CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Nuclear Security Culture in Practice

A Handbook of UK Case Studies

Karl Dewey, George Foster, Prof. Christopher Hobbs & Dr. Daniel Salisbury

2021

Table of Contents

CASE STUDIES

Supported by:

Department for Business, Energy & Industrial Strategy

LIST OF FIGURES

Glossary

AGR	Advanced Gas Cooled Reactor
BEIS	UK Department for Business, Energy and Industrial Strategy
BNFL	British Nuclear Fuels Limited
CGN	China General Nuclear Power Group
CIRAS	Confidential Incident Reporting and Analysis Service
CPNI	UK Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
DBT	Design Basis Threat
DRS	Direct Rail Services
ED&I	Equality, diversity and inclusion
EDF	EDF Energy
GDF	Geological Disposal Facility
HPC	Hinkley Point C
HR	Human resources
IAEA	International Atomic Energy Agency
INS	International Nuclear Services
MCA	Maritime and Coastguard Agency
NCSC	National Cyber Security Centre
NDA	Nuclear Decommissioning Authority
NISR	Nuclear Industries Security Regulations
NTS	Nuclear Transport Solutions
NSCP	Nuclear Security Culture Programme
ONR	UK Office for Nuclear Regulation
PNTL	Pacific Nuclear Transport Limited
RWM	Radioactive Waste Management
SLT	Senior leadership team
SyAPs	Security Assessment Principles
TTX	Tabletop exercise

Acknowledgements

This handbook was developed through the UK's Nuclear Security Culture Programme (NSCP), implemented by a King's College London (King's-) led, academia-industry consortium and managed by the Department for Business Energy and Industrial Strategy (BEIS). Other consortium members include Nuclear Transport Solutions - a nuclear transport specialist; and Amport Risk - a specialist nuclear security and resilience consultancy. The authors are grateful for the support provided by UK government under this programme and to the interviewees from the four organisations under study: International Nuclear Services (INS); Direct Rail Services (DRS); EDF Energy; and Radioactive Waste Management (RWM). Thanks also to Amport Risk for facilitating interviews and to Hannah Mulvey, Sally Horspool and Amelie Stötzel for their help in producing the handbook.

Overview & Executive Summary

Overview & Executive Summary

> "THE IMPORTANCE OF THE HUMAN FACTOR WHEN IT COMES TO SECURITY PLANNING, MAINTENANCE, OPERATION AND TESTING IS NOW WIDELY RECOGNISED"

This handbook provides new practical insights into efforts to strengthen the human factor within nuclear security systems, through exploring how security culture programmes have been established within different nuclear organisations. The importance of the human factor when it comes to security planning, maintenance, operation and testing is now widely recognised, with the International Atomic Energy Agency (IAEA) noting that weaknesses in this area are 'generally a contributor to all nuclear security-related incidents.'[1] Through a series of real-life case studies this handbook seeks to identify the challenges that are likely to be faced in implementing nuclear security culture programmes and the various approaches that can be taken to overcome these. The analysis presented draws on interviews, conducted over a period of 15 months, with over 20 practitioners from four UK-based nuclear companies.[2]

Efforts have been made to ensure that each case study is as comprehensive as possible, although it should not be assumed that every facet of security culture is covered within them. Similarly, while a number of good practices are identified within the cases, care should be taken when applying these more broadly. It is essential to consider how these may need to be modified in order to be effectively translated into different national and organisational contexts. Also included within the handbook are actual examples of security culture-related resources developed by some of the companies under study. It is hoped that these will provide inspiration and guidance for others looking to develop and launch such programmes.

Despite significant differences in terms of the size, history and type of operations of the organisations featured in this handbook, a number of common themes have emerged. These relate both to the intrinsic challenges faced in establishing nuclear security culture programmes and essential elements that underpin their successful development. These are summarised briefly below:

[1] International Atomic Energy Agency, Nuclear Security Culture: Implementing Guide, IAEA Nuclear Security Series No.7 (Vienna, 2008), p. 5.

[2] The organisations that took part in this study were EDF Energy, Radioactive Waste Management (RWM), International Nuclear Services (INS) and Direct Rail Services (DRS). In February 2021, INS and DRS were merged into a new business, Nuclear Transport Solutions (NTS).

Common themes

- Obtaining high-level organisational buy-in and engagement at the Executive and Board levels is an essential step in the development of effective and sustainable nuclear security culture programmes. Here, organisations should consider establishing a security-focused executive position and incorporating security targets into corporate milestones. Effective messaging and communication at these levels is best achieved through framing security initiatives in terms of business requirements and broader risk-management.

- It is common in nuclear organisations for security to lag behind safety in terms of prominence and staff engagement, with safety culture typically being a more established concept. Thankfully, safety and security culture have a common basis and similar methods and approaches exist for both their assessment and promotion. This overlap should be exploited by organisations looking to achieve parity across these two areas through, for example, joint awareness-raising and training activities, and the extension of relevant safety-related systems to include security.

- The value of nuclear security can be difficult to articulate, particularly within organisations that have never experienced a serious security-related incident. This may result in security being perceived at different levels as either an unnecessarily expense or an obstacle to conducting core business activities. To overcome this, efforts should be made to 'demystify' security, making it relatable to different occupational groups. Such efforts should include targeted training and engagement, which explore security issues in different working environments, drawing as appropriate on real-life nuclear and non-nuclear incidents.

- There is clear benefit to creating the conditions for active and continuous two-way dialogue on security issues with staff at all levels to encourage buy-in and develop innovative solutions, which balance security concerns with operational efficiency. This can be achieved through a mix of engagement strategies, ranging from large workshops to smaller working groups, allowing for detailed discussion regarding the integration of security into different working processes.

- In undertaking security-related awareness-raising and training, emphasis should be placed on variety, with resources also refreshed regularly so that they don't become stale. Ideally these resources should be easily digestible and relatable, promote lateral thinking and avoid jargon. Where possible, it is also valuable to include an interactive element, which might range from short multiple-choice quizzes or scenario-based discussions to detailed red-teaming, Tabletop exercises, where participants are asked to play the role of the adversary.

- The regular benchmarking of nuclear security culture within an organisation is an essential step in ensuring that the security systems in place will defend against the full spectrum of threats. It is also important in informing the development of future security culture-related initiatives. Methodologies for the self-assessment of nuclear security culture have been developed by the IAEA and others, that can be adopted and tailored to different environments. In addition, organisations can benefit from implementing short security-related checks on a more regular basis, for example through ad hoc challenges and cyber penetration testing exercises.

Before providing the detailed case studies, the handbook continues with a brief exploration of nuclear-related threats and associated security approaches, considering their evolution over time. This is followed by an introduction to nuclear security culture, starting with its genesis in nuclear safety before outlining the IAEA model for nuclear security culture and associated guidance.

Evolving threats and approaches to nuclear security

Concerns over the security of nuclear materials date back to the very start of the nuclear age. Initially focused on acts of state-sponsored espionage, these have since broadened to include terrorist groups, criminal organisations and other non-state actors. Traditionally, approaches to strengthening nuclear security were focused on improving physical protection, in defence against external adversaries, summed up in the classic formula of 'guns, guards and gates.'[3] However, priorities have shifted over time, driven by a growing recognition that these elements alone are unlikely to be effective against the full spectrum of today's threats.

One area of particular concern is the risk posed by 'insiders' – individuals with both malicious intent and authorised access to nuclear assets, who have the knowledge, access and authority to bypass and defeat many of the traditional elements of physical and other security systems.[4] Studies have shown that insiders represent the greatest threat to security across a range of industries.[5] In an effort to tackle insider threats, a growing emphasis has been placed on personnel-focused security measures, designed to mitigate the risk of insiders 'exploiting their legitimate access to an organisation's assets for unauthorised purposes.'[6]

To be effective, the application of protective, but in particular, personnel measures requires the active involvement of staff far beyond the core security team. This includes those who may be employed in operational, technical, management, administrative and other roles. It is often these individuals who will be best placed to observe significant changes in a colleague's behaviour and/or identify non-routine acts that may be malicious in nature. They are also well placed to observe possible weaknesses in how co-workers are implementing security and to encourage corrective action.

This whole-organisation approach to security, where all personnel take an appropriate degree of responsibility, has been promoted in the nuclear industry and other sectors through the concept of security culture. Achieving an effective organisational culture of security can be far from straightforward. Indeed, scholars have detailed a number of serious incidents which demonstrate how weak security practice by both security and non-security personnel is a relatively common occurrence.[7]

[3] William Tobey, 'Planning for Success at the 2014 Nuclear Security Summit', Stanley Foundation Policy Analysis Brief https://stanleycenter.org/wp-content/uploads/2019/09/TobeyPAB1213a.pdf (December 2013), p. 5.

[4] Matthew Bunn and Scott D. Sagan, 'A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes,' (Cambridge, Mass.: American Academy of Arts and Sciences, 2014), p.1.

[5] Bruce Wimmer, Business Espionage: Risks, Threats, and Countermeasures (Butterworth-Heinemann, March 2015), p. 85.

[6] 'Personnel and People Security', Centre for the Protection of National Infrastructure, https://www.cpni.gov.uk/personnel-and-people-security, website accessed 28th April 2020.

[7] Matthew Bunn and Scott D. Sagan, Insider Threats (Cornell Studies in Security Affairs, 2017) pp. 1-216.

Nuclear security culture: Genesis, IAEA model and guidance

Efforts to understand the relationship between human factors and nuclear operations dates back many decades. Initial work in this area drew on the field of human factors engineering, with a focus on ensuring safe operations. It was recognised that 'as large-scale human-machine systems become more complex, and as automation plays a greater role, accidents are increasingly attributed to human error.'[8] This work gained considerable momentum in the 1970s and 1980s as a result of the high-profile nuclear accidents at Three Mile Island and Chernobyl. Human error relating to both design and operation were found to be key causal factors behind both incidents,[9] and these events resulted in a concerted international effort to establish a 'safety culture' in all nuclear facilities.[10] This key concept was promoted by the International Atomic Energy Agency (IAEA), who developed detailed guidance in support of state efforts to establish this within their nuclear organisations. The IAEA model of nuclear safety culture drew on research in the area of management studies, specifically the work of organisational psychologist Edgar Schein, whose model of organisational culture and leadership formed the basis of this approach.[11]

While the importance of culture was embedded within nuclear safety programmes from the 1980s, it was not until the late 1990s that the concept started to be used in relation to nuclear security. Security culture was included as a fundamental principal in the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM), and three years later was further developed in a dedicated IAEA guidance document.[12] This 2008 IAEA implementing guide explicitly recognised that 'a human factor is generally a contributor to all nuclear security-related incidents.'[13] It also put forward a series of key characteristics, deemed to be important in cultivating a culture that 'leads to more effective nuclear security.'[14] These are organised in a framework which – similar to the IAEA guidance on safety culture – draws on Schein's three-level model for understanding and analysing an organisation's culture.

The IAEA framework for nuclear security culture contains 37 characteristics, which are separated into beliefs and attitudes, principles for guiding decisions and behaviour, management systems, personnel behaviour and leadership behaviour. These are in turn linked to over 200 associated performance indicators, which provide useful guidance for organisations looking to practically cultivate an effective security culture. These indicators are necessarily generic and consequently should be tailored to specific organisations and their needs. Regular benchmarking is also recognised as an important part of any security culture programme, with the IAEA publishing in 2017 additional guidance for organisations on how to self-assess nuclear security culture.[15] Related

[8] Thomas B. Sheridan, 'Risk, Human Error, and System Resilience: Fundamental Ideas,' Human Factors: The Journal of the Human Factors and Ergonomics Society (2008), Vol.50, No.3, p.418.

[9] 'Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident,' Report by the International Nuclear Safety Advisory Group, Safety Series No.75-INSAG-1, International Atomic Energy Agency, Vienna, 1986, p.9

[10] 'Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident,' p.76.

[11] Edgar H. Schein, Organizational Culture and Leadership (San Francisco: Jossey-Bass, 1985).

[12] International Atomic Energy Agency, Nuclear Security Culture: Implementing Guide, IAEA Nuclear Security Series No.7 (Vienna: International Atomic Energy Agency, 2008).

[13] Ibid., p.5.

[14] International Atomic Energy Agency, Nuclear Security Culture: Implementing Guide, IAEA Nuclear Security Series No.7 (Vienna: International Atomic Energy Agency, 2008), p. 19.

[15] International Atomic Energy Agency, Self-assessment of Nuclear Security Culture in Facilities and Activities, Nuclear Security Series No. 28-T (Vienna, 2017) https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf

security culture enhancement guidance is also under development by the IAEA.[16]

Other international and national bodies, such as the World Institute for Nuclear Security (WINS) and the UK's Centre for the Protection of National Infrastructure (CPNI), have also developed information and tools for organisations embarking on security culture programmes.[17] These and the aforementioned IAEA guidance are now being utilised by a significant number of nuclear organisations around the world. However, to date, little information has been shared on challenges encountered in establishing such programmes and how these might be overcome. This handbook attempts to address that gap.

[16] International Atomic Energy Agency, Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and/or Radioactive Material, NST027 Draft Technical Guidance (Vienna, 2016) https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst027.pdf

[17] For example, Nuclear Security Culture – A World Institute for Nuclear Security Best Practice Guide (February, 2019), accessible via http://www.wins.org/ and Key Attributes of an Excellent Nuclear Security Culture, UK Nuclear Industry Safety Directors' Forum (June 2013), accessible via the Nuclear Institute https://www.nuclearinst.com/write/MediaUploads/SDF%20documents/Security/Key_attributes_of_an_excellent_Nuclear_Security_Culture.pdf.

Case Studies

Case study I: International Nuclear Services

Company overview

International Nuclear Services (INS) was a wholly-owned subsidiary of the UK's Nuclear Decommissioning Authority (NDA), specialising in nuclear transport, design and licensing.[18] Formally established in 2008, its origins and nuclear transport experience dated back more than 40 years as the former Spent Fuel Services and Transport Division of British Nuclear Fuels Limited (BNFL), which was restructured in the mid-2000s.[19] INS also managed Pacific Nuclear Transport Limited (PNTL), a subsidiary company, which operates a fleet of ships that are dedicated to the long distance transportation of nuclear material by sea, conducting approximately 200 shipments over the past four decades.[20] INS has sought to offer its customers 'extensive and proven expertise in irradiated fuel management and transporting nuclear materials.'[21]

In February 2020, the NDA announced that it was simplifying its transport and logistics operations, 'bringing together responsibility for transport and packaging, along with the operational, commercial, engineering, legal, and regulatory expertise that underpin nuclear transport and logistics, into one division.'[22] This involved an effective merger of INS and its PNTL subsidiary with Direct Rail Services (DRS), a separate NDA subsidiary organisation that transports nuclear material by rail, which is explored in a separate case study in this handbook. In early 2021, INS and DRS became part of the newly formed Nuclear Transport Solutions (NTS).[23] This INS case study, supported by interviews conducted in late 2019, seeks to understand how nuclear security culture was developed at INS in recent years, before its 2021 merger. It explores both the challenges encountered and relevant initiatives that were launched in this area.

