Value and Challenges of Regularised Consultations and Information Sharing between Facility Security Managers[1]

Dr Roger Howsley

Executive Director, World Institute for Nuclear Security (WINS)

INTRODUCTION

This paper examines the role of the Nuclear Facility Security Manager and the benefit to information sharing, which has as its objective the improvement of nuclear security effectiveness. It highlights potential obstacles and advantages to developing a much more dynamic and performance-based nuclear Security Programme and the need for demonstrable competence amongst nuclear security managers, who promote a broad and inclusive attitude towards security.

TRADITIONAL ROLES AND RESPONSIBILITIES

If we were to stop and think about what we imagine different professionals to look like, how they might have been trained, their attitudes, etc. what would we conclude? Think about some stereotyped images; Bankers and Financiers, Teachers, University Professors, Nurses, Engineers. Perhaps some are easier than others.

If we were to stereotype a "typical" Nuclear Facility Security Manager, what image does the job title convey?

What about age and gender? Professional background and training? Behavioural attributes? Culture and attitude?

And if we think about a "typical" Nuclear Security Regulator, what image do we have? Is it the same or different to the Security Manager?

What images or preconceptions do we have about information sharing amongst and between these communities of professionals and between their communities and others at nuclear sites, including engineers, technologists, financiers and accountants, the research and development community? What do we imagine are the underlying beliefs amongst Security Managers about information sharing, classification guides, rules and regulations, and "need to know".

How do we think this stereotyped impression of beliefs and attitudes and behaviours amongst the security community affects the nuclear facility Security Plan and its effectiveness?

---

[1] Presented to ***Nuclear Security: Seoul, the Netherlands and Beyond,*** 13-14 Sept 2012, London

How are these attributes viewed by the rest of the employees and managers at the nuclear facility? Do we think the security departments/teams have the right attributes? Is anything missing? Would there be advantages to having additional or different attributes? How would the rest of the nuclear facility management respond to different attributes amongst the security teams and what would they like to see changed if they were asked? And are there things that the rest of the management team would need to address in their behaviours if they wanted changes in the behaviours and attitudes amongst the security personnel?

In short, if we were developing a Security Plan, or more appropriately a Security *Programme*, from scratch at a "model facility", including the selection and professional development of those people with nuclear security accountabilities, what we want to decide and how would it differ from what we typically experience at nuclear facilities? And what would this mean for information sharing and communication? What is the difference between a Security *Plan* and a Security *Programme*?

And what of the Security Regulator? Are there any changes required there? Is the regulation of nuclear security different from nuclear safety or are there common approaches and principles? Can nuclear security regulation be performance based with leading indicators and what does this mean for information sharing and communication? Is the only way to regulate nuclear security through rules and regulations?

These questions and their answers are very important if we want to achieve the most effective arrangements for security, but they are seldom asked and rarely addressed.

DEVLOPING THE SECURITY PROGRAMME AT THE MODEL FACILITY

A good starting point for the "model facility" is to ask, "Who is accountable for nuclear security?" Is it the Security Director, the Chief Operations Officer, the Chief Executive (CEO), the Board? The most likely answer is the Chief Executive, overseen by the Board; this is typically the legal position in most countries.

Is it OK for the CEO to totally delegate this responsibility to the Security Director? Would the CEO totally delegate the responsibility for safety to the Safety Director? Almost certainly not; most nuclear organisations have very senior committees that oversee nuclear and conventional safety with the clear objective of making safety a priority and ensuring that it is performance based. So, a reasonable working position is that security should be as important as safety and that it should be approached in a comparable fashion, with an inclusive oversight programme, by Functional Directors that can contribute and challenge the way that the programme is designed, delivered and measured.

But some of those in the security community might argue that significant parts of the Security Plan are classified and that having it overseen by a cross functional team of Directors/Senior Managers is not possible for reasons of confidentiality. But if we examine this position it rapidly becomes obvious that it is a false argument. Here are some reasons why:

