nuclear industry, namely knowledge, authority and access. As a Security Manager within the mine, Crimmins had a detailed knowledge of the security measures in place across the facility. Indeed, his role gave him responsibility for the maintenance and operation of some of these systems. His position also gave him unrestricted access to all parts of the facility and this freedom of movement was crucial to the success of the diamond theft. Finally, in a hierarchical system, Crimmins' authority was never questioned by subordinates or by the labourers who mined and sorted the diamonds. This explains why he could transport the diamonds using the rather unusual method of film cannisters.

The case illustrates very well the threat that the diamond industry faces from insiders at all levels, and this point is directly applicable to the nuclear industry. Moreover, the case study highlights the need for a robust security culture that promotes vigilance and encourages responsibility for security among all staff within an organisation. Had employees in the sorting area questioned the irregular movements of Crimmins, for example, this may have prompted a targeted internal investigation and, at the least, disrupted the operation.

Suggested Discussion Points:

The case study also offers a number of possibilities for in-class debate and discussion. Key questions for discussion with students might include:

- What security flaws can you identify in Argyle's systems at this time? Are these predominantly physical protection issues or human issues?
- Could this scenario have been prevented?
- What measures would you implement to strengthen Argyle's security after this incident?
- What steps could Argyle take to promote the development of a broader security culture within the mine? What aspects of nuclear security are relevant here?
- What are the most important parallels you see with nuclear security here?

15 It should be noted that despite an investigation of this issue of corruption by a Task Force established by the Australian Federal Police, the allegations of corruption did not result in any prosecutions due to the fact that a number of police officers refused to cooperate with the investigation.

Case Study 9: Bank of Ireland – Shane Travers

Perpetrator Profile

Setting out the perpetrator profile for this case study is not a straightforward matter. The robbery was carried out by a gang of armed men, who coerced a Bank of Ireland employee into providing access to over 7.5 million Euros in cash. Given the knowledge the gang had, both of the employee's level of access and of the level of funds present in the bank at the time of the robbery, police strongly suspected insider involvement. Shortly after the burglary was committed, a separate Bank of Ireland employee was arrested, but ultimately, a lack of evidence meant that no charges were pressed.

Facility and Security Systems

The Bank of Ireland is the oldest commercial bank in Ireland. One of the 'big four' financial institutions, the bank represents an enormous and sprawling commercial operation with an annual revenue of some 1.8 billion Euros. As with all major financial institutions, Bank of Ireland faces a range of security threats and expends considerable resources on efforts to protect its assets.

Physical protection measures include time-locked vaults, CCTV surveillance, panic buttons and armed guards around large movements of cash. Financial institutions such as Bank of Ireland also liaise closely with local authorities to develop a comprehensive risk assessment. Information security is also a priority and leads to regular network scans and patch checks. The Central Bank of Ireland also recently began undertaking inspections of financial institutions to assess their ability to deal with cyber attacks.

Incident Summary

This case study relates to the biggest bank robbery in the history of the Republic of Ireland. In February 2009, an armed gang coerced a Bank of Ireland employee, Shane Travers, into removing over 7 million euros from the bank and handing it over to the members of the gang at a Dublin rail station. The theft constituted a so-called 'Tiger kidnapping' where Travers' partner and members of her family were held hostage at gunpoint while he carried out the gang's request.

The ordeal began when a group of six armed men accosted the Travers' partner, Stephanie Smith, and her mother outside her home in Kilteel near Dublin. Travers was already inside with Smith's nephew. The family was taken away in a van while Travers was forced to drive to the bank. The gang was aware that the branch at which Travers worked had recently taken delivery of a significant cash transfer and Travers was instructed remove the cash and bring it to a train station in the North of the city. The gang was well prepared and Travers was provided with photographs of his partner being held at gunpoint, as well as photographs of another employees' homes, to use to convince his colleagues to help him if necessary.

Travers carried out the instructions and succeeded in withdrawing the money. Security protocols at the bank were largely ignored – police should have been called as soon as Travers arrived at the bank, an amount of cash of that size normally requires multiple authorizations before release, etc. – and a number of Travers' colleagues actively assisted him in his task once they saw the photograph and heard his explanation. Staff later argued that they felt it was better to let the thieves have the money as they believed the gang could be hunted down by police at a later date and it was more important to secure the release of the hostages.

The gang escaped with the money and a police investigation ensued. The investigation revealed that the gang had strong links to organized crime in Dublin and that it was highly likely that an insider at Bank of Ireland was involved in the planning. The gang had a detailed knowledge of Travers' routine, for example, and knew that he would be spending the night at his partner's house. The gang also had key details of other employees with access to the bank vault. As mentioned above, a Bank of Ireland employee was subsequently arrested by police, but no charges were brought against the individual. Seven arrests were made in connection with the robbery yet in the end, only two men were charged.