Operational environments and security risks

INS implemented nuclear security in three major operational environments: its offices; ships which transport nuclear material; and the associated docks and berthing facilities. These had widely varying attributes and consequently, it was necessary for INS to consider a broad range of potential threats, possible targets and security solutions. For example, INS' offices had a largely administrative function – with staff overseeing the company's operations, as well as managing central services such as information technology, human resources and finance. Consequently, in this environment considerable attention was placed on information and cyber security, protecting key operational details (i.e. the timings and locations of shipments), as well as sensitive personnel-related and financial information. At vessels and docks, additional onus was placed on physical security measures, which had to protect not just sensitive information and systems but nuclear material from theft or sabotage.

[18] 'Our Heritage', International Nuclear Services, https://www.innuserv.com/our-heritage/ (Website accessed 26th June 2020); In April 2021 INS became part of Nuclear Transport Solutions (NTS) and is consequently referred to in this handbook in the past tense, although many of the vast majority of security systems and processes developed by INS will form part of NTS approach to security https://nucleartransportsolutions.com/ (Website accessed 8 February 2021).

[19] 'Nuclear Development in the United Kingdom', World Nuclear Association, https://www.world-nuclear.org/information-library/country-profiles/countries-t-z/appendices/nuclear-development-in-the-united-kingdom.aspx (October 2016)

[20] 'About us', Pacific Nuclear Transport Limited, https://www.pntl.co.uk/about-us/ (Website accessed 26th June 2020); Please note PNTL is owned by the UK's INS (68.75%), France's Orano (formerly Areva: 12.5%) and a consortium of Japanese nuclear companies (18.75%).

[21] International Nuclear Services, https://www.innuserv.com/ (Website accessed 26th June 2020).

[22] 'The NDA will bring its transport and logistics expertise together', GOV.UK, https://www.gov.uk/government/news/the-nda-will-bring-its-transport-and-logistics-expertise-together (4th February 2020)

[23] Nuclear Transport Solutions (NTS) https://nucleartransportsolutions.com/ (Website accessed 8th February 2021)

Major challenges encountered

The diversity of operating environments and wide range of individuals employed at INS presented an intrinsic challenge for fostering an effective nuclear security culture across all working environments. Although a relatively small company of several hundred employees (150 at INS; 150 at PNTL), staff were drawn not just from the UK's nuclear estate but also from the maritime sector and, as such, they may have entered the company with very different experiences with regards to security and a range of threat perceptions. For example, individuals coming from the maritime sector will typically have focused on security in relation to criminality and piracy, while those from remote UK nuclear sites may have yet to experience a serious security incident. Consequently, significant time was devoted to raising awareness amongst staff of the full range of malicious actor threats and how they may manifest across INS operations.

When shipping nuclear material INS had to take into account, even over the course of a single journey, changes to both the threat environment and to nuclear and maritime regulations, as different national waters are transited.[24] This can result in tensions if maritime and nuclear regulations misalign or security and operational issues conflict. For example, while it is standard maritime practice to openly transmit navigational information, this may present a significant security risk given the cargo that INS ships are carrying. In terms of resolving regulatory issues INS helped facilitate dialogue between the Maritime and Coastguard Agency (MCA) and the Office of Nuclear Regulation (ONR), resulting in a Memorandum of Understanding (MoU). This helped facilitate collaboration between regulators in common areas, while also clarifying who has primacy in different scenarios, serving to enhance command, control and communication with respect to security.

More broadly, and as will be discussed in detail in the next section, recent efforts by INS to strengthen nuclear security culture took place during a shift in UK nuclear security regulation. This regulatory change, which required a new approach to security at the organisational level, presented certain challenges for the INS security team. A particular challenge related to changing what for some individuals was a deeply ingrained approach to security, which had been built up over decades of working in the UK nuclear sector under the former regulatory regime.

Strengthening security culture during a regulatory transition

In recent years, INS' efforts to strengthen nuclear security culture internally have been intertwined with a shift in UK nuclear security regulation from prescriptive to outcome-focused Security Assessment Principles (SyAPs).[25] Under this new regulatory regime UK nuclear licensees must justify their security measures in relation to assessed threats, rather than aim to meet prescribed standards. These changes allow licensees greater latitude in tailoring security solutions to risks and were welcomed by the INS security team as a positive development. As noted by the Head of Security at INS, a former nuclear security regulator, the new system allows "Regulators to be regulators again, as opposed to security advisors".[26]

[24] 'Presentation by Ben Whittard', World Institute for Nuclear Security, https://www.youtube.com/watch?time_continue=2770&v=885S25ZoFvo&feature=emb_logo (5 June 2020)

[25] Introducing new SyAPs security plans, Office for Nuclear Regulation, http://news.onr.org.uk/2018/11/introducing-new-syaps-security-plans/ (13th November 2018).

[26] Security Manager, Interview with the authors, 9th December 2019.

Recognising that this regulatory transition would require a significant reshaping of how INS approached nuclear security, the security team engaged the Executive early on in the process to gain the necessary high-level buy-in and support.[27] This was achieved by emphasising not just the potential security benefits but also the likely cost savings and leadership role that INS could play by actively embracing this change. After obtaining the backing of the Executive, the INS security team "Reviewed everything from physical protection systems to information security to training and tactics".[28] Ultimately, this approach proved effective with INS becoming the first member of the UK's nuclear estate to have a SyAPs plan approved by the ONR in April 2017.[29] At the end of 2017, INS achieved the lowest-level of nuclear security regulatory focus, reducing the frequency of regulatory inspections and their associated costs.[30] This was granted thanks to a demonstrably robust security programme, focused on continuous improvement, which had been positively assessed at every ONR regulatory intervention.

Promoting buy-in through active engagement

To help ensure INS' new approach to security under SyAPs would be both operationally effective and widely accepted, an extensive outreach campaign was launched to solicit viewpoints from across the entire business. To this end, individuals from all functional areas were approached and asked to feed into the re-drafting of INS' security plan and policies in an effort "Not just to keep the regulator happy", but to ensure their effectiveness and encourage a broader sense of security ownership and buy-in amongst different stakeholders.[31] A significant amount of this work took place in small working groups, involving approximately five to 10 employees from different departments, so that the company-wide implications of new security measures could be fully assessed. Working groups provided a useful forum for gathering critical feedback from beyond the security team on new security procedures, allowing for the early resolution of potential problems and reducing the future likelihood of non-compliance. In addition to the small working groups, a series of larger workshops were held to explain the changes, discuss the broader involvement of INS staff in security and address any concerns that individuals might have.

These engagement mechanisms provided detailed insights into how different parts of the business interacted with security and hence what effective solutions might look like. Here care was taken to ensure that sensitive assets were protected, without unduly inhibiting operations. Engagement mechanisms also served to increase overall understanding of security and its importance throughout the company. This approach represented a marked change to how the security team interacted with staff and how security-related information was communicated within INS. As noted by some interviewees the security team previously used to be physically separated and had only relatively limited one-way interaction regarding security with individuals from other parts of the business.[32] Under the new approach, rather than simply presenting security measures and how they should be followed, far greater emphasis was placed on a two-way discussion with the security team in an effort to ensure staff understood "Why policies are the way they are".[33] This was deemed to be particularly effective in helping middle management understand the purpose of new regulations and INS' evolving security approach, which they could then effectively relay to their teams. More broadly, the 'root and branch reform' served to help the security team at INS develop stronger working relationships with key individuals across the business.

[27] Security Officer, Interview with the authors, 9th December 2019.
[28] Security Manager, Interview with the authors, 9th December 2019.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Security Officer, Interview with the authors, 9th December 2019.
[33] Ibid.

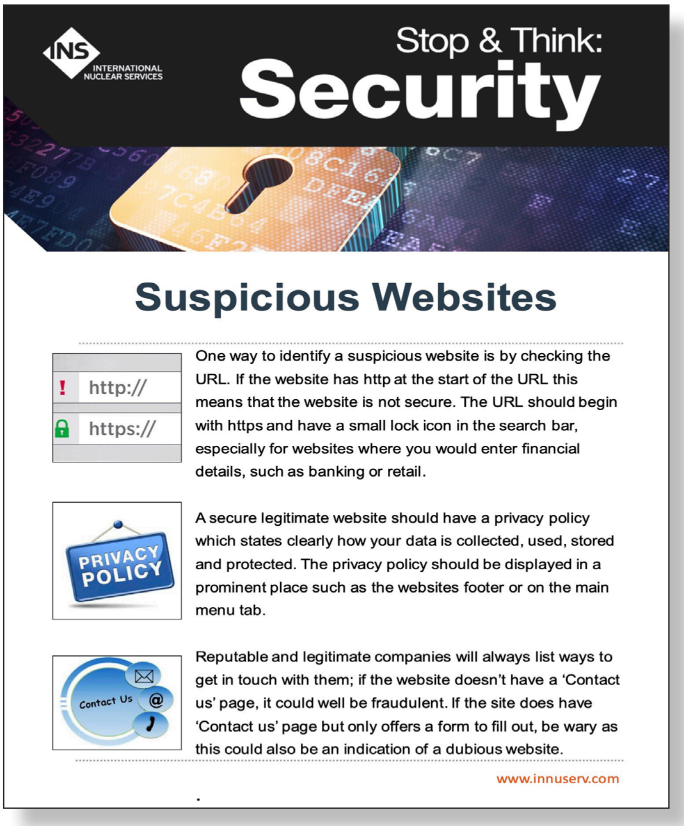
This approach was deemed to be particularly effective with respect to the shipping teams, whose physical separation from the corporate security team had previously limited levels of interaction. Under the new regime, the security team regularly engages with crews, gaining a deeper insight into what measures work and what needs improvement. This was received positively by the shipping teams who "Have more say in terms of what goes on now", which helps in terms of fostering buy-in and developing innovative security solutions drawing on their specialist expertise.[34] Feedback to the security team can be critical, particularly where new measures may impact safety or operations. An example provided involved the planned installation of new security equipment to a ship's bridge. Following an initial trial, it was discovered that this would have a significant negative impact on ship operations, which led to a redesign with increased input from the shipping team's operational experience.

Nuclear security leadership

As discussed previously, by actively embracing the change in regulatory approach with respect to nuclear security, INS was able to demonstrate leadership within the NDA and broader UK nuclear estate. Nuclear security is now explicitly represented on the INS Executive Board with the establishment of a new Director of Safety, Security & Environment (SSE) in 2020. This helped in maintaining a strong focus on security at the executive level, ensuring security is regularly discussed which helps to promote broader organisational buy-in.

Security was also represented in corporate milestones, with the senior team at INS accountable for turning these into individual goals and metrics, which are related to staff bonuses. For example, recent milestones included aligning INS' Information and Communications Technology (ICT) programme with the NDA's Cyber Security Programme and conducting a nuclear security culture assessment exercise, using the Centre for the Protection of National Infrastructure's (CPNI) SeCuRE 4 survey-based toolkit.[35]

INS also appointed a Security Culture Manager who was responsible for a wide of range of activities aimed at ensuring that security was understood and prioritised within different groups. These activities included awareness-raising, training and regularly gauging staff members attitudes and behaviours in relation to security, by using questionnaires and focus groups.



INS
INTERNATIONAL NUCLEAR SERVICES
! http://
https://
PRIVACY POLICY
Contact Us

Stop & Think:
Security

Suspicious Websites

One way to identify a suspicious website is by checking the URL. If the website has http at the start of the URL this means that the website is not secure. The URL should begin with https and have a small lock icon in the search bar, especially for websites where you would enter financial details, such as banking or retail.

A secure legitimate website should have a privacy policy which states clearly how your data is collected, used, stored and protected. The privacy policy should be displayed in a prominent place such as the websites footer or on the main menu tab.

Reputable and legitimate companies will always list ways to get in touch with them; if the website doesn't have a 'Contact us' page, it could well be fraudulent. If the site does have 'Contact us' page but only offers a form to fill out, be wary as this could also be an indication of a dubious website.

www.innuserv.com

FIGURE 1: STOP AND THINK CAMPAIGN POSTER: 'SUSPICIOUS WEBSITES'
COPYRIGHT: CPNI / NTS

[34] Shipping Team Staff Member, Interview with the authors, 9th December 2019.
[35] SeCuRE 4: Assessing Security Culture, Centre for the Protection of National Infrastructure https://www.cpni.gov.uk/secure-4-assessing-security-culture (Website accessed July 2020).

Awareness-raising and training

INS undertook a wide range of internal security-related awareness-raising and training activities. This included an induction course, which covered a wide variety of security-related scenarios and a tour of an INS vessel, even for individuals in office-based roles, so that all staff could better visualise the maritime operating environment and the associated risks. In delivering security-related training, variety was seen as extremely important to ensure that employees did not become tired of the material presented. Efforts were also made to promote lateral thinking by placing staff in the mind of the adversary, for example, by asking staff to consider the relevance of vraious information about INS from a hacker's perspective. Emphasis was also placed on security-related information and training being easily digestible and relatable. For example, the security newsletter that used to be more than 10 pages in length was condensed to a single page, with links to useful further reading. Furthermore, large company security briefings involving hundreds of people were minimised and replaced with smaller, more tailored meetings for different occupational groups.