- Custody of nuclear material is almost always with the Operational teams who are entrusted to account and control for the materials; they have complete knowledge of where nuclear materials are stored and processed and the routes by which they are moved into and out of facilities. Line management is also best placed to assess the personal behavior of staff and contractors and to detect anomalous behavior and malicious actions on plant,
- Engineering departments are generally accountable for plant modifications, design analysis, building layouts, etc and for process control, instrumentation, etc; they have an intimate knowledge of building construction and layout and the way in which control systems operate,
- Human Resource departments generally take the lead on recruitment policy, employee satisfaction surveys, training and professional development, etc; they are well placed to help assess insider threats and concerns over employee behavior, perhaps seeing patterns that are not evident to the line management of individual departments,
- Legal Departments/General Counsel are responsible for providing sound legal advice on how the organisation complies with its Licence to Operate, including security-related matters such as powers of arrest, trespass, regulatory interpretation, legal challenges and prosecutions, etc., and any actions involving regulatory deficiencies and weaknesses in corporate performance,
- IT departments are usually responsible for IT network design, implementation and maintenance, and for detecting any unauthorised intrusions or attacks; it is they, rather than the security department, that help protect, defend and investigate IT anomalies that might indicate malicious activity,
- Safety and Emergency Planning departments are responsible, amongst other things, for emergency evacuation plans and their exercising, for helping advise on how to improve operational safety through operational changes and better design, to conduct hazard analyses and response, etc.; they are intimate with safety control systems, how they might be circumvented, and how sequences of fault conditions (caused by accidental or malicious actions) could seriously affect critical safety systems.

All of the above have significant influences and interactions with the management of security and all of these interactions need to be thought through as a team and

decisions taken about how to make the security "programme" more inclusive and effective. Appointing an Executive Committee of Directors, responsible for the oversight of nuclear facility security, is a highly effective and efficient way of achieving this goal, but what does this mean for the organisation and what changes might it drive?

Examples include:

- The Security Community will need to think about what, if anything, in their Security Plan is highly confidential (secret) that cannot be shared on a controlled basis with other Functional Directors, on behalf of the CEO who we have already concluded is accountable to the Board for security performance. Certain armed response tactics might be included in the list but a useful exercise for our model facility is to attempt to highlight possible areas of secrecy and to see if they withstand the challenge that they cannot be shared, on a controlled basis, and to repeat this exercise under what would be "normal" and "emergency" facility conditions. This will highlight an important principle of security; that of risk management, because information sharing under "normal" conditions may be considered by the security community as unacceptable but which under emergency conditions become essential. Unless there are mechanisms to share the information under emergency conditions and the implications of this "new" information to the rest of facility management are acceptable and/or actionable, then difficulties are almost certain to arise.

- Secondly, the Functional Directors which comprise the Oversight Committee need to know what strategic and operational questions to ask about security. They almost certainly need to have a level of competence in the security field that is higher than they currently think they do, in order to properly consider the interactions with and consequences for their areas of delegated accountability, and how they can contribute to the Security Programme. How do they get this insight, where might "best practice" be defined and where do they go for this training?

Having established cross-functional oversight of the Security Programme, the original "Secret" Security Plan agreed with the Security Regulator may suddenly look inadequate and narrow in scope, leaving many questions unanswered. There may be recognition in the organisation that a more comprehensive and dynamic approach needs to be taken to security planning and execution. There may also be recognition that investment decisions, both for capital and operational security expenditure, need better oversight, given their expense and the increases over recent years. Questions may start to be asked by the other Directors about security performance; "What are we getting for the investment in security?" "What has changed or

improved since we made these investment decisions?" Performance metrics may begin to emerge, both lagging and leading metrics, which can be discussed at and by the Oversight Committee.

Critically, questions may also begin to emerge about benchmarking and comparative performance; "How does our performance compare to Organisation B's?" what does Organisation B spend on …; How have other organisations dealt with this particular problem? Do we apply best practice in this area?

This relatively simple process of involving cross-functional oversight and thereby asking questions and taking a more inclusive approach to security management can have a dramatic impact on the way that security is perceived by an organisation; old approaches based on secrecy and compartmentalisation suddenly seem outmoded, ineffective and inefficient. Information sharing becomes the norm and joint accountability develops.

Ironically, for the Security department and the Regulator who previously controlled the Security Plan and felt comfortable with it, this "new" approach to the Security Programme can have significant benefits for security implementation. But success depends on changes in attitude and a framework for professional development that is generally absent in most nuclear organisations.

PROMOTING SECURITY LEADERSHIP AND EFFECTIVE SECURITY PROGRAMMES

Having used the concept of the model facility to examine new ways of improving the effectiveness of nuclear security and having identified the key factors that influence performance and ownership, we must now consider the actions necessary to make these changes in practice in as many organisations as possible with custody of nuclear and other radioactive materials.

