WINS-SASIG Roundtable on "The Business Case for Security Investment"

London, UK. 14-15 February 2019

REPORT

INTRODUCTION

Nuclear sites are spending considerable time and money on upgrading security arrangements to meet more and more stringent corporate and regulatory requirements. Increases in operational security costs at nuclear facilities have risen steadily over recent decades; estimates now suggest that the operational security budget at nuclear power facilities has increased by a factor of x4 since 9/11; what used to cost 5 million now costs 20 million.

Much of the increase can be attributed to the cost of enhanced guarding arrangements, a higher ratio of armed guards or police being deployed at nuclear facilities, and greater attention being given to cybersecurity measures.

In spite of such expenditure, however, it remains difficult to analyse security costs in order to determine whether the security choices being made are also the best investment decisions and to demonstrate whether the balance of expenditure is right.

It's a complex problem that starts with the national threat assessment, the design basis threat for the nuclear sector and the assumptions made about adversary capability and intent. It also depends on the risk appetite of the government, regulator and licensee and their assessment of the reputational and financial consequences of a successful attack on security.

We know that calculating a conventional return on investment (ROI) is challenging for nuclear security programmes because of the lack of real data, but that doesn't lessen the need to prioritise and justify security expenditure. Nor does it lessen the need to justify the balance between expenditure between security areas, such as physical protection, cybersecurity and security awareness/culture.

A lot can be learned from other business sectors, such as aviation, where the analysis of ROI and annualised loss expectancy (ALE) are required to justify whether a particular security investment is worthwhile. Although the nuclear industry operates in a different context, how organisations approach security expenditure analysis is comparable. Encouraging a wider discussion on nuclear security expenditure and reviewing security expenditure analysis originating from other sectors would support the development of financial models to help inform decision makers in the nuclear industry. Ultimately, it would lead to identifying metrics that help to ensure security expenditure is targeted at the most effective measures and unnecessary expenditure are reduced.

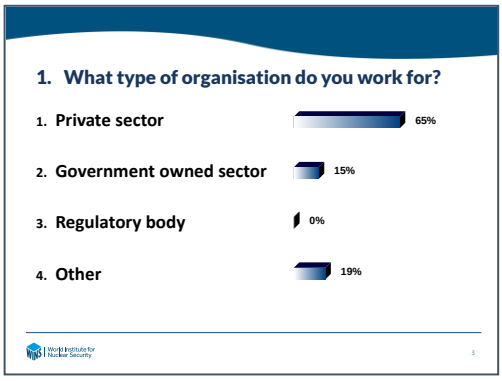
OBJECTIVES OF THE ROUNDTABLE

The Security Awareness Special Interest Group (SASIG) and the World Institute for Nuclear Security (WINS) partnered together to give senior security professionals from all sectors an opportunity to debate these issues, share best practices and new approaches, and encourage the development of financial models that help to inform decision makers in the security industry.

This joint initiative was designed to answer the following questions:

- What is the current state of security expenditure and the trends that are being observed?
- What systems of risk assessment and investment justification methodologies are currently being used?
- How credible is it to allocate financial expenditure to each major element of the design basis threat? Would this provide useful information?
- How useful is modelling and simulation to help assess whether security expenditure is effective and efficient?
- What can we learn from the risk management approach to safety and other fields in the nuclear sector?
- What can we learn from other sectors that need effective physical protection, such as aviation security, and that are experiencing cyberattacks?
- Are there technological developments that could reduce the financial costs of security? Over what timescale might they be deployed?

The roundtable was hosted by Burges Salmon in London on 14 and 15 February 2019. It brought together a group of 40 experts and leading thinkers in security matters, performance evaluations and financial matters. The event, which was professionally facilitated by Mr Julian Powe, included expert presentations and plenary and breakout sessions to provide maximum engagement. In addition, an instant electronic voting system was used to allow participants to anonymously share their views on selected questions.