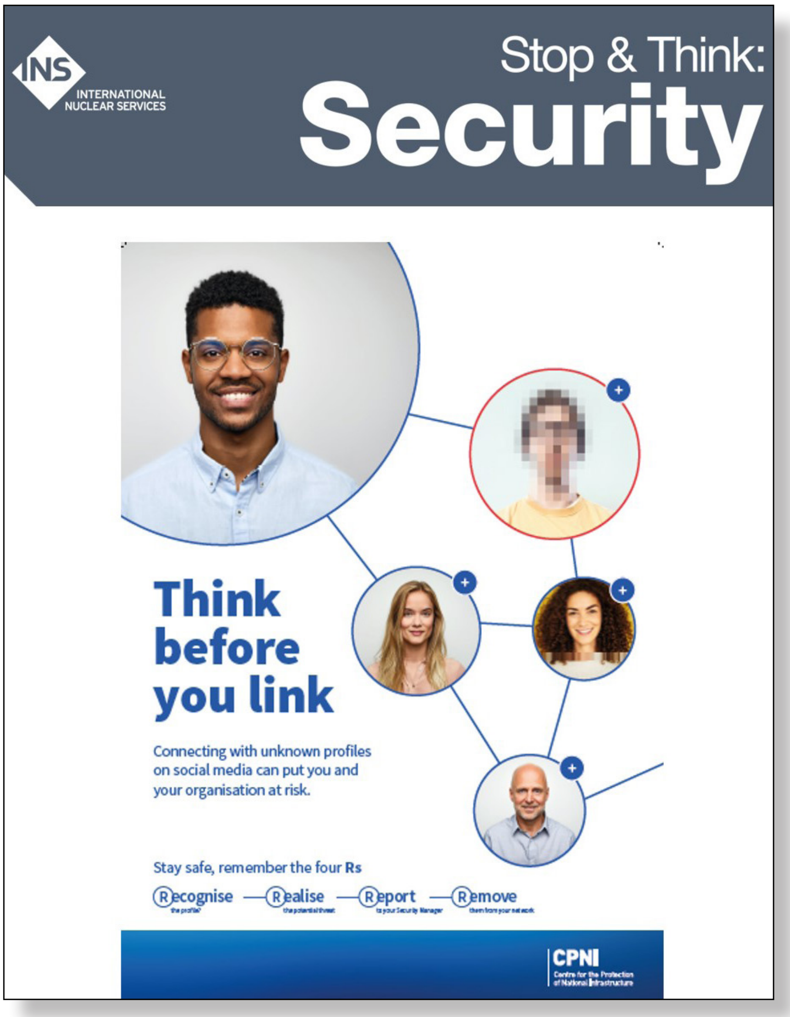

INS
INTERNATIONAL NUCLEAR SERVICES
Stop & Think:
Security
Think before you link
Connecting with unknown profiles on social media can put you and your organisation at risk.
Stay safe, remember the four Rs
Recognise the profile?
Realise the potential threat
Report to your Security Manager
Remove them from your network
CPNI
Centre for the Protection of National Infrastructure

FIGURE 2: STOP AND THINK CAMPAIGN POSTER: 'THINK BEFORE YOU LINK'
COPYRIGHT: CPNI / NTS

In addition to mandatory security training, a wide range of optional sessions were developed for staff. This included short 30-minute sessions delivered over lunchtimes, known as 'Bite Size Briefings' which were used to transmit key corporate messages, including those relating to security.[36] These were developed in response to staff feedback, which revealed that full afternoon briefings were too long and poorly attended. Here, recent security-related 'Bite Size Briefings' have included sessions on cyber security, insider threats and information classification and control. These topics were initially identified by staff as key areas around which they would be keen to further their understanding. Sessions were typically designed around specific scenarios or real-life examples and included opportunities for questions and answers. Care was taken to remove jargon and consider the application of key security concepts in different settings to make them relatable. Delivered in a similar manner to the aforementioned 'Bite Sized Briefs' were 'Security Focus Groups' targeted at managers. Initially held to explore the implications of SyAPs, they were then extended to a range of different topics. These lasted between one and two hours and had strong interactive elements, such as role-playing different security-related scenarios. Typically, these were limited to no more than 12 attendees to ensure active participation, with attendees selected from across the business and from different managerial levels.

[36] Human Resources Staff Member, Interview with the authors, 9th December 2019.

Where appropriate, in developing security engagement activities, INS also sought to incorporate relevant national level guidance and resources. For example, the UK's Centre for the Protection of National Infrastructure (CPNI) 'It's OK to Say' educational programme.[37] In addition to the materials developed by CPNI, the INS security team produced a short video on behavioural observation and reporting, as well an associated quiz which took staff just 10 minutes to view and complete. This was completed by over 80% of INS staff, with this high uptake reflecting its short form and flexible delivery; staff were able to watch the video and complete the quiz in their own time.[38]

Recognising that the need for security does not stop at the company gates and that staff could unwittingly reveal sensitive information outside of working hours and the workplace, the INS security team also placed emphasis on the handling and communication of sensitive information at both work and home. This included awareness-raising on the wide range of potentially security-relevant information and how this should be protected, for example, through limiting work-related discussion on social media or considering what company information can be stored on mobile devices. This targeted outreach resulted in an increase of requests about how to mitigate against these potential vulnerabilities, for example by using two-factor authentication on all devices.

Before heading to sea, INS crews took part in a detailed training exercise in which they had to respond to a range of possible threats. This involved all crew, not just senior staff, to emphasise that everyone has a part to play in a real emergency, even if it was just assembling in a particular area. Prior to this, staff would undertake a Maritime Integration Training (MIT) Exercise – which involved at least half a day of security training including one to two hours of role-playing, encompassing realistic scenarios (including insiders and external adversaries) and interjects from a directing team. Prior to conducting operations involving nuclear material, INS also engaged with the UK's Royal Navy who provided training on defensive strategy and techniques while at sea, and regular updates on the changing maritime risk environment. This included live weapon firing as part of different scenarios, which was assessed from a regulatory perspective, with the Royal Navy also acting as observers.

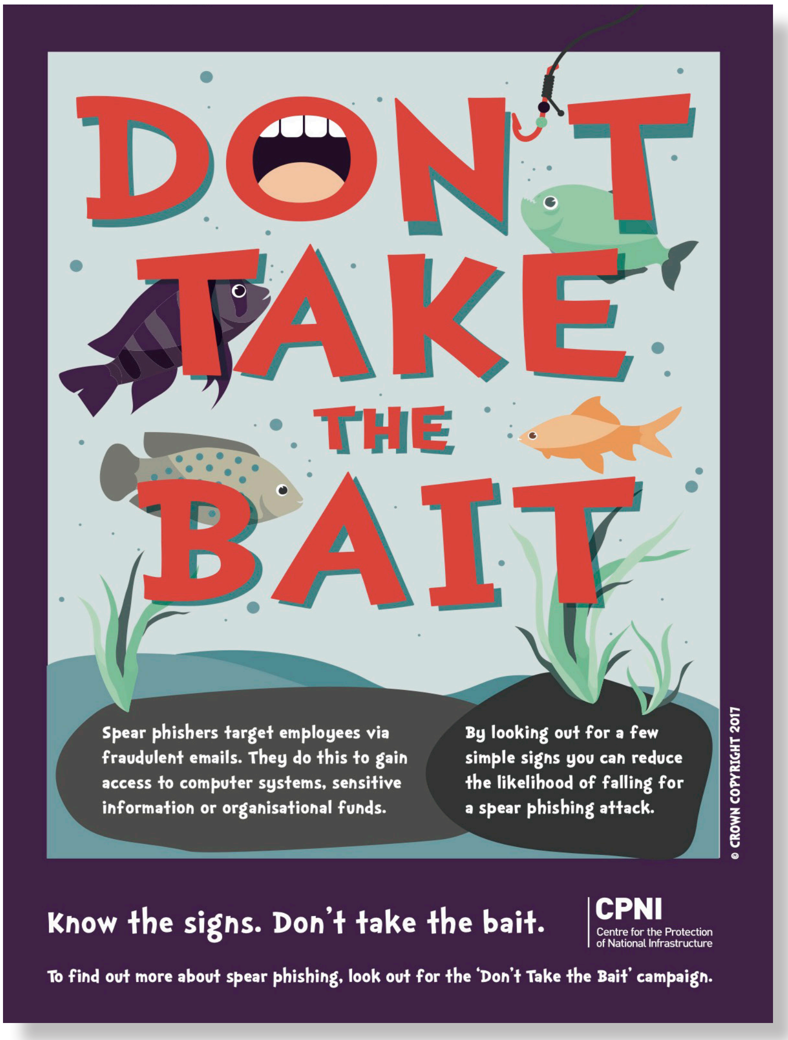

DON'T TAKE THE BAIT
Spear phishers target employees via fraudulent emails. They do this to gain access to computer systems, sensitive information or organisational funds.
By looking out for a few simple signs you can reduce the likelihood of falling for a spear phishing attack.
© CROWN COPYRIGHT 2017
Know the signs. Don't take the bait.
CPNI
Centre for the Protection of National Infrastructure
To find out more about spear phishing, look out for the 'Don't Take the Bait' campaign.

FIGURE 3: ANTI-PHISHING CAMPAIGN POSTER: 'DON'T TAKE THE BAIT'

COPYRIGHT: CPNI

[37] 'It's OK to say educational programme', Centre for the Protection of National Infrastructure https://www.cpni.gov.uk/its-ok-to-say-education-programme (Website accessed 4th July 2020).
[38] In an effort to further increase its appeal, security staff also included humorous outtakes at the end of the video.

Security testing, challenge and accountability

A wide range of security testing mechanisms were employed by INS to identify potential issues and improve compliance with different measures. This included ad hoc challenges, for example, intermittent random checks of staff ID passes to ensure these were up-to-date and being used appropriately. These types of quick security checks took place in addition to more formal annual evaluations of different security systems, to mitigate the risk of complacency. In terms of cyber security, monthly penetration testing exercises were performed. These might have included, for example, the creation and dissemination of realistic phishing material to a sub-set of the INS workforce. This was varied every month in an effort to ensure that exercises remained effective at identifying potential weaknesses. If these testing campaigns revealed significant issues, then additional training was provided to further educate staff on cyber security risks and how these may manifest in their working environment.[39] At a more informal level, INS sought to promote a 'culture of positive challenge,' framing certain security measures as looking after staff, in terms of a broader 'arms around' approach.[40] For example, in implementing clear desk policy, the last person leaving was encouraged to take extra care and look around their broader area for any items left out. Human resources also made themselves available for staff should they need to discuss personal issues that might impact on their work.

These approaches helped inform expectations, both individually and collectively. One interviewee noted how there "Used to be more of a blame culture [at INS]", but staff are now proactively engaging with security measures in an effort to ensure greater compliance as they are, "Doing it for each other".[41] In addition, INS sought to intertwine security with a broader working culture that emphasised the importance of being attentive and accountable. There were also efforts to increase equality, diversity and inclusion (ED&I) to gather input from a greater variety of voices from within the company, with one interviewee noting that INS had worked hard to develop an "open sharing culture", noting that "it wasn't always like this".[42]

Security was also incorporated into annual appraisals for all staff, who were required to complete a dedicated Security Appraisal Form (SAF). This was filled in by both employees and their line managers and provided to the security team, who subsequently flagged and investigated any issues or inconsistencies. Security-related questions were also added to INS' broader monthly review, where operational goals were assessed. This enabled the regular gathering of data on employees' attitudes and behaviours with respect of security, helping identify potential warning signs in advance so that corrective action could be taken. In addition, shipping teams were required to complete a security-specific self-assessment after each crew rotation (on average six times a year), which provided information on their competence across different security areas. This went beyond the annual regulatory requirement but was deemed useful by INS in troubleshooting potential issues and reinforcing the importance of security amongst all staff.

Following a security infraction, the initial step involved a conversation with the individual and their line manager, with the violation and actions taken recorded by the security team. Depending on the severity of the breach, this might have ranged from simply showing the individual what errors were committed, to re-training or a formal investigation. In the event that violations continued, the security team would have become directly involved to further reinforce the message. If this failed to have an impact then extreme cases would be escalated to Human Resources, with possible outcomes

[39] Security Officer, Interview with the authors, 9th December 2019.
[40] Human Resources Staff Member, Interview with the authors, 9th December 2019.
[41] Operations Staff Member, Interview with the authors, 9th December 2019.
[42] Human Resources Staff Member, Interview with the authors, 9th December 2019.

including suspension or dismissal of the individual in question. In general, discussions around security violations were at least initially framed sympathetically to emphasise the benefits of positive behaviour "Rather than trying to berate people".[43] Care was taken to ensure that these processes were applied consistently across INS, with clear messaging that managers were not given special treatment. Not all measures aimed at promoting compliance with security measures were punitive; individuals were also rewarded for making an active effort to promote security or flag potential issues. Rewards included entry into a draw for a voucher, or verbal recognition at team meetings, the latter of which was the preferred option for the majority of staff interviewed.

Security-related reporting and other initiatives

Despite efforts to create an open and transparent working environment, it was recognised that there may be occasions where staff did not feel comfortable raising security issues directly with their line manager or the security team. To cater for this, INS operated a 'Safe Steps' scheme, which allowed people to report issues without attribution; this included a communal post-box (called 'Step-Forward') and an email address, which was possible to message anonymously. This scheme was in addition to the security team's 'Secure Behaviours' initiative, whereby employees openly reported on potential security issues, and how security training and other engagement activities could be further improved. It was clear that these mechanisms were utilised, with interviewees noting that several staff had recently reported a malfunctioning turnstile, which was viewed as a form of positive engagement with security.

In addition to Human Resources, staff had access to an Employee Assistance Programme (EAP), which was offered by an independent third party. This was focused on helping employees overcome personal problems that might have adversely impacted their work performance, health and wellbeing, with support offered via email exchanges, telephone calls and a face-to-face meeting. Staff also had access to a wellbeing coach since late 2018. This was a confidential service where staff could have in-depth discussions about challenges at work and at home. This could be accessed individually or in small groups to resolve issues, for example between two employees or an employee and their line manager. More broadly, efforts were made to recognise and de-stigmatise the very real impact of personal issues in the workplace; this included a member of the Executive speaking out about their mental health challenges.

Summary

In recent years, INS has made significant changes to its security programme, with a focus on i ncreasing company-wide engagement. A wide range of initiatives were launched to this end to raise awareness of security, identify staff needs and develop appropriate and engaging training. This took place against a background of a significant shift in nuclear security regulation in the UK, which INS embraced and utilised to gain high-level buy-in for their efforts, while also using this as an opportunity to re-develop certain security measures and processes, with input from different occupational groups to increase their effectiveness. These developments appeared to have been welcomed by INS staff who described a more open and transparent working environment where it was possible to raise security issues and concerns without fear of retribution and engage in productive two-way discussions with the security team.

[43] Ibid.

Case study II: Direct Rail Services

Company overview

Direct Rail Services (DRS) was a specialist rail freight company that transported nuclear material between nuclear sites in the UK.[44] Established in 1995 by British Nuclear Fuel Limited to handle nuclear material movements, ownership of DRS was transferred in 2005 to the UK's Nuclear Decommissioning Authority (NDA).[45] It was one of a handful of government-owned rail companies in the UK.[46] In February 2020, it was announced that DRS was to be merged with the remainder of the NDA's transport and logistics portfolio, 'to simplify structures across the group,' and in April 2021 it became part of the newly-created Nuclear Transport Solutions (NTS).[47] Over the years, DRS had diversified its business into other areas – transporting large quantities of non-nuclear intermodal freight and providing services to other industries.