WINS has been active over the last three years developing materials and mechanisms to support these changes and to promote their implementation, including;

- Promoting security as a management activity rather than an area of just technical expertise; clearly there is a need for specialists in physical protection, cyber security, personnel security etc, but these have to fit within the inclusive management and organisational framework described above

- Identifying best management practices for security, rather than listing technical requirements or rules that must be complied with. WINS has published over 25 International Best Practices for Security Management[2] based on facilitated workshops on five Continents. Each Best Practice Guide is authored by a seasoned professional who has done the job and

[2] See Annex 1

experienced what it takes to do it right; and the Guides are peer reviewed by other practitioners to try and make the advice as relevant as we can. The Best Practice Guides are closely aligned to the "requirements" of INFCIRC 225/Rev5 and complements the work of the IAEA that encourages its Member States to adopt sound principles of nuclear security,

- Recognising that security "knowledge" needs to be available to functional departments other than Security so that they are competent to oversee the security programme and understand the interactions with other organisational activities, priorities and strategy. Most Functional and Business Directors, including the CEO and the Board, need proper induction and professional development in nuclear security management in order to discharge their own accountabilities and the mission of the organisation. But, currently, this is frequently overlooked because organisations are stuck in the old model of there being a Security Plan that is owned almost exclusively by the Security department.

This latter point relating to professional development is the key to more effective security management in the future, and WINS has begun to address that through the launch of the WINS Academy[3].

PROFESSIONAL DEVELOPMENT

The basis for professional development is to understand the requirements of the profession and to ensure that practitioners are well trained and certified to undertake the task, particularly where there are public or societal service dimensions to the profession, as is usually the case. No one would undergo surgery with an unqualified surgeon or board an aircraft piloted by someone who might have taken some flying lessons but who didn't demonstrate their competence through testing and examination. So, is it reasonable to ask whether those with nuclear security accountabilities have responsibilities with a public or societal responsibility? Are there any potential consequences to the public or society if those managers with security responsibilities make bad or ill informed decisions? WINS believes that there are and that the professional development of such managers is of fundamental importance and has been seriously overlooked by practitioners and their regulators.

For that reason, the WINS Academy will work to establish role definitions for typical nuclear managers with such responsibilities and define a competency framework and training materials. These will include Board Directors, CEOs, Functional Directors, etc so that there is a comprehensive programme of professional training available.

[3] See the WINS website www.wins.org for further information on the WINS Academy and the programme of implementation

PEER REVIEW

The ultimate aim of establishing a new framework for security through the development of Security Programmes and professional development is to encourage the peer review of security by practitioners. Peer review is well established in the nuclear safety field and has resulted in marked improvements in safety and operational performance, as evident through the work of INPO and WANO.

Security peer review has lagged behind for many of the reasons already identified in this paper; unnecessary secrecy and an ill-founded belief that security is the responsibility of the Security department, its regulator and ultimately by the individual State concerned. There is no doubt that accountability for security frequently rests with the State; for matters of legislation, regulation, and State-related agencies that provide intelligence, border controls and armed response capabilities. But it is equally true that the peer review and sharing of information by practitioners that implement nuclear facility Security programmes are also important and necessary to identify and implement best practices on the ground because it will be the action taken in the first few minutes of a terrorist attack that will determine the future shape of events and their potential consequences. The international community, States and their regulators, and the industry itself would be well advised to recognise these benefits and to take action to improve information sharing in a controlled manner.

ANNEX 1: BEST PRACTICE GUIDES PUBLISHED BY WINS

	BEST PRACTICE GUIDE TITLE
1	NUCLEAR SECURITY FOR SCIENTISTS AND ENGINEERS
2	LEARNING FROM OPERATING EXPERIENCE
3	HUMAN RELIABILITY
4	EFFECTIVE SECURITY REGULATION AND IMPLEMENTATION
5	TRACKING TRANSPORT OF NUCLEAR MATERIAL
6	SECURITY OF HIGH ACTIVITY RADIOACTIVE SOURCES
7	MAKING SECURITY EFFICIENT
8	MODELLING AND SIMULATION IN NUCLEAR SECURITY
9	WORKING EFFECTIVELY WITH EXTERNAL RESPONSE FORCES
10	GUARD FORCE TRAINING AND MOTIVATION
11	SECURITY EXERCISES
12	MATERIAL CONTROL AND ACCOUNTANCY IN SUPPORT OF NUCLEAR SECURITY
13	NUCLEAR SECURITY CULTURE
14	SECURITY EQUIPMENT MAINTENANCE
15	MANAGING INTERNAL THREATS
16	THREAT ASSESSMENT
17	SECURITY GOVERNANCE
18	ACCOUNTABILITY AND LIABILITY FOR NUCLEAR SECURITY INCIDENTS
19	INTEGRATED APPROACH TO NUCLEAR SAFETY AND SECURITY
20	SECURITY BY DESIGN
21	MANAGEMENT AND DEPLOYMENT OF ARMED GUARD FORCES
22	NUCLEAR SECURITY GUARD SELECTION AND RECRUITMENT
23	SECURITY OF WELL LOGGING RADIOACTIVE SOURCES
24	SECURITY OF IT & IC SYSTEMS AT NUCLEAR FACILITIES
25	COMMUNICATING NUCLEAR SECURITY INFORMATION