Relevance to Nuclear Security

The Bank of Ireland study illustrates the challenges of coercion in the context of insider threats. In this case, the lives of Shane Travers' partner and family were in the balance and this served as effective leverage for the gang. Preoccupied with their safety, Travers broke a number of security protocols within the bank and complied fully with the requests of the armed gang.

The relevance to the nuclear context is clear: employees under coercion could be persuaded to provide malicious actors with access, materials and/or sensitive information. In this instance, the subject of coercion is driven by fear and may well use his/her knowledge of the facility to circumvent security systems.

Suggested Discussion Points:

The case study also offers a number of possibilities for in-class debate and discussion. Key questions for discussion with students might include:

- In your opinion, what are the key security challenges in this scenario?
- Could a similar scenario taken place in a nuclear facility? If not, why not?
- What measures could be implemented with a view to increasing the resilience of a facility to attacks through coercion?
- What broader lessons can be drawn from this case study with regard to security culture and the relationship between physical protection measures and the human element of security?

Case Study 10: Desert Diamond Casino – Adam Thomas Vega

Perpetrator Profile

Adam Thomas Vega was a member of staff at the Desert Diamond Casino in Tucson, Arizona, U.S. from May 2001 to July 2007. During this time, Vega worked as a slot floor person and his responsibilities included providing service to gaming machine guests, performing minor repairs to gaming machines, troubleshooting machines and documenting malfunctions unable to be repaired at machine level. Of most relevance to this case study, Vega also dealt with issues around jackpot payouts and was required to act as a witness/verifier on jackpot payouts and associated documentation. As part of his job, Vega also carried a personal 'bank' of 5,000 USD in order to hand pay patrons who won slot machine jackpots in amounts under 1,200 USD. In short Vega held a position of considerable responsibility.

The position of slot floor person usually requires prior experience in the gaming industry, yet the role is not particularly well paid, with income ranging from 10-15 USD per hour on average. Against this background, it is highly likely that Vega's motivation for protracted theft was financial. Interviews conducted with security and surveillance personnel in the casino industry also suggests that the majority of employee theft falls into this motivational category.

Facility and Security Systems

According to certain estimates, over 60% of theft within the casino industry is carried out by employees or insiders. In an industry dealing in enormous amounts of money each year – the annual revenue of the Las Vegas casino market was approximately 6.2 billion USD in 2012 – the potential threat to commercial business is significant. For obvious reasons, little information exists on how insiders steal from casinos. There is, however, some information in the public domain.

Casinos are normally equipped with a comprehensive security system that relies heavily on liberal use of CCTV. Gaming tables are closely monitored remotely and also by 'pit managers', employees who supervise card dealers etc. The slot machine area is subject to similar supervision. Given the significant amounts of money that pass through these businesses, the use of two-person rule is also common, particularly in areas where money is counted or changes hands such as in the 'cage' (where chips are exchanged for cash). It should be noted, however, that while casinos employ a robust security system, they are keen to maintain a low security profile lest this detract from the pundits' gambling experience. Casino security officers, for example, are present on-site but rarely have a major presence in the gaming area.

With regard to the specifics of this particular case study, it is also worth noting the normal procedure around the payment of slot machine winning jackpots. The process was a relatively straightforward one. Any time a patron won a jackpot at a slot machine, an electronic notification would be generated and a slot floor person would respond to the winning machine. The slot floor person would enter his card into the machine and then enter the jackpot amount into a keypad on the machine. Upon the amount being entered, an electronic signal would be sent to a cash booth station and a jackpot slip generated. This would then be signed by the employee and verified by another slot floor person. The jackpot slip comprised two copies, the Accounting copy and the 'Cage' copy. The patron would be paid from the initial slot floor person's personal bank. This done, the slot floor person would deposit one copy of the jackpot slip in the casino's audit box and the other copy would be taken to the cage and exchanged for cash. In this way, the slot floor person ensured that his personal bank was replenished to the original 5,000 USD.

The system here was designed to provide a rapid means of verifying and processing patron jackpot wins, while at the same time maintaining a robust accounting system. Clearly, the slot floor person was integral to this process and held considerable responsibility. As we will see, however, the system had considerable potential to be abused.

Incident Summary

This case study relates to the largest casino related theft by an employee in Arizona casino history. In April 2009, Adam Thomas Vega of Tucson was convicted of stealing a total of 664,442 USD from the Desert Diamond Casino in Tucson, Arizona where he worked as a slot floor person. The crime involved approximately 585 unique incidents with no individual amount exceeding 1,195 USD (the significance of this amount is explained below).