Interviews in support of this study were conducted in early 2020, before DRS' integration within the larger NDA infrastructure portfolio was announced. During this period, the company had an annual turnover of £80 million a year and employed more than 450 people, moving nuclear material by rail most days.[48] Despite diversifying its business to include non-nuclear goods and services, DRS was continuously guided by a 'Nuclear-First' strategy, meaning that the nuclear aspects of the business always took priority, and other aspects could only be rationalised if they did not detract from this mission.[49] Nuclear movements constituted a minor part, approximately 5% of DRS' freight movements, but represented 48% of the company's turnover.[50]

Operational environment and security risks

Ensuring the security of nuclear material while in transport presents a significant challenge. For many, this is the point when nuclear material is at its most vulnerable to theft or sabotage, as it is outside of the layered physical protection systems provided by fixed nuclear sites.[51] Nonetheless, the movement of nuclear materials by rail can arguably be more easily secured than via road, given that railways are for the most part already separated from the public by fences and other physical security infrastructure. Rail shipments also typically involve moving material in containers that weigh many tens of tons, which provides an intrinsic barrier to theft. However, these positives are countered by the predictability of rail movements, which are made public in railway timetables, and by the prevalence of hobbyist train enthusiasts, which may also provide potentially useful information for would-be adversaries.[52]

[44] In April 2021 DRS became part of Nuclear Transport Solutions (NTS) and is consequently referred to in this handbook in the past tense, although many of the vast majority of security systems and processes developed by DRS will form part of NTS approach to security https://nucleartransportsolutions.com/ (Website accessed 8 February 2021).
[45] 'About DRS', Direct Rail Services, https://www.directrailservices.com/about-us/ (Website accessed 30th June 2020).
[46] Other nationalised rail companies in the UK include passenger services NI Railways, LNER and Northern Trains, and Network Rail, which owns and operates rail infrastructure.
[47] 'DRS incorporated into NDA's transport portfolio', Rail Magazine, https://www.railmagazine.com/news/network/drs-incorporated-in-to-nda-s-transport-portfolio (10th February 2020); Nuclear Transport Solutions (NTS) https://nucleartransportsolutions.com/ (Website accessed 8th February 2021)
[48] 'About DRS', Direct Rail Services, https://www.directrailservices.com/about-us/ (Website accessed 30th June 2020)
[49] Compass, Direct Rail Services, Issue 14, https://www.directrailservices.com/PDF/Compass14.pdf (Spring 2018)
[50] Business Director, Direct Rail Services, Interview with authors, 23 January 2020.
[51] Fact Sheet: Nuclear Transportation Security, published by The White House 6 April 2016, Available at: http://www.nss2016.org/document-center-docs/2016/4/1/fact-sheet-nuclear-transportation-security
[52] 'Terrorism Fear Derails Train-Spotters,' BBC News, http://news.bbc.co.uk/1/hi/uk/2943304.stm (28th May 2003).

For DRS, security also encompassed a wider range of assets and activities than might be found in other nuclear organisations. As well as nuclear materials and sensitive information, commercial goods such as alcohol, cigarettes and other products that were transported for supermarkets also had to be protected. These shipments may have presented a more attractive target for a far wider range of would-be adversaries than for nuclear assets, although theft from rail containers in the UK was thankfully rare. According to the British Transport Police, over the last five years, the UK experienced an average of 19 rail-related thefts annually.[53] DRS also had three distinct operational environments to which security was applied including the trains, depots and yards and administrative offices.

Major challenges encountered

The diversity of individuals and working environments at DRS presented a potential challenge to building an effective security culture. In terms of staff, these included three major groups – office workers, maintenance and depot employees and train drivers – who each worked in distinct environments and had different roles to play in ensuring security. Some encountered clear reminders of security on a daily basis – fences with razor wire, armed guards and metal detectors – while for others security was less visible. Staff who joined DRS also came from a wide range of professional backgrounds. For example, while many staff had worked elsewhere in the nuclear industry, others had backgrounds in the rail sector and little to no prior exposure to nuclear risks. In this context, interviews revealed that in general, staff that worked at DRS with non-nuclear backgrounds were initially far more familiar with safety than security issues.

Another key challenge that emerged from the study was the negative perceptions of security that had built up at DRS over the years, with many staff viewing security as an impediment that could serve to limit operations and business development. Historically this had resulted in staff reducing their engagement with the security team out of fear that 'they won't let you do that.'[54] This created a divide between security and non-security personnel, which was further exacerbated by the security team's natural inclination to restrict security-relevant information and their decision-making process. More broadly, this was relatively common practice within the nuclear industry, thanks to a widespread pre-existing culture of secrecy associated with civil nuclear security that developed over time due to the strategic nature of nuclear technology. Other challenges faced by the security team included competing for bandwidth with other issues, such as safety and effectively engaging with operational staff who did not work in a fixed, office-based environment.

Strategy for developing an effective nuclear security culture

To overcome these challenges, the DRS security team recognised that they needed to increase their outreach to staff, provide greater clarity on the need for certain security measures, and where possible, develop a tailored approach to promoting security within the organisation's different occupational groups and working environments. To both reach more people and increase their level of engagement with nuclear security it was also accepted that the engagement mechanisms utilised needed to evolve and be diversified. For example, while sending security instructions and guidance by email was an easy and convenient means of distribution, it was found to be largely ineffective in

[53] Figures provided by British Transport Police, FOI request 637-20.
[54] Operations Officer, Interview with authors, 23 January 2020.

terms of staff pick-up. It was also recognised that responsibility for promoting strong security practice was not just the job of the security team, and that strong relationships needed to be established with other key departments. For example, Human Resources played an important role in processing security-related checks, enforcing compliance and applying security 'after care.'[55] Efforts to emphasise the safety and security aspects of DRS' business subsequently began before individual staff members were hired. For example, key words were inserted into employment adverts to emphasise that DRS was a safe and security-oriented business.

It was also recognised that building an effective nuclear security culture was a continual process and one where it was important to guard against complacency. Security was one of several competing operating principles and, like all companies, staff and management had limited resources at their disposal and could be easily overwhelmed with information. Past experience had shown that delivering security messages over and over in the same way quickly became ineffective. With staff members progressively less likely to internalise requirements and guidance, and more likely to make inadvertent mistakes.

Leadership, organisational structure, oversight and reporting

Historically, security at DRS was managed within a broader compliance function with staff also taking on a variety of non-security roles and responsibilities, including safety. Security was re-organised in 2017 into a dedicated team of approximately 10 individuals, which included specialists in physical security, cyber security and resilience. This team was led by a new Director of Security and Resilience, who reported directly to the DRS Managing Director and Executive Team. This restructuring recognised that the amount of work involved in managing compliance across a range of functional areas could negatively impact the effective implementation of security. Separating out security also helped to demonstrate its importance within the broader business, while providing security-related staff with more focused responsibilities. Representation at the Board level was also deemed to have been beneficial in terms of increasing senior management's understanding of and support for nuclear security. The Board was frequently briefed on evolving risks and mitigation steps, and developed corporate milestones for nuclear security, as well as criteria for demonstrating security improvement.

Following the separation of security from safety, efforts were made to ensure a close working relationship between these two key functional areas. This is important as security will have had to compete with safety for bandwidth from time-to-time, which was a challenge frequently seen in both the nuclear and rail industries. To this end, efforts were made to establish a close working relationship between the Director of Security and Resilience and the Director of Health, Safety, Environment and Quality (HSEQ), who met regularly. Furthermore, the security team often worked in partnership with the safety team, for example to jointly conduct internal safety and security inspections. This had proven beneficial in terms of ensuring regulatory compliance, which could be complex as DRS had multiple regulators including the Office for Nuclear Regulation, the Environment Agency and the Office of Rail Regulation. There are also plans, under NTS, to further increase joint site inspections with personnel from both the safety and security teams. For the added benefit of facilitating joint association by staff between safety and security, reinforcing the perception that safety and security are both equally important and 'two sides of the same coin.'[56]

[55] 'Measurement of Competence', Office for Nuclear Regulation Guide, CNS-TAST-GD-3.3 Revision 1 p. 15 (March 2020) http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-3.3.pdf

[56] Security Officer, Interview with authors, 23 January 2020.

DRS invested significant effort into enhancing provisions for mental health in the workplace. This included training mental health champions and first aiders at multiple levels within the organisation. DRS sought to foster an active culture of discussing this issue, which was seen as beneficial in the early identification of potential safety and security issues. DRS also had access to internal and external security reporting and 'whistle blowing' lines – including the Confidential Incident Reporting and Analysis Service (CIRAS) system, which was used across the rail industry.[57] Established to enable the anonymous reporting of safety issues, this mechanism could also be used to flag potential security concerns, although efforts were made to foster a culture at DRS where reporting was also possible through internal processes.

Awareness-raising and communication

Given the diversity of DRS staff, the security team sought to adopt a flexible and tailored approach to security awareness-raising, utilising a range of different technologies and messaging strategies. Core to this was the continual promotion of DRS' 'safe, secure and reliable' strapline. This featured in workplace posters, as well being displayed on objects around the office such as mouse mats, booklets and other merchandise. It was also found on screensavers and within employees' email signatures. Continually encountering security messaging can – as security staff noted – serve to 'burn it into the brain.'[58] When producing company-wide material (such as posters) care was taken to ensure the messages were easily digestible by staff. Guiding principles included being accessible and user-friendly without including too much information that might overwhelm the target audience. In general, DRS sought to streamline its security-related guidelines and information, writing in plain English and removing jargon. Certain procedures were amalgamated and simplified, while the company's intranet contained a range of easily accessible and user-friendly reference material.

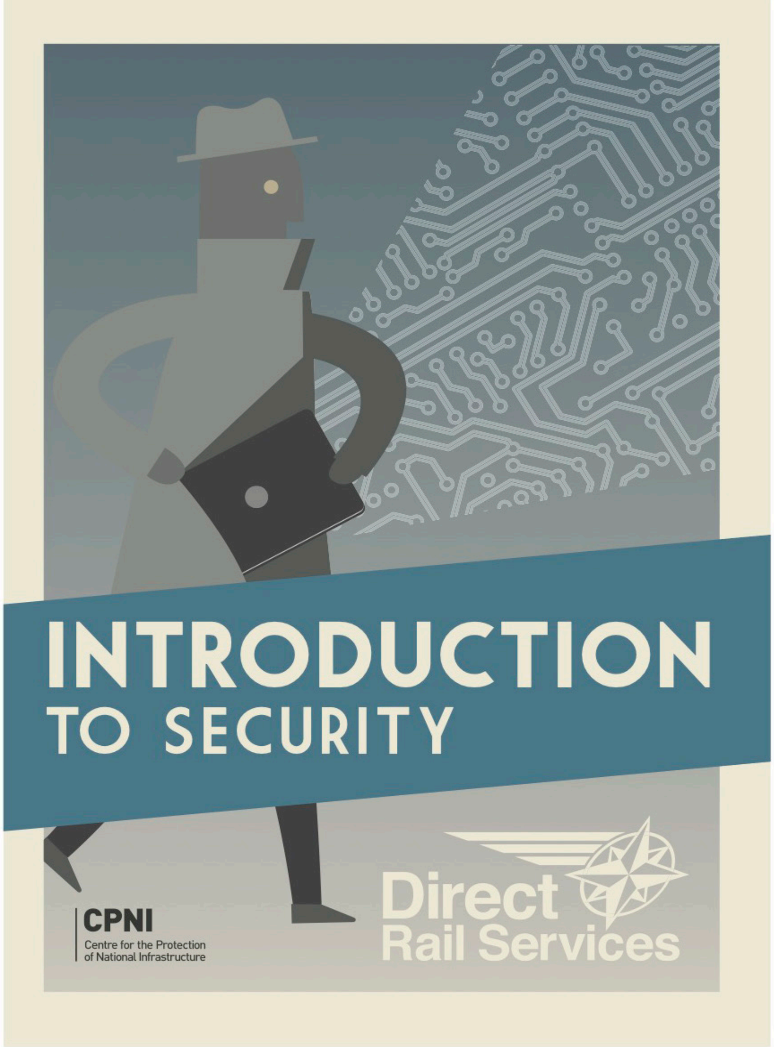


FIGURE 4: INTRODUCTION TO SECURITY (COVER)

COPYRIGHT: CPNI / NTS

In approaching awareness-raising activities, the DRS security team was cognisant that overfamiliarity could lead to complacency. As such, security-related materials and campaigns were balanced with other messages and periodically refreshed. This required the development of a coordinated communications plan working with other areas of the business. Allowing for security awareness-raising activities to be balanced with other areas such as health and safety and HR

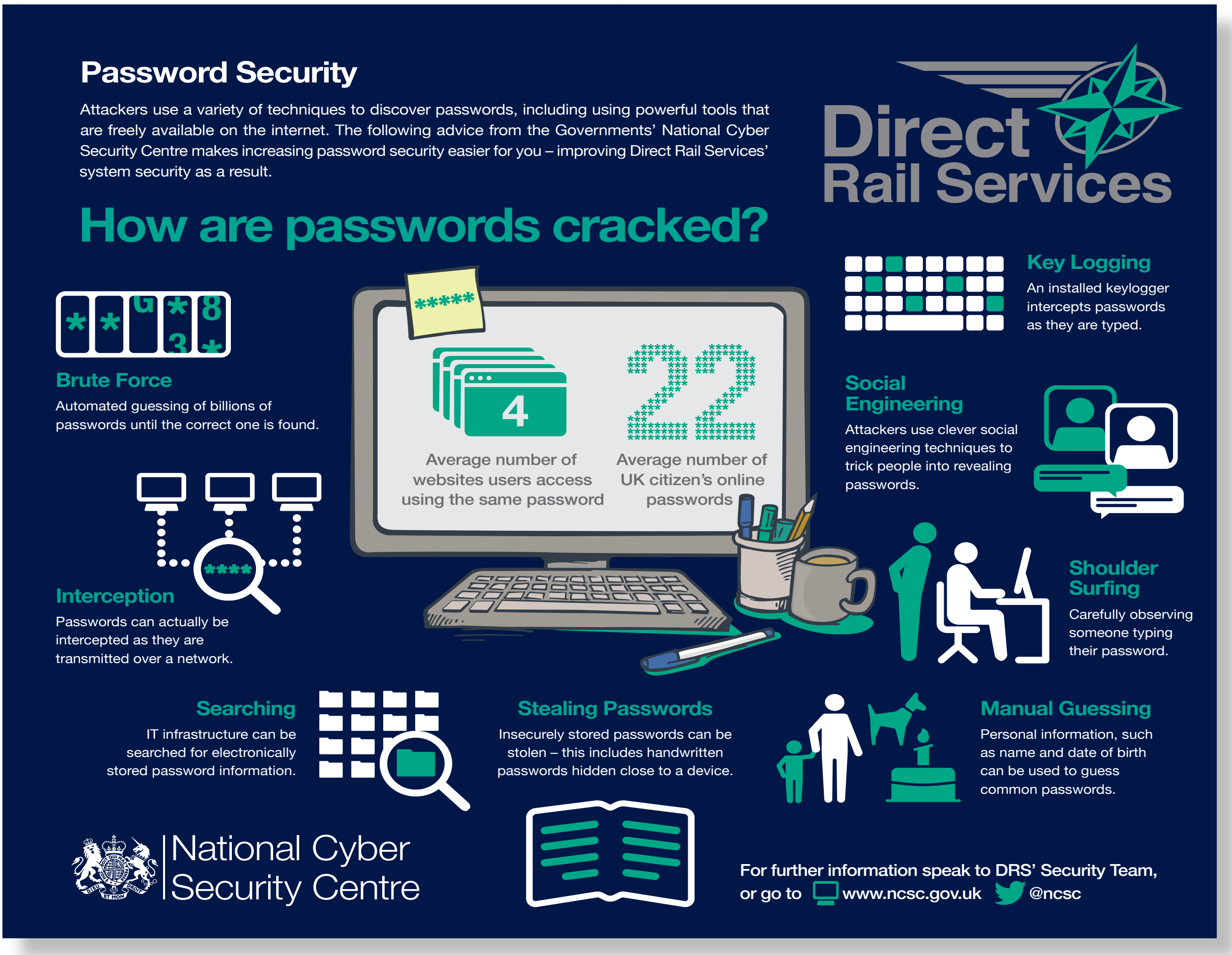
[57] Confidential Reporting for Safety, https://www.ciras.org.uk/ (Website accessed 30th June 2020).