ROUND TABLE PROGRAMME

DAY 1: THURSDAY, 14 FEBRUARY 2019

OPENING SESSION

Mr Ian Truman, Legal Director, Burges Salmon and **Mr Martin Smith, Chairman and Founder of the SASIG**, opened the event, greeted the participants and delivered brief welcoming remarks. **Dr Roger Howsley, WINS Executive Director**, welcomed the participants on behalf of WINS, detailed the objectives of the round table and provided a preliminary overview of the agenda.

Participants' expectations

Participants were then asked to introduce themselves at their tables and to share their expectations for the roundtable. Examples of their remarks include:

- Information and idea sharing. Take general experience, hone it down and re-apply to our own issues.
- Understand what is out there. Update/refresh our practices, look at different cultures, benefit from opportunities to improve by learning from someone else.
- Increase the function of security as a business enabler. Provide a stable platform.

- Understand the needs of the customer, tailor the service to the need.
- Harness the different disciplines in the room.
- Support alignment of security investment and need. Better communicate on security investment and its benefit to the organisation.
- Better engage with the board and the organisation as a whole.
- Understand how others estimate their return on investment (value for money).

SESSION 1: THE NUCLEAR PICTURE

The objective of Session 1 was to provide an overview of security expenditure in the nuclear sector, review trends observed in the last 10 years, and address the extent to which nuclear security expenditure are driven by regulators and/or external events. It also gave participants the opportunity to discuss various methods of risk assessment and investment justification methodologies that are currently being used and to explore possible differences between the nuclear industry and other sectors.

Ms Susan Perkins, Nuclear Energy Institute (NEI), USA, opened Session 1 with a presentation on security expenditure by US utilities. After providing an overview of the role of NEI, Ms Perkins briefly described key security regulatory requirements for nuclear power plants in the US and the physical security programme implemented by operators. She also provided some figures on various security costs and compared them to other operational and capital expenditure.

Achieving business discipline in security

In an E-voting question on expenditure justification, the majority of participants indicated that they believe it is possible to apply business disciplines to justify security expenditure. In a brief discussion of the E-voting results, many participants claimed they were already doing this since it forms the basis of any effective risk management approach. They also indicated that security capital expenditure is approved in the same way than other expenditure because security is simply a category of risk to be addressed (a specialist business but not a special one).

Risk assessment and investment justification

Mr Mark Neate, Sellafield Ltd, UK, provided a second nuclear perspective on the topic. He began by describing some of the activities that are conducted at Sellafield and the complexity of the associated regulatory environment. He then explained Sellafield's overall approach to managing environmental, safety and security risks, as well as recent efforts to achieve unified command and control. In addition, Mr Neate described Sellafield's risk management and assurance frameworks and provided detailed information on security expenditure and a breakdown of costs.

Participants were then asked to discuss risk assessment and investment justification methodologies at their tables and to identify usual pitfalls. Key findings from the discussions were:

- Risk perception and reality differ. Emotion is a driver, especially regarding nuclear matters.
- The type of regulation impacts the investment decision making process. Outcome-based regulation is usually more flexible, but it should preferably include some prescriptive requirements, such as for corporate governance and reporting.
- It is essential to understand the company's risk appetite, where the risk lies, and who owns the risk when it crystallises.
- You need to walk the board through risk scenarios. What is the probability they occur during board members' term of service? Within a 10-year cycle? You need to translate risk management expert messages into a narrative which can be understood at the board level.
- Business cases should focus on objectives not processes. Throwing money at processes does not always lead to results.
- You need to identify influencers. Some people may not have budgets but a lot of influence.
- It is essential to develop integrated approaches addressing all risks and to focus investments on maximum expected outputs. There is a need to demonstrate that security is an investment, not just a cost, and to communicate on the benefits of security resources for other purposes (e.g. emergency preparedness).
- Physical and cyber security have different risk mitigation philosophies. Each sector adapts to its assumptions and perceptions.
- Risk needs to be quantified. Figures are important. It is challenging to have quantified risk indicators for nuclear security (not enough incidents). It is difficult to have a sensible discussion and effectively address a low-likelihood event that could have a massive impact.
- Measuring impact is essential to determine if investment is effective.