From 2001-2005, Vega did not engage in any criminal activity at the casino (at least, none that ever came to light). However, during this period, he gained a comprehensive knowledge of the security system of which he was part. Vega also befriended many of his colleagues working on the casino floor. At the point at which the thefts began, Vega had noticed that certain slot floor procedures were not rigorously enforced, in particular the verification process for jackpot wins.

This knowledge proved crucial as Vega's plans for theft developed and while the jackpot win process discouraged interference due to the presence of a patron having legitimately recorded a win, Vega realized that lax verification processes could be used to exploit another process – the jackpot override process.

On rare occasions, a patron would score a jackpot on a slot machine but the machine would fail to send a signal to the online system. On such occasions, the casino implemented a jackpot override process. This involved a slot floor person entering the information as he normally would on the machine keypad. The information is sent to the cash booth station where a supervisor would be required to verify the jackpot and enter a password. This would cause the cash booth station to produce an override jackpot ticket with the term 'override' printed in the top left corner. Normally, this would then be signed by the attending supervisor and the payment process would continue as normal (ie the patron paid from slot floor person's bank, copies of ticket deposited in audit box and cage).

In preparation for his thefts, Vega obtained at least one supervisor password. He bypassed the slot machines and began generating jackpot override tickets directly from the cash booth machine using the stolen password. His presence at the cash booth machine was normal and therefore not questioned. However, out of the 585 jackpot tickets that Vega generated over two years, only one was signed by a supervisor. Throughout this period the lack of verification was ignored or overlooked by other members of staff, both in the cage and in the accounting team that dealt with the deposit box. It is likely that these employees assumed that the supervisor password requirement was an adequate barrier to exploitation of the system.

Furthermore, Vega kept all of his jackpot override tickets below 1,200 USD (the majority were for 1,195 USD). This was significant as under US laws, tax must be paid on winnings of over 1,200 USD on slot machines. When this amount is won on a slot machine, the casino is required to provide the winner with a W-2G tax form. Furthermore, the organisation must file its own W-2G with the IRS. In an attempt to avoid the scrutiny of the authorities and recognition by the casino, Vega made sure to keep stolen amounts below the 1,200 USD threshold.

Vega's illicit activity lasted two years until the changes in accounting personnel led to closer scrutiny his activities, triggered by the missing supervisor signature.

Relevance to Nuclear Security

The case of Adam Vega holds considerable relevance for the nuclear industry. The casino industry is renowned for its emphasis on security and implements a range of procedures, often adopting the 'layered' approach seen in the nuclear industry. This security focus is not surprising given the scale and persistence of the threat to casino assets, primarily chips and cash. Measures such as two person rule and two-layer verification are directly comparable to the nuclear industry, as is the heavy reliance on CCTV surveillance.

The Vega case illustrates, however, the significance of knowledge and access in terms of insider threats. Employees, and particularly those engaging directly with security systems, are best placed to identify weaknesses in existing systems and/or develop innovative ways of exploiting the barriers to theft or other illicit activity. The Vega case is marked by a series of failures (primarily managerial and accounting) that are demonstrative of a flawed security culture within the casino. The fact that the thefts occurred regularly over a two-year timeframe and were only detected after a change in personnel is evidence of the weaknesses here. Other issues such as password protection also have direct bearing on the nuclear industry.

Suggested Discussion Points:

The case study also offers a number of possibilities for in-class debate and discussion. Key questions for discussion with students might include:

- What security weaknesses can you identify in the Vega case?
- Are these weaknesses that could exist in the nuclear industry?
- What, in your view, is the primary indicator of a weak security culture here?
- What measures could the casino take to strengthen its security culture?
- How important is employee understanding and awareness in this case study?

Key Sources for Non-Nuclear Case Studies

Case Study 6

- Slay, J. and Miller, 'Lessons learned from the Maroochy Water Breach', pp. 73-82 in E. Goetz and S. Shenoi (eds.), IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection (Boston: Springer, 2008)
- Marshall D. Ahrams and Joe Weiss, 'Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia', Presented at the Annual Computer Security Applications Conference (December 2008)
- Hacker Jailed for Revenge Sewage Attacks, The Register, http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ (31st October 2001)
- Michael Swearingen, Steven Brunasso, Joe Weiss, and Dennis Huber, 'What you need to know (and don't) about the Aurora Vulnerability', Power: Business and Technology for the Global Generation Industry (1st September 2013) http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/
- Brent Kessler, 'The Vulnerability of Nuclear Facilities to Cyber Attack', Strategic Insights, Vol. 10, Issue 1, pp. 15-25, Spring 2001.
- Staged cyberattack reveals vulnerability in grid, YouTube, http://www.youtube.com/watch?v=fJyWngDco3g&feature=related