[58] Operations Officer, Interview with authors, 23 January 2020.

processes. At the time as the NSCP visit, DRS was running its 'Zero Harms' programme. This programme was aimed at emphasising how DRS operations should not have any negative impact on people, assets and the environment. Previously the company had run campaigns focused on mental health as well as security.

Other awareness-raising efforts included joint safety-security 'shares' at the start of team meetings. Here, managers were encouraged to draw on recent events, such as terrorist attacks, thefts involving insiders and other security incidents from a range of industries, to engage staff members in discussion. This was seen as beneficial in creating an environment where security issues could be discussed, while also enabling the incorporation of new educational materials, and raising the profile of security more generally within the company.

For many of the staff interviewed, their engagement with security began even before they joined DRS when entering the vetting process. This served to sensitise them to the company's privileged role, and the consequences to them as individuals of potentially losing their clearance. Although vetting was not be legally required for all roles, DRS had a policy of over-compliance in this area and ensured that its staff, as well as members of its broader supply chain, were cleared before commencing work.



Password Security

Attackers use a variety of techniques to discover passwords, including using powerful tools that are freely available on the internet. The following advice from the Governments' National Cyber Security Centre makes increasing password security easier for you – improving Direct Rail Services' system security as a result.

How are passwords cracked?

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Interception

Passwords can actually be intercepted as they are transmitted over a network.

4

Average number of websites users access using the same password

22

Average number of UK citizen's online passwords

Key Logging

An installed keylogger intercepts passwords as they are typed.

Social Engineering

Attackers use clever social engineering techniques to trick people into revealing passwords.

Shoulder Surfing

Carefully observing someone typing their password.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

For further information speak to DRS' Security Team, or go to www.ncsc.gov.uk @ncsc

FIGURE 5: PASSWORD SECURITY CAMPAIGN POSTER: 'HOW ARE PASSWORDS CRACKED?'

COPYRIGHT: NATIONAL CYBER SECURITY CENTRE / NTS

Finally, recognising that DRS' business did not operate at a single or static location, the security team developed a philosophy of 'getting out and about,' in an effort to effectively engage the wider work-force.[59] This led to the increased visibility and accessibility of the security team, allowing them to 'make it personal' in support of embedding security processes.[60] Here, the security team's relatively diverse demographic – with members from a range of age groups – was believed to have also been useful in getting key messages across to different stakeholders. These approaches helped in developing effective two-way communication with regards to security, improving the security team's understanding of on the ground realities. In this regard, the security function's work was somewhat of a balancing act between visibility – being out actively engaging the DRS workforce – and ensuring their administrative and other duties were completed.

Security briefings and training

Security-related information was provided to employees in a range of different formats, including security briefings, webinar videos accessible on the intranet, and at informal face-to-face conversations. Time was set aside during briefings so that staff could ask detailed questions to the security team. In delivering security-related information, care was taken to utilise simple language and relatable examples. For example, when discussing password complexity, care was taken to deliver this in an accessible and engaging way such as using an example of a combination lock on a biscuit tin to demonstrate cryptographic concepts.[61] Efforts were also made to make security 'personal' by providing information centred around real-life applications, which was viewed as a particularly effective way of embedding core security principles and raising awareness of different threats.

In terms of security-related training, the DRS security team recognised that the various occupational groups had different needs and availability. Where possible, security training was fitted into broader courses and provided in such a way that it would not disrupt operations. For example, it was recognised that it would not be possible to take all 20 rail fitters away from their work for a day of classroom-based security training, as this would result in business 'grinding to a halt' due to the constant maintenance that needed to be performed on DRS trains.[62] For staff such as fitters and engineers who spent most of their time out in the workshops, there were fewer clear opportunities for classroom learning. Engagement by the security team with this occupational group also uncovered a preference for face-to-face instruction. To accommodate this, the security team delivered information on key security processes in person as well as through electronic means to smaller groups, working around shift patterns. For train drivers, the DRS security team took advantage of the frequent refresher operational courses that they were required to undertake, by adding security-relevant elements. Mandatory security briefings and required security-related tests were also sent to train drivers through tablet computers, recognising that train drivers regularly used these to access DRS systems while at work.

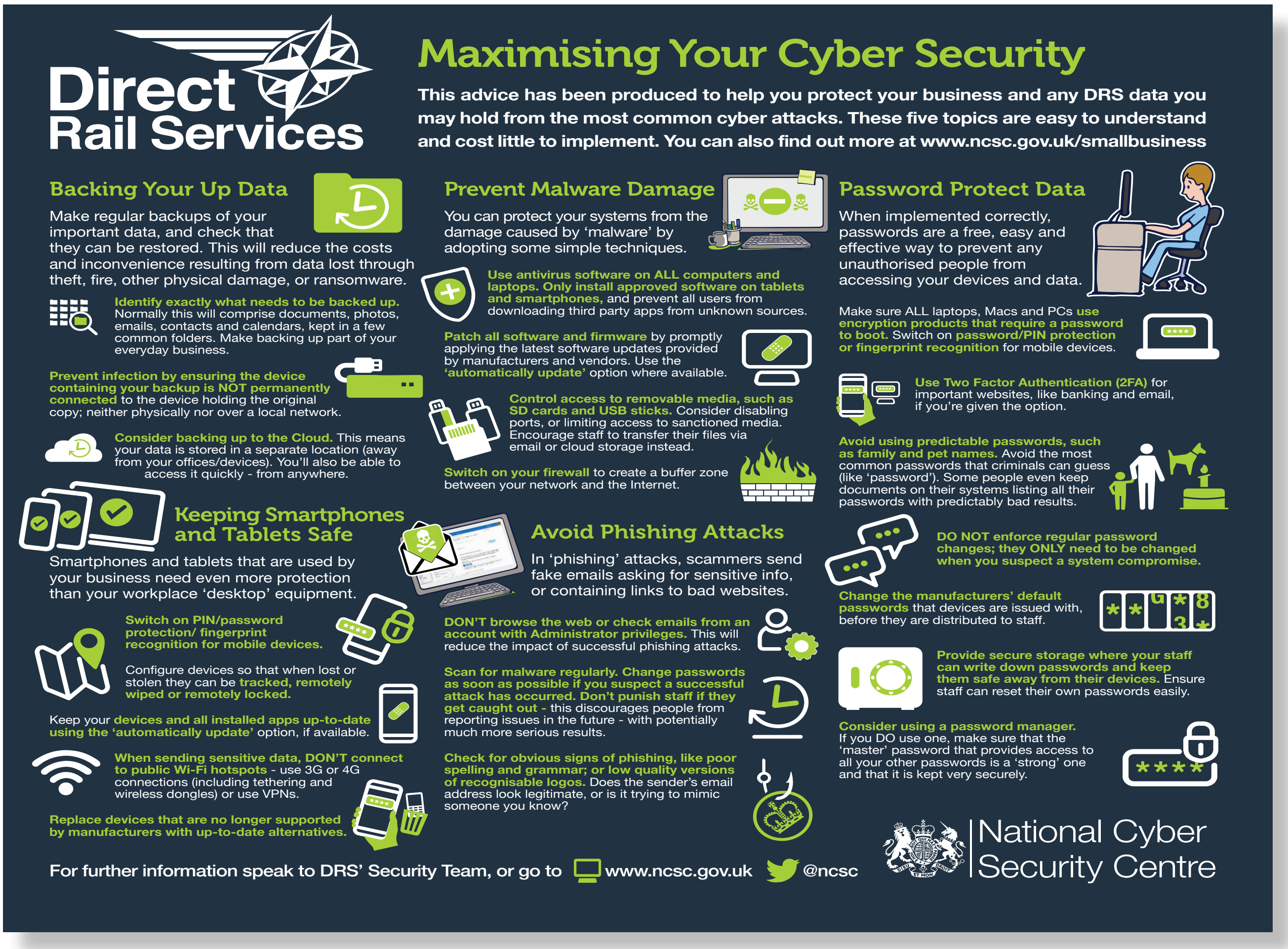
New staff were exposed to security during the onboarding process when they joined the company and periodically during their employment. DRS was also in the process of developing a 'Training Academy,' which will be taken forward under NTS and will consolidate existing courses (including those related to security) and seek to provide these in a more systematic manner. Special emphasis will be placed on making training relevant to employees' roles, using recent and relevant examples and trying to diversify the voices and means of training using new tools. This includes

[59] Ibid.
[60] Ibid.
[61] Security Officer, Interview with the authors, 23 January 2020.
[62] Ibid.

making training relevant to employees' broader lives, with the idea that it is easier to impart security-related guidance if it is also seen to be beneficial at home. For example, discussion of email phishing for bank details, or the release of personal information, for example, when signing up for online offers, may not be directly relevant to the transportation of nuclear material, but are seen as excellent hooks around which to discuss password and cyber security. The increased relevance to home or family life was also relevant to other security requirements, such as the requirement for vetted staff to inform DRS about their travel plans when going abroad. This personalised approach was widely seen as positive amongst this study's interviewees.

DRS staff were also encouraged to take advantage of broader training opportunities offered within the NDA estate. Relevant security-related resources produced by the NDA were integrated into DRS training activities. DRS also drew on materials developed by the UK Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC). Efforts were also made to diversify training in terms of methods and speakers, with emphasis placed on making sure presentations were interactive. Videos were also used to break-up lecture-type delivery. Value was also seen in involving external speakers to diversify the delivery of the security message. Even if the content and message was roughly the same as those delivered by internal trainers, good external speakers were seen as breaking any sense of familiarity and better holding audience attention.

In terms of training methods, the use of tabletop exercises (TTXs) proved to be particularly powerful. Efforts drew on broader best practice, which was then tailored to DRS' needs. For example, the DRS security team regularly attended police and other security-related TTXs events to explore decision making, allocation of resources and potential consequences during a security incident.



Direct Rail Services

Maximising Your Cyber Security

This advice has been produced to help you protect your business and any DRS data you may hold from the most common cyber attacks. These five topics are easy to understand and cost little to implement. You can also find out more at www.ncsc.gov.uk/smallbusiness

Backing Your Up Data

Make regular backups of your important data, and check that they can be restored. This will reduce the costs and inconvenience resulting from data lost through theft, fire, other physical damage, or ransomware.

Identify exactly what needs to be backed up. Normally this will comprise documents, photos, emails, contacts and calendars, kept in a few common folders. Make backing up part of your everyday business.

Prevent infection by ensuring the device containing your backup is NOT permanently connected to the device holding the original copy; neither physically nor over a local network.

Consider backing up to the Cloud. This means your data is stored in a separate location (away from your offices/devices). You'll also be able to access it quickly - from anywhere.

Keeping Smartphones and Tablets Safe

Smartphones and tablets that are used by your business need even more protection than your workplace 'desktop' equipment.

Switch on PIN/password protection/ fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked.**

Keep your **devices and all installed apps up-to-date using the 'automatically update'** option, if available.

When sending sensitive data, DON'T connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Prevent Malware Damage

You can protect your systems from the damage caused by 'malware' by adopting some simple techniques.

Use antivirus software on ALL computers and laptops. Only install approved software on tablets and smartphones, and prevent all users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.

Control access to removable media, such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer their files via email or cloud storage instead.

Switch on your firewall to create a buffer zone between your network and the Internet.

Avoid Phishing Attacks

In 'phishing' attacks, scammers send fake emails asking for sensitive info, or containing links to bad websites.

DON'T browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.

Scan for malware regularly. Change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if they get caught out - this discourages people from reporting issues in the future - with potentially much more serious results.

Check for obvious signs of phishing, like poor spelling and grammar; or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Password Protect Data

When implemented correctly, passwords are a free, easy and effective way to prevent any unauthorised people from accessing your devices and data.

Make sure ALL laptops, Macs and PCs **use encryption products that require a password to boot.** Switch on **password/PIN protection or fingerprint recognition** for mobile devices.

Use Two Factor Authentication (2FA) for important websites, like banking and email, if you're given the option.

Avoid using predictable passwords, such as family and pet names. Avoid the most common passwords that criminals can guess (like 'password'). Some people even keep documents on their systems listing all their passwords with predictably bad results.

DO NOT enforce regular password changes; they ONLY need to be changed when you suspect a system compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage where your staff can write down passwords and keep them safe away from their devices. Ensure staff can reset their own passwords easily.

Consider using a password manager. If you DO use one, make sure that the 'master' password that provides access to all your other passwords is a 'strong' one and that it is kept very securely.

For further information speak to DRS' Security Team, or go to www.ncsc.gov.uk @ncsc

National Cyber Security Centre

FIGURE 6: PASSWORD SECURITY CAMPAIGN POSTER: 'MAXIMISING YOUR CYBER SECURITY'

COPYRIGHT: NATIONAL CYBER SECURITY CENTRE / NTS

These resources were then subsequently adapted for delivery to DRS staff and in joint events with their sister nuclear transport company International Nuclear Services (INS). TTXs were particularly believed to have been useful in helping more technically-focused staff think through the range of consequences that may have resulted from different security-related incidents.

Information and cyber security practice

Information and cyber threats were viewed as one of the greatest risks for DRS. Like most nuclear organisations, DRS stored nuclear-related sensitive information on a secure network, with USB ports blocked on computers, and access to potentially hostile websites denied. Dedicated training was held on cyber-related threats at induction sessions for new employees, with a focus on the risks of phishing attacks. A strict clean-desk policy was also implemented to ensure that no sensitive information was left out and unsecured. Sweeps were routinely conducted by the security team to check compliance with this, and employees were encouraged to anonymously report if they observed repeat offenders. In addition to the more visible manifestations of information security, DRS also monitored electronic access through automated software, which logged and analysed user IT behaviours. This was set-up to flag potentially suspicious actions such as individuals logging in remotely at night or sending email attachments to personal accounts.

More generally DRS sought to shift what was a pre-existing culture of information restriction from 'need to know' towards a 'need to share' philosophy. To this end, information classification became a key process at DRS to ensure that sensitive information was not widely released and conversely that non-sensitive information was not restricted as this could inhibit operations, business development and stakeholder engagement activities.[63]

Security testing and security culture assessment efforts

The DRS security team implemented several routine testing exercises in an effort to gauge staff awareness and understanding of security measures. These included 'clear desk' checks and simulated phishing email campaigns. To maximise the utility of security testing, clear aims and objectives were worked out before starting each campaign. 'Clear desk' checks involved inspecting each desk in different offices after hours, at random intervals. After each test, cards were placed on each desk with a pass/fail score. Scores were noted and persistent offenders were provided with an opportunity to refresh their understanding of the rules, with the potential for escalation to Human Resources if required.

To replicate frequently encountered cyber-attacks, the IT team created and distributed phishing emails to colleagues. These were carefully designed to make them look legitimate. They were also varied to avoid colleagues becoming familiar with certain templates and distribution strategies. If employees clicked the links embedded within them, these incidents were centrally logged by the system. Security-related tests revealed that individuals may make inadvertent mistakes from time to time. Consequently, while relevant staff were reminded of security measures, focus was placed on 'serial offenders' and changing their behaviour. The security team also believed these tests were useful in both raising awareness of security amongst staff and helping benchmarking compliance with specific measures.

[63] Business Services Officer, Interview with authors, 23 January 2020.

DRS also made considerable use of surveys to assess security culture among their colleagues and proactively identify potential issues that may affect security implementation. These included a dedicated in-depth security survey delivered to all colleagues every two years, and a shorter 'temperature check' survey in the year in between. Security questions were also included on more regular staff surveys designed to probe a wider range of issues. Survey completion rates were relatively high, averaging around 60%, with Department Heads strongly encouraged to ensure that their teams were fully engaged. Information from surveys was also combined with staff feedback at exercises and training as well as informal comments that were provided to the security team to build a rich picture of security awareness.

Summary

DRS made considerable efforts to place security at the centre of its operations – of equal importance to safety. To this end, security was reframed as an enabler, rather than a constraint, with an increased focus on prevention as well as protection. This approach placed people at the centre of security, with effective engagement built on a strategy of developing close personal relationships and an improved image of the security department. These changes did not occur in isolation and required close collaboration with other departments, such as human resources, to ensure both consistency of messaging and that security, safety and other business areas were delivered as part of a coordinated, rather than competing effort. Helped to an extent by the relatively small size of the company, it is clear that the aforementioned improvements that were made over the course of several years, served to strengthen security culture at DRS.

Case study III: EDF Energy

Company overview

EDF Energy (EDF) is an integrated energy company specialising in electricity generation and the sale of natural gas. The company operates a range of technologies including, since the 2009 takeover of British Energy, the UK's operating fleet of nuclear power stations. These account for approximately 20% of the UK's energy mix, employ around 13,000 people, and supply electricity to over five million households and businesses.[64]

When the interviews for this case study were conducted, EDF was undergoing a period of transition as its older nuclear power reactors approach decommissioning with new reactors either being constructed or planned. To facilitate this transition, new organisational structures are also being constructed and aligned – processes which themselves are substantial undertakings. At the close of 2020, EDF had eight operating nuclear power plants, which between them host 15 reactors: 14 Advanced Gas Cooled Reactors (AGRs); and one Pressurised Water Reactor. The AGRs were first connected to the grid in the 1970s and 1980s and are scheduled to be retired over the next decade. To offset this drawdown the UK Government continues to invest in nuclear and in October 2015, EDF and China General Nuclear Power Group (CGN) signed a Strategic Investment Agreement for the construction and operation of Hinkley Point C (HPC) with each firm holding 66.5% and 33.5% of the Agreement, respectively.[65] Operations at HPC are scheduled to begin in 2025.

This case study seeks to understand how nuclear security culture has been promoted at EDF Energy, the challenges encountered and how they have been overcome.

Operational environments and security risks

At its heart, EDF is a large engineering firm which conducts nuclear-related business across related, but differing units governed at the corporate level. These encompass nuclear new build activities, the operating estate (both nuclear and thermal) and an expanding renewables business. The company is currently responsible for maintaining security at nine large nuclear sites within the UK, eight operational nuclear power plants and one new build.[66] This diversity of environments presents different challenges for the implementation of nuclear security, which are set to be compounded by the upcoming decommissioning of six of the seven operational sites. As such EDF must maintain security as the majority of its existing fleet is retired and decommissioned, while also ensuring effective knowledge management, so that its security best practices are consolidated and transplanted into the HPC new build.

Like other UK nuclear sites, EDF has developed security systems to mitigate a broad range of potential threats. The most pressing of these threats are perceived to be anti-nuclear protesters, cyber-attacks and insiders.[67] These may manifest in different ways depending on the operational environment.

[64] IAEA. (Undated). Power Reactor Information System (PRIS) database. Online. Accessed December 2020. Available at: https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=GB

[65] EDF. 92015). Press release: Agreement for construction of HPC nuclear power station. Accessed December 2020. Available at: https://www.edfenergy.com/energy/nuclear-new-build-projects/hinkley-point-c/news-views/agreements-in-place

[66] Heysham 1 and 2 nuclear powers stations are collocated on a single site.

[67] EDF Head of Security interview with the authors, 23 October 2020.

For example, regular protests in relation to the Hinkley Point have been held over the last decade, and in 2011 anti-nuclear demonstrators blockaded the Hinkley Point site in response to the new build plans.[68]

Major challenges encountered

In acquiring British Energy in 2009, EDF inherited a company with a mature working culture centred around the safe operation of nuclear technology, with the importance of nuclear safety widely accepted and promoted across its estate. In contrast, nuclear security at the time was relatively compartmentalised, with its value and necessity far less clear.[69] Even within the security team, the value of security was difficult to articulate, with a widespread perception that security was an expensive overhead and an impediment to the business' primary role of power generation. This resulted in a culture of secrecy with respect to security, the promotion of unnecessarily expensive 'gold-plated' solutions and a 'mystified' opaque approach to the development and implementation of new measures.[70]

As such, a major challenge that faced EDF in early 2010s was how to transform pre-existing attitudes towards security, both within the security team and across the wider business. In addressing this challenge, EDF has adopted an integrated approach where security and safety considerations are viewed together across business structures, procedures and processes. Here, security is viewed simply as another hazard to be managed.

During this transition, the following challenges were encountered:

- Adaptability – In order to raise security to the same prominence as safety, it was necessary for members of the security team to fundamentally change their approach and ways of working. This was difficult for some who, based upon their past experience, found it hard to transition from a framework of beliefs based upon prescriptive thought, regulation and solutions to a more open and transparent approach. Under the new approach, security is enabled by a risk-managed approach, where it is integrated with all other risks, rather than considered as a discrete activity or discipline, being the sole preserve of the few. These seek to be supported by clear and effective communications and information which is accessible yet appropriately protected.

- Diversity – Traditionally the security team at UK nuclear sites was made up largely of men with military or policing backgrounds. While these groups bring important transferrable skills and experiences to the delivery of security, it was recognised by EDF that a greater diversity of voices within the security team would be beneficial. By promoting recruitment from a wider range of disciplines and encouraging gender diversity, the security team has been able to develop broader insight into security challenges and their associated solutions whilst promoting language and engagement that are more easily articulated and understood by different audiences.

- Outreach – EDF has numerous occupational groups and consequently tailors its security awareness effort to engage individuals effectively across its workforce. Broadly speaking, staff at nuclear power plants can be divided into two categories: those with hands on responsibilities for engineering processes (known internally as 'plant-touchers') such as technicians, maintenance staff and contractors; and enabling staff who work in areas such as administration, human resources, occupational health and security. Approximately 50-60% of staff at a nuclear

[68] Press Association. (2011). 'Hinkley Point power station blockaded by anti-nuclear protesters' in The Guardian, 3 October. Online. Available at: https://www.theguardian.com/environment/2011/oct/03/hinkley-point-protest-nuclear-power
[69] EDF Security Operations Manager interview with the authors, 23 October 2020.
[70] EDF Head of Security interview with the authors, 23 October 2020.

power station are plant touchers who have limited access to IT workstations in their day-to-day roles.[71] Consequently, security awareness initiatives and training has had to be tailored and delivered in a different manner for these two groups to ensure it meets their operational require ments and is not overburdening.

- Cost efficiencies – Recently, Board-level direction has targeted spend efficiencies which have posed a challenge to all functional areas in terms of maintaining essential and desirable outputs within a constrained budgetary profile. Regarding security delivery, these were overcome by forward collegiate planning, including the construction and alignment of new organisational structures to retain and consolidate key security knowledge and working practice.

Strengthening security culture through effective and adaptable leadership

Clear and effective leadership is widely recognised as fundamental to the development of an effective security culture. As previously noted, British Energy's security function was somewhat compartmentalised, and seen by some as an expensive obstacle to efficient operations. To overcome this the security team sought to promote the necessity of nuclear security to the EDF Executive by emphasising the hazardous nature of nuclear technology, the regulatory requirements for security, and the reality of the threat.[72] Within EDF Generation and Nuclear New Build, the Head of Security is embedded within the senior leadership team (SLT), reporting to the Directors for Safety, Security and Assurances, with security-related messaging presented to the Board through existing structures and in a manner consistent with other Board business.

For example, security issues were framed in terms of business requirements and risk-management – a format very familiar to the Board because the company has an established risk management process, with 10 identified areas of enterprise risk. Relevant members of the SLT are assigned responsibility for managing individual areas of enterprise risk, with the Head of Security responsible for personnel, physical and cyber security across all business areas. In turn, managers must demonstrate to the Risk Committee changes in risk profiles, which in turn informs the company mitigation and investment strategies.

In addition to safety-security concerns, EDF is a commercial company and the Board is mindful of financial and reputational risks. This allows the security team to draw on examples from comparable industries to give further context to their messaging. For example, to emphasise to the Board the increased security risks of more employees working remotely, the security team drew on the example of global shipping and logistics company, Maersk, utilising information available from open sources. On 27 June 2017, Maersk was attacked by the NotPetya ransomware.[73] The attack resulted in significant disruption and is estimated to have cost Maersk US$300 million in lost revenue.[74] The high financial cost helped cement the gravity of potential cyber risks to EDF and gained Board-level support for ensuing cyber-security campaigns.[75]

Clear communications and reporting structures have been key enablers of security at EDF, and by using simple targeted language, the security team successfully re-engaged the Board on security, and in turn the Board has used its authority to drive support for security initiatives across the company.

[71] EDF Security Operations Manager interview with the authors, 23 October 2020.

[72] EDF Head of Security interview with the authors, 23 October 2020.

[73] Palmer, Danny. (2019). 'Ransomware: The key lesson Maersk learned from battling the NotPetya attack' in ZDNet. 29 April. Online. Available at: https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/

[74] Palmer, Danny. (2017). 'Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk,' in ZDNet. 16 August. Online. Available at: https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/

[75] EDF Security Operations Manager interview with the authors, 23 October 2020.

In successfully engaging with the Executive to use their authority to drive change, EDF's security team demonstrated effective and adaptable leadership which can be distilled into several key principles, namely:

- Integration into business structures;
- Security seen as an integral part of being a nuclear professional;
- Clear and tailored communication; and
- An integrated risk-management approach.

This allowed the team to recast the security function from a 'self-serving dark art' to a key business enabler.[76] As well as gaining executive level support, these principles were also effective in socialising the need for, and importance of, security across the broader workforce. In addition to the above, the security team has drawn upon wider company strategies for managing change and exploiting regulatory synergies.

In terms of managing change, upcoming company-wide challenges are anticipated and security-related risks are mitigated in an organised fashion. In addition, changes in the UK regulatory approaches, discussed in the previous case studies in this handbook, have helped support the development of outcome-focused security solutions. Although this has required additional resources, EDF has utilised this to consolidate its cultural transformation and 'bake-in security' to its overall working and safety culture.[77] Examples of these principles in action are discussed in the following sections.

Integration into business structures

EDF's security team successfully engaged with both its Executive and the wider company by using pre-existing business structures. Within EDF, there is a system of cross-site co-ordination groups (known as Peer Groups) where staff members connect with their counterparts across the business, regardless of where they are geographically located. These allow for role-specific communications, keeping different teams up to date with relevant issues.[78]

By using the pre-existing Peer Group system, the security team has been able to integrate security into the company's business structures across the operating estate without adding a further layer of bureaucracy. In addition to allowing for tailored outgoing communications to specific groups (see Clear and Tailored Communications below) the Peer Groups are able to provide feedback to the corporate headquarters and security governance structures to address any areas of conflict.[79]

Similarly, new processes have been introduced such as the Security Protected Plant Identification (SPPI) process which integrates all engineering, safety and security design capabilities to determine critical facilities warranting protection. This SPPI process is aligned with a pan-business Maintaining Design Integrity (MDI) process to ensure coherence and consistency of design processes across the business.[80] This approach in turn informs the corporate risk management process demonstrating the integration of security risk into core business processes and objectives. By understanding both

[76] Ibid.
[77] Ibid.
[78] EDF Head of Security interview with the authors, 23 October 2020.
[79] Ibid.
[80] Ibid.

regulatory and real-world requirements, the security team has been able to act as an 'intelligent customer' during the SPPI process and assess and apply proportionate security measures. As such, EDF has been able to avoid 'gold-plated' solutions and reduce costly and redundant spending.[81]

Clear and tailored communications

For EDF's new security approach to be understood and applied by staff, it was recognised that the needs of different occupational groups, their preferred communication channels and formats should be considered. In addition to a 'demystified' (i.e. more open) approach, the security team has sought to diversify its staff to reflect a range of backgronds, including technical specialists. These measures, and 'speaking the language' of the different occupational groups, have achieved better security buy-in across the company.[82]

As noted, the security team made effective use of the pre-existing Peer Groups to facilitate security-related communication across the fleet. Each Peer Group contains site leads who disseminate information amongst their respective teams. This helps ensure consistency across the company, whilst also functioning as an effective means of reaching different target audiences. Engagement through the Peer Groups has allowed the responsibility for the security function to be broadened across staff, with individuals from a wide range of backgrounds and skill sets feeding into the implementation of new measures. This has enhanced security engagement and reach across the fleet.