Case Study 7

- Vikram Dodd, 'British Airways worker Rajib Karim convicted of terrorist plot', The Guardian, 28th February 2011, http://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim
- 'BA worker Rajib Karim convicted of terror charges', BBC News, 28th February 2011, http://www.bbc.co.uk/news/uk-england-tyne-12561994
- Duncan Gardham, 'British Airways bomber jailed for 30 years', The Telegraph, 18th March 2011, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8391162/British-Airways-bomber-jailed-for-30-years.html
- 'Excerpts from Rajib Karim terror plot messages', The Northern Echo, 28th February 2011, http://www.thenorthernecho.co.uk/news/8880903.Excerpts_from_Rajib_Karim_terror_plot_messages/?ref=rss
- 'Man jailed for 30 years for terrorism offences', Metropolitan Police, 18th March 2011, http://content.met.police.uk/News/Man-jailed-for-30-years-for-terrorism-offences/1260268719101/1257246745756
- 'Criminal Sentence – Rajib Karim', The Law Pages, http://www.thelawpages.com/court-cases/index.php?res=1.

Case Study 8

- 'Royal Commission into whether there has been any corrupt or criminal conduct by Western Australian police officers', Perth, 14th August 2003, http://www.slp.wa.gov.au/publications/publications.nsf/DocByAgency/A6287B2BB0C1A84A48256D75002F96C2/$file/S030814.pdf
- Russell Shor, 'Probe still seeks stolen Argyle gems', JCK Magazine, May 1996, http://webcache.googleusercontent.com/search?q=cache:irSqnG9qpDkJ:www.jckonline.com/1996/05/01/crime-watch+&cd=1&hl=en&ct=clnk&gl=us&client=safari
- Duncan Graham, 'Diamond Talk Brings End to Argyle Caper', The Age, 17th May 1996, http://webcache.googleusercontent.com/search?q=cache:CEmE_O2JJ3oJ:www.diamondtrading.com.au/diamond-trading-articles/1996/5/17/diamond-talk-brings-end-to-argyle-caper/+&cd=10&hl=en&ct=clnk&gl=us&client=safari
- 'Theft of diamonds: One more found guilty', New Straits Times, 19 May 1996, https://news.google.com/s?nid=1309&dat=19960519&id=c8pOAAAAIBAJ&sjid=YB8EAAAAIBAJ&pg=6722,4146520&hl=en
- Keith Gosman, 'The Great Kimberley Diamond Heist', Sydney Morning Herald, 15th April 1994.

Case Study 9

- '7.6m tiger kidnapping probe progresses with arrest of bank employee', Irish Examiner, 30th January 2010, http://www.irishexaminer.com/ireland/icrime/76m-tiger-kidnapping-probe-progresses-with-arrest-of-bank-employee-110939.html
- Gavin McLoughlin, 'Central Bank undertakes new inspections for cybersecurity', Irish Independent, 10th May 2015, http://www.independent.ie/business/irish/central-bank-undertakes-new-inspections-for-cybersecurity-31209627.html
- Robert Mackey, '7 arrests after Ireland's biggest bank heist', New York Times, 28th February 2009, http://thelede.blogs.nytimes.com/2009/02/28/7-arrests-after-irelands-biggest-bank-heist/?_r=0
- Shawn Pogatchnik, 'Bank of Ireland Employee Steals Millions To Pay Ransom', Huffington Post, 25th May 2011, http://www.huffingtonpost.com/2009/02/27/bank-of-ireland-employee-_n_170546.html?

Case Study 10

- 'Indictment as to Adam Thomas Vega', USA v. Vega, Arizona District Court, Case No.4:08-cr-01101, http://www.plainsite.org/dockets/2bostddpd/arizona-district-court/usa-v-vega/
- Sheryl Kornman, 'Casino worker embezzled $644,000', Tuscan Citizen, 11th April 2009.
- Brian Pedersen, 'Fake casino tickets land former Desert Diamond worker in prison', Arizone Daily Star, 30th September 2009, http://tucson.com/news/fake-casino-tickets-land-former-desert-diamond-worker-in-prison/article_0f396e1b-74c4-50d3-a69e-ecc09599c0e0.html
- 'Casino employee pleads guilty for embezzling $644,442 from Tucson casino', Office of the United States Attorney, District of Arizona, 10th April 2009, http://www.justice.gov/sites/default/files/tax/legacy/2009/04/20/txdv09_2009-127(Vega)%5B1%5D.pdf

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