Risk management approach

EDF frames its approach to security in risk management terms, where security risks are primarily seen as the integrated management of available resources to reduce common high hazard areas. This proved effective in conveying key messages regarding security measures and approaches to the company's senior leadership who were already well-versed in risk management concepts. This is illustrated in the company's business risk register where of the 10 major risks, two are related to security.[83]

A risk-managed approach was also successful in engaging staff who are also well-versed in safety issues. New staff are sensitised to the approach during their inductions, with security expectations built into occupational roles alongside safety. As a result, like safety concerns, security requirements have been deliberately crafted as a risk that is to be managed. As such, the security team sees its main task as the management of the prevalent hazard and is encapsulated by the phrase security is 'just another hazard to be managed.'[84]

Managing change and exploiting regulatory synergies

To retain and transfer its security expertise as the company's strategic path moves to decommissioning and a nuclear new build programme EDF is creating a Technical Client Organisation (TCO). Bringing the Design Authority and Intelligent Customer functions together with security from across the new build and operating estates. The TCO supports new projects from cradle to grave, acting as a knowledge centre which sets standards and establish requirements, for delivery by different site teams. As part of this knowledge-management the TCO will include a security culture standard across the new nuclear estate.[85]

[81] Ibid.
[82] EDF Security Operations Manager interview with the authors, 23 October 2020.
[83] EDF Head of Security interview with the authors, 23 October 2020.
[84] Ibid.
[85] Ibid.

EDF's new approach to security has also coincided, and been enabled, by the introduction of Security Assessment Principles (SyAPs) for the regulation of nuclear security in the UK, which emphasise outcome-based security delivery. Although the introduction of this new regulatory approach has been expensive to the business, the need to clearly demonstrate security outcomes under SyAPs has helped accelerated security awareness and integration and provided broader freedom to innovate in the delivery of security.

Awareness-raising and training

For staff across all EDF's environments, security begins with vetting requirements and on-boarding processes where staff are introduced to company procedures and expectations. After their inductions, the company also engages with various rolling communications campaigns. For example, its 'All Eyes Open' campaign is one of several enduring company-wide communications designed to sensitise staff to 'spot the absence of the normal' or 'the presence of the abnormal.'[86] This includes unusual physical manifestations (for example: unattended bags or things being in the wrong place) but also staff behaviours, such as employees adopting unusual work routines or changes in attitudes. This is reinforced by posters and notices situated throughout company locations, which are regularly renewed.

The 'All Eyes Open' campaign forms part of EDF's 'challenge culture' where it is stressed that staff should openly call out perceived transgressions, with such observations forming an important part of staff duties. To support this, the company has a 'no blame policy' aimed at encouraging staff to report unusual activities, regardless of outcome or impact on performance. To cement this, EDF has engaged with Trade Unions to reassure them that their members would not be penalised if reports are made. EDF are keen to note that within the company, consistent with the risk-management approach, 'security culture is part of safety culture,' and that to differentiate between the two creates an artificial delineation from both an operational and organisational perspective.[87] This is reflected in the company's language, particularly in training and awareness materials, where comparisons to

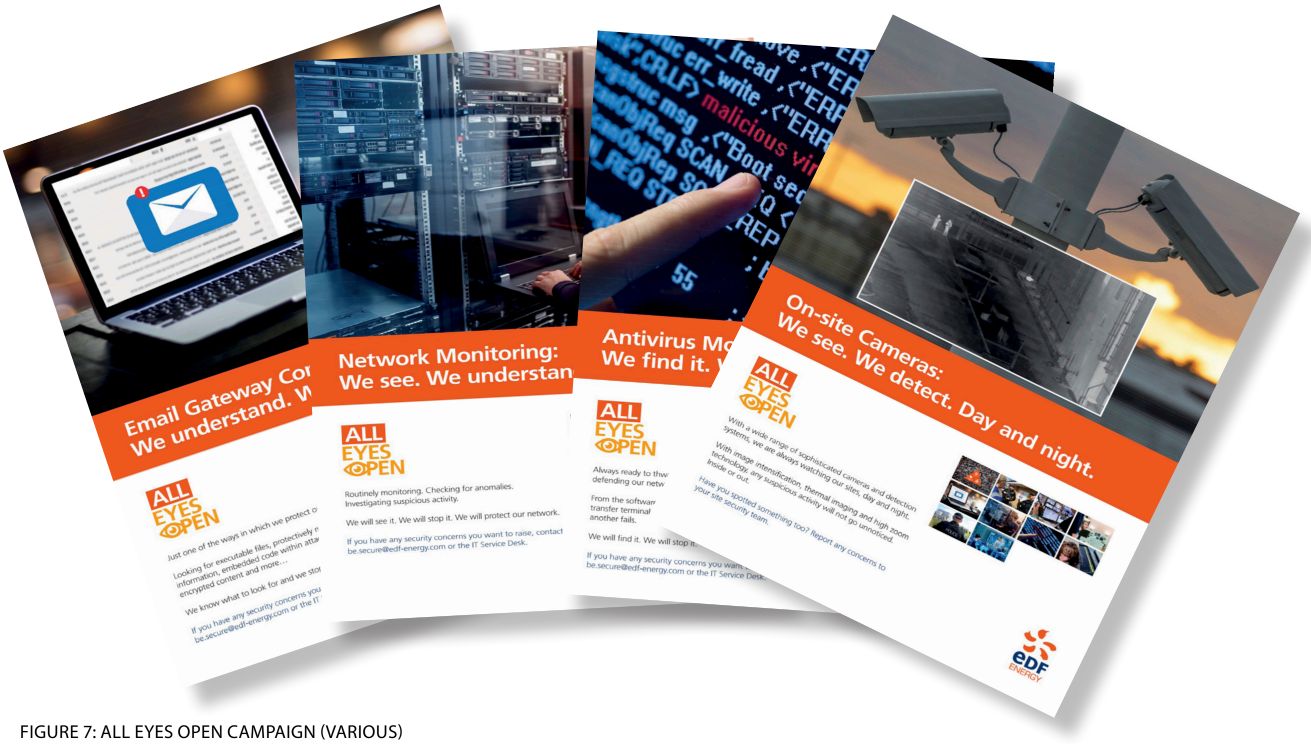

Email Gateway Co
We understand. W
ALL EYES OPEN
Just one of the ways in which we protect o
Looking for executable files, protectively m
information, embedded code within atta
encrypted content and more…
We know what to look for and we sto
If you have any security concerns you
be.secure@edf-energy.com or the IT
Network Monitoring:
We see. We understan
ALL EYES OPEN
Routinely monitoring. Checking for anomalies.
Investigating suspicious activity.
We will see it. We will stop it. We will protect our network.
If you have any security concerns you want to raise, contact
be.secure@edf-energy.com or the IT Service Desk.
Antivirus Mo
We find it. W
ALL EYES OPEN
Always ready to thw
defending our netw
From the softwar
transfer terminal
another fails.
We will find it. We will stop it.
If you have any security concerns you want
be.secure@edf-energy.com or the IT Service Desk.
On-site Cameras:
We see. We detect. Day and night.
ALL EYES OPEN
With a wide range of sophisticated cameras and detection
systems, we are always watching our sites, day and night.
With image intensification, thermal imaging and high zoom
technology, any suspicious activity will not go unnoticed.
Inside or out.
Have you spotted something too? Report any concerns to
your site security team.
EDF ENERGY

FIGURE 7: ALL EYES OPEN CAMPAIGN (VARIOUS)

COPYRIGHT: EDF

[86] Ibid.
[87] Ibid.

safety are stressed. For example, reporting potential security concerns are compared to pulling a fire alarm, with the rationale that no-one could be criticised for raising a fire alarm if they believed people's lives were in danger – whether there was ultimately a fire or not.

In addition to company-wide messaging, care is taken to deliver bespoke safety-security messages for specific occupational groups. As noted, staff at EDF tend to fall into one of two categories – 'plant touchers,' responsible for hands-on roles, and 'enabling staff.' Enabling staff are primarily office-based and as such, can be targeted through conventional means, such as email communication, newsletters, and desktops log-in security compliance campaigns. In contrast, plant-touchers have more practical hands-on roles and do not have regular access to work terminals or email. To effectively reach this group security messages have been integrated into their daily meetings, which also serve as a useful forum for discussion and present an opportunity to explain why something is potentially an issue. Consequently, when security-related issues and threats are introduced, care is taken to explain the rationale, and the link between them. Here it has been shown that by focusing on improving understanding, rather than simply badging procedures as 'just security', improves compliance.

Safety-security messages are constantly refreshed and reinforced with wider site communications and training days. Other outreach initiatives include 'turnstile days,' where on selected days, a site's security team will physically stand at entrance turnstiles and, for example, remind staff about their obligation to inform Human Resources if their domestic or financial situation has changed.

Identifying security-related issues

To ensure on a daily basis that security issues are identified and reported, Occupational Health, Human Resources and Security collaborate to form a 'Golden Triangle.'[88] By scheduling regular meetings between the three departments, EDF has sought to allow department leads to freely discuss issues, including those relating to personnel. As well as enabling staff support for challenging personal circumstances, the group is able to address potential early warning signs amongst staff and take steps to mitigate any vulnerabilities that might otherwise lead to an increased risk of insider activity. EDF is fortunate as its size and scale allow it to offer numerous employee assistance programmes, such as counselling and/or debt management assistance. These programmes form part of a benefits package that helps to attract and retain qualified staff, but which also played a positive security role through reducing staff members' emotional and/or financial stresses.

Enabling effective security communication

As previously discussed, the use of Peer Groups to communicate horizontally on security-related issues has been considered particularly effective by EDF and allows for issues to be addressed at an appropriate level. In general, security issues are relayed from the EDF Group Headquarters security team through the Technical Safety Support Manager (TSSM) Peer Group.[89] TSSMs represent the third most senior position at a nuclear plant, coming directly beneath the Station Director and Plant Manager. The allocation of a security lead to the TSSMs was a deliberate choice because, in addition to being slightly removed from the upper leadership, therein allowing a broader perspective on operations, TSSMs also have responsibilities for meeting regulatory requirements (both ONR and the Environment Agency) and emergency arrangements. As such, TSSMs are also regarded as the 'conscience of the station' and have considerable clout in daily operations. For example, the

[88] EDF Security Operations Manager interview with the authors, 23 October 2020.
[89] Reflecting EDF's guiding principles, the TSSM title was not expanded to include security, as it is seen as being embedded in the safety function.

introduction of SyAPs was accompanied by an information campaign disseminated via the TSSM Peer Group. This triggered conversations and understandings about the new requirements within each power station and was considered an effective means of reaching the different working communities. Peer groups can also be used in conjunction with one another and other departments. For example, should the Group security team feel site security managers were under-performing, this would initially be communicated through the Plant Managers' Peer Group. However, if issues persisted, then other groups such as HR, and TSSMs would also be mobilised to ensure consistent communications and awareness of issues.

Security culture assessment

To help assess the broad impact of these initiatives, EDF also conducts an annual Nuclear Safety Culture Survey, which since 2019 has included a security section. The security section includes eight questions based upon the CPNI SeCuRE 4 Security Culture Survey material.[90] Although not extensive, the questions are seen as relevant to gaining a broad understanding of the security culture environment. At the time of interview, only two Nuclear Safety Culture Surveys with a security section were conducted, although results will help inform a baseline understanding and act as a barometer of overall attitudes.

Summary

EDF has worked to integrate security into its long-established safety culture, which remains focused on the protection of people and the environment from unacceptable radiological consequences, regardless of the initiating event. This integration has been driven by the self-identification of potential issues, although regulatory requirements have also helped establish and sustain a focus on security. Central to the company's approach is having confidence in the role of the security team and their understanding of regulatory and real-world requirements. This is then translated into clear security actions, communications and training – drawing on the aforementioned networks, structures and partnerships. With an emphasis placed on the language and format employed, to reach the various groups within the company. Improved communications have had wide-ranging effects ranging from allowing the security team to demonstrate value to the executive level, but more practically to 'demystify' security amongst staff. As part of this, EDF has sought for security considerations to be better understood and applied by staff, 'baking it into' normal working practices.

At the plant level, a major impact has been appropriate delegation and empowerment of differing functional management structures to oversee security matters. Reflecting the practicalities of large engineering sites, it was stressed that one should not 'under-estimate the influence of the peer groups,' and their impact on working practices.[91] By understanding the demands of operating a large engineering firm, the company selected the TSSMs as the appropriate level for security roles. Although this is lower than the previous Plant Manager level, it is considered as better housed and more effective, by virtue of its influence.

With the eventual decommissioning of much of its nuclear fleet, and other factors, the need for cost efficiencies is also driving change. EDF's experience in nuclear safety and security is hard won and the company seeks to consolidate this into a single location, via the TCO. By retaining a centre of knowledge that can advise on best practices and standards, the company is looking to the future and the transplantation of these approaches and behaviours at new sites.

[90] CPNI (Undated). "SeCuRE 4: Assessing Security Culture". Online. Accessed December 2020. Available at: https://www.cpni.gov.uk/secure-4-assessing-security-culture

[91] EDF Security Operations Manager interview with the authors, 23 October 2020.

Case study IV: Radioactive Waste Management

Company overview

Radioactive Waste Management (RWM) is a public organisation, established by the UK government as a subsidiary of the Nuclear Decommissioning Authority (NDA) in March 2014. It is responsible for planning, delivering, and ultimately managing to the end of its operational life the UK's Geological Disposal Facility (GDF) – the UK government's preferred long-term solution to national radioactive waste disposal needs. This work is currently in its early stages, with the focus on site selection. In November 2020, RWM announced its first 'Working Group,' while a second Working Group was announced in January 2021.[92] These groups will discuss with local partners and the community their potential involvement in this project.[93]

Although construction work on the GDF is yet to start, to prepare for delivery, RWM is undergoing a business transformation. Beginning as a small research organisation, RWM is getting ready to deliver one of the largest construction projects in Europe, with the GDF planned to host nuclear waste for hundreds of years. Reflecting this transition, RWM's workforce is increasing rapidly; for example, from April to December 2020 the company's staff almost doubled from 120 to 230 full-time employees.[94] This case study seeks to understand the challenges faced by RWM, as the organisation focuses on developing an effective nuclear security culture while undergoing this transition.

Operational environments and security risks

With construction of the GDF yet to begin, RWM's current operational environment is its headquarters in Didcot, Oxfordshire. As an office-based organisation, cyber security is the prevalent security concern, with the organisation encountering the broad spectrum of common cyber-threats faced within many office environments. However, as the GDF progresses through its various pre-construction, construction, and operational phases, security threats will diversify and physical security measures will also become increasingly important. At the time of writing, with the project in its early planning stages, security in relation to nuclear threats, as outlined in the UK's national Design Basis Threat (DBT), are considered negligible owing to the current absence of nuclear materials, waste or sensitive nuclear information. This places a cyber security focus on broader activity, in relation to the protection of sensitive personal data and commercial information. Similar to other commercial businesses, emphasis is placed on the confidentiality, integrity and availability of information so that commercial activities can be readily and securely delivered, while at the same time seeking to develop robust systems and processes that will be able to protect sensitive nuclear information as RWM transitions.

Confidentiality is of paramount importance in RWM's approach, with the UK government adopting a 'voluntarist approach' to the GDF, as outlined in a 2014 White Paper on 'Implementing Geological Disposal.' This requires community consent as a precondition to the planning process.[95] RWM's

[92] HMG (2021). 'RWM welcomes launch of second GDF 'Working Group'', Radioactive Waste Management. 14 January. Online: Available at: https://www.gov.uk/government/news/rwm-welcomes-launch-of-second-gdf-working-group

[93] HMG (2020). 'RWM welcomes announcement of first 'Working Group'', Radioactive Waste Management. 4 November. Online: Available at: https://www.gov.uk/government/news/rwm-welcomes-announcement-of-first-working-group

[94] Interview with RWM Security Managers, 4 December 2020.

[95] HMG (2014). 'Implementing Geological Disposal', Department of Energy and Climate Change. 24 July. Online. Available at: https://www.gov.uk/government/publications/implementing-geological-disposal; HMG (2014). 'Geological Disposal Facility siting process review', Department of Energy and Climate Change. 24 July. Online. Available at: https://www.gov.uk/government/consultations/geological-disposal-facility-siting-process-review

engagement with communities of interest is dependent upon trust and maintaining confidence in communications and the integrity of shared information. Consequently, weak cyber controls have the potential to incur reputational costs to RWM, damage community relations and impact upon the willingness of others to engage with the company through the Working Groups. This resulted in cyber security being identified as a key business risk at the very start of this project.[96]

Once site selection is complete, cyber security will play an increasingly significant role during the GDF's design and construction phases alongside physical and personnel security measures, when information regarding security planning and systems will require protection. This requirement will be further emphasised as construction and waste-emplacement operations are launched. This will require the attention of security measures to protect information, the compromise of which could materially impact security delivery.

Baselining nuclear security culture

In its current operational context, it is perceived internally within RWM that there is a relatively low-level baseline of nuclear security culture, stemming from its lack of sensitive nuclear information and assets. This has complicated the task of the security team, which seeks to advocate for the value of security and establish it as a core business enabler. Despite the high-level acknowledgement of the importance of nuclear security culture and the future requirement to raise security culture across the business, awareness of the risk and associated risk responsibilities is not yet mature enough, nor is the requirement sufficient at this time to drive a framework for a comprehensive nuclear security culture programme.

RWM recognises that it does not yet have full awareness of its threat profile or its risk mitigation responsibilities. To better understand its current organisational culture and provide a foundation for a comprehensive future programme, an improvement project is underway to define RWM's organisational culture and its functional scope, which is currently represented by a strapline of 'Safe, Secure and Sustainable'. RWM is also working on developing security capacity and capability, initially to meet key requirements such as GDPR and the Nuclear Industries Security Regulation (NISR) 22, which covers nuclear licensee cyber security reporting responsibilities. The ultimate goal of utilising the internal expertise created through these initiatives, is to embed security culture and for staff across all areas to take greater ownership of its security risk profile and mitigation efforts. This reflects in part a maturing insight by the Executive into the requirements and challenges associated with building broader nuclear security functionality and resilience, which will continually evolve as the organisation transitions. Cyber security and information assurance requirements will serve to drive what is an evolving nuclear security culture.

Major challenges encountered

One consequence of the organisation's ongoing expansion is the need to rationalise competing management priorities, including security concerns. Like all organisations, RWM's senior leadership must balance a wide variety of considerations and decide which areas should be prioritised. One impact of this is that, at the time of writing, there is an internal perception that the executive management group has not considered this a high priority, and that it is yet to use its influence and authority effectively in support of the development of an effective nuclear security culture. This is likely influenced by the current absence of nuclear material or GDF-related sensitive nuclear information and will change as RWM becomes a delivery organisation.

[96] Interview with RWM Security Managers, 4 December 2020.

RWM brings together a wide array of disciplines and technical specialities required to fulfil its mission. Unsurprisingly this has created numerous working practices, with staff arriving from various organisational backgrounds – each bringing their previous ways of working and experiences to the company. Coupled with its rapid expansion, RWM is not yet in a position where it has established a dominant operational culture into which it can integrate the new influx of people, or position security culture as a key consideration. As such the current situation presents both a challenge and an opportunity. Members of RWM currently describe the organisation as being "On the first rung" of developing its nuclear security culture, which will take form as the organisation matures.[97] An important step of this process will be to define and articulate RWM's ethics, vision and mission statement which will include safety, security and sustainability as integrated core elements of its corporate values.[98]

RWM's embryonic nuclear security culture also suffers from a lack of firmly established security processes and their integration into working practises. RWM's security team are in the process of forming and consolidating relationships with other key security-related stakeholders, such as communications and human resources. However, as of December 2020, many security processes have been developed ad hoc and are yet to be fully embedded and integrated across departments.

The pace and scale of RWM's growth also presents a challenge for its security team in terms of integrating itself within all areas of the organisation. As noted, RWM is yet to receive sensitive nuclear information or nuclear material. As a result, nuclear security, as distinct from broader operational security, is not yet mature enough in threat and risk perception to have achieved a place which has sufficient impact, leverage and influence. As such, the organisation is still yet to adopt a

SMALL ACTIONS,
BIG
CONSEQUENCES:
YOUR GUIDE TO BEING SECURITY SAVVY

CPNI
Centre for the Protection
of National Infrastructure

FIGURE 8: SMALL ACTIONS, BIG CONSEQUENCES: YOUR GUIDE TO BEING SECURITY SAVVY (COVER)

COPYRIGHT: CPNI

[97] Ibid.
[98] Ibid.

structured approach to building a framework for a strong nuclear security culture. Currently, there is a general perception amongst the workforce that security is fragmented and can be an impediment to work. This can result in security processes being bypassed. For example, although security reviews are embedded in all work processes, as operational staff are expected to 'deliver at pace', it is relatively common for project work to commence without consulting the in-house security team. Potential security issues are then identified at later reviews, thus often work must be revised so that projects remain secure. Key lessons learnt from these situations have been early engagement with the security team so that projects can take a 'secure by design' approach, and 'avoid quick fixes' where security is 'built on' rather than 'built in.'[99]

RWM is seeking to better articulate the value of security through several means (discussed below). However, one challenge has been a difficulty in visualising potential threats and connecting their action to potential impacts.[100] This stems from the unique nature of the GDF, as well as a broader historical approach around communicating security risks within the UK nuclear industry, which has traditionally tended to be abstract and therefore hard for staff to comprehend and relate to. To overcome this, a new communications strategy is being developed, aimed at presenting clear 'hooks' so that employees understand and act to minimise security risks. In support of this, the security team is looking to draw upon examples of security culture failings from a range of industries to make security messages more relatable.

Recognising these challenges to the development of an effective nuclear security culture, RWM's security team have sought to implement a multi-pronged approach to its improvement, with key initiatives outlined below.

Increasing leadership engagement

Dedicated efforts have been made to reach out to RWM's senior executives on security to increase leadership buy-in so that, in turn, their authority can be used to implement structural changes across the company. To date, RWM's executive group have commissioned two assessments of its operational culture.[101] The first, sponsored by the Transformation Directorate, will look at RWM's broader culture as the organisation moves from a research to a delivery organisation. The second involves a workforce survey delivered by the Health, Safety, Security, Environment and Quality (HSSEQ) Directorate, which contains the security team, will seek to identify areas of improvement across the HSSEQ functions.[102]

The two pieces are complementary and intended to give a baseline understanding of RWM's operational culture, including security. As this progresses, RWM's security team has continued to e ngage with executive leadership to stress the potential impact of poor security, and enabling elements of good practice, for example, by noting how security underpins sustainability and safety. This is an ongoing long-term engagement process which may gain greater traction as RWM's engagement with the regulator increases when plans for GDF are finalised and then subjected to regulatory scrutiny. In effect, more frequent and demanding future regulatory engagement is expected to accelerate the growth of RWM's nuclear security culture. In addition to working through the HSSEQ Director, the security team have also continued to engage with the executive level

[99] Ibid.
[100] Ibid.
[101] Ibid.
[102] This survey covers five themes including: Accountability; Metrics; Working with the supply chain; Vision and values; and Executive engagement.

themselves, while also inviting external experts to deliver briefs to lend additional weight to their own messaging. In addition to the Executive, the security team has also sought to secure greater buy-in across a wide range of mid-level managers, engaging key stakeholders in HR, communications, engineering and elsewhere.

Standardising security procedures

The security team is also looking to map various ad hoc security initiatives to re-develop them into established business-wide procedures embedded within all formal company-wide processes. These include mandating the need for consultation with all stakeholders (including security) when there is a proposed procedural change, and the embedding of security-related sanctions into the HR disciplinary framework. The intention behind the initiative is to address the current negative impact of inefficient security processes and procedures which were developed without a coherent planned framework.

Security training, awareness-raising and outreach activities

The security team is working with HR to increase the regularity of security training. At present, this forms part of the staff induction process. The intent is to expand this and the technical specification for a revised training programme is currently being drafted, incorporating training requirements from across the HSSEQ Directorate. In its current form, after initial staff induction, security training will need to be periodically refreshed at least annually. To prevent over-familiarity, the new programme will emphasise the need for additional and updated training material. This is intended to keep staff informed of security threats and how to respond, with the greater variety of training material aimed at retaining staff engagement. During this training, the security team is also looking to challenge the negative light in which security is often seen in an effort to change staff attitudes. Rather than being a hindrance, key messaging during training will emphasise security's enabling role in RWM's overall mission.

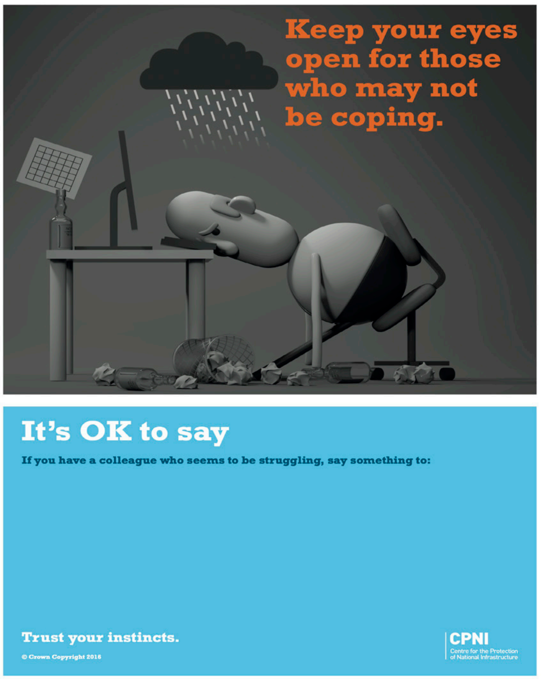

Keep your eyes open for those who may not be coping.
It's OK to say
If you have a colleague who seems to be struggling, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure

FIGURE 10: 'IT'S OK TO SAY' CAMPAIGN POSTER: 'KEEP YOUR EYES OPEN' COPYRIGHT: CPNI

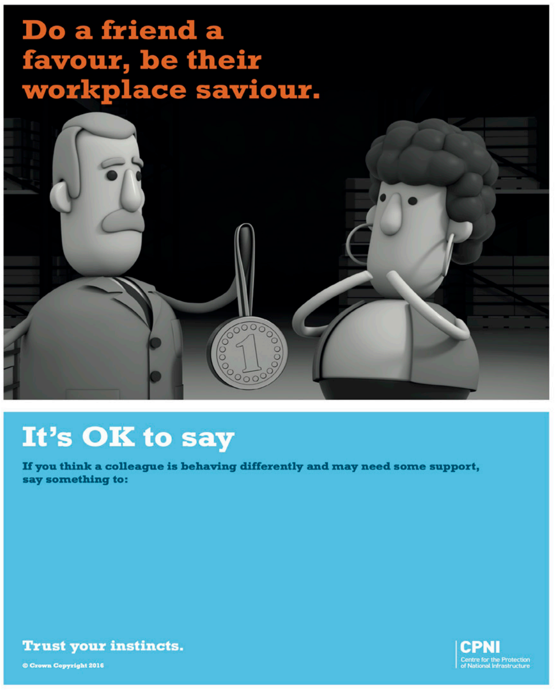

Do a friend a favour, be their workplace saviour.
1
It's OK to say
If you think a colleague is behaving differently and may need some support, say something to:
Trust your instincts.
© Crown Copyright 2016
CPNI
Centre for the Protection of National Infrastructure

FIGURE 9: 'IT'S OK TO SAY' CAMPAIGN POSTER: 'DO A FRIEND A FAVOUR'

COPYRIGHT: CPNI

Beyond its management engagement and training activities the security team is also looking to increase its broader outreach to staff members. To this end it is working with the corporate communications team to instigate security messaging, through multiple media channels. As noted, RWM's corporate values will include safety, security and sustainability. These will be emphasised through a corporate communications campaign, including in person staff meetings as well as poster campaigns, screensavers and the company newsletter. Security has also sought to piggyback on other campaigns, for example, the electronic Christmas advent calendar, wherein different departments were able to provide a message for the company's workforce which was shared across the intranet.

Summary

RWM is a company in transition, which expects to face a range of security-related challenges as it moves from a research-orientated to a programme delivery organisation. At present its security-related risks are largely reputational, for example, scenarios in which weak cyber security could serve to undermine trust in the GDF and increase local opposition to development plans. These risks will broaden and deepen in the future as sensitive nuclear information is held, construction work on the GDF commences and radioactive material is loaded into the repository.

Nuclear security culture at RWM is hampered by competing management priorities, its rapid expansion and the lack of a dominant pre-existing operational culture. This represents a challenging environment within which to embed security. Currently, nuclear security culture is embryonic within RWM, although it will no doubt improve as the organisation matures and regulatory engagement increases. Deficiencies in this area have come to Executive's attention and efforts to baseline and understand the organisation's operational culture, including security are underway.

RWM's security team have also continued to grow and work with all levels within the organisation to raise awareness of the importance of an effective nuclear security culture and how this can be achieved. First and foremost, the security team is seeking to cement its engagement with the Executive so that it can use its influence and authority to propagate reforms throughout the organisation.

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