SESSION 2 - ALIGNING SECURITY EXPENDITURE TO THE POSTULATED THREAT

The objective of Session 2 was to review the possibility of allocating financial expenditure for security to each major element of the design basis threat and to discuss whether such an approach would provide useful information.

Mr John Patterson, Mission Analysis Limited, UK, initiated the discussion with a case study based on his career experience in the UK Army. The study demonstrated the challenges involved in designing and implementing security systems that address the concerns, priorities and risk appetite of different stakeholders involved in a project.

Mr Jonny Price, EDF Energy, UK, provided a complementary perspective with a presentation on the UK regulatory context and current trends in security costs. He also described EDF's overall approach toward security assessment and planning and some challenges his organisation faces when considering security investments.

In response to an E-voting question, 80% of participants agreed that security expenditure could be allocated to different elements of the security threat. However, a participant also commented that cost can only be broken down to a certain level of detail and that the process itself is not obvious or even always meaningful. (You might be able to identify expenditure, but does this mean you can measure actual impact and benefit?)

Participants also mentioned the value of assessing the cost of a security function but agreed that the task is complex, especially when it comes to integrating multiple budgets and objectives (cross-cutting approach and impact). They added that boards want visible signs (quantified evidence) that the organisation is responding to specific threats (cyber threats, insiders, etc.) that have caught their attention. They agreed that more transparency on security expenditure would support benchmarking but also said that many organisations are still reluctant to share such information.

SESSION 3: BENCHMARKING RISK MANAGEMENT PRACTICES AND INVESTMENT JUSTIFICATION METHODOLOGIES FROM DIFFERENT SECTORS

The objective of Session 3 was to foster the exchange of experiences among participants from the various sectors represented at the roundtable and to explore cybersecurity risk management practices and investment justification in greater detail.

Mr Mark Raeburn, CEO and founder of Context Information Security, UK, offered a perspective on cybersecurity and associated risk management practices. He emphasised how quickly the landscape changes in the cyber world and how important it is to educate senior managers and other decision makers so they can better understand the risk, as well as tools and techniques that help to mitigate it.

Follow up discussions revolved around key considerations for good investment decisions. Participants agreed that good investment is a collective effort that requires identifying priorities and focusing on expected outcomes. They also said there is a need to develop short- and long-term approaches to risk mitigation and encouraged the use of dedicated tools, including modelling and simulation, to support the decision-making process. Participants also recommended using a common language that is adapted to decision makers and developing a common understanding of the risk terminology (common format), including common indicators/criteria (common metrics).

SESSION 4: REDUCING THE COST OF SECURITY WHILE MAINTAINING ITS EFFECTIVENESS

The objective of Session 4 (the last session of day 1) was to identify security metrics and assessment processes that can support security decisions and demonstrate whether security is being managed efficiently.

Ms Lisa Clarke from Bruce Power, Canada, opened Session 4 by with a general overview of Bruce Power and its overall approach to security risk management. She then described the usual drivers for security expenditure and how Bruce Power Emergency and Protective Services approach to developing a long-term strategy for security investment. Ms Clarke also described some good practices for raising the profile and credibility of the security function in the organisation and ensuring its effective integration into the strategic missions of the company. She concluded her presentation with a case study on investment prioritisation and security equipment selection.

In a complementary presentation titled *Refreshing a Cyber Security Strategy*, **Ms Alison Dyer, Urenco UK,** described her organisation's strategy for conducting a comprehensive review of the cyber risk and for developing an action plan that helps to mitigate the identified risks. She also explained the process for conducting a risk assessment and what the outcomes of such a process are, including a board paper and costed plan. She concluded by sharing some lessons learned from conducting a comprehensive review of cyber risk.

Building on the two presentations and as final exercise of the day, participants were asked to review and discuss performance metrics for human reliability and cyber and physical protection. In particular, they were asked to identify the most important leading metrics that demonstrate resilience should an organisation be attacked and how to frame these metrics in a manner that would convince decision makers.

A majority of participants indicated they do not believe that strong performance metrics for security programmes are well established. They highlighted the importance of leading indicators and encouraged organisations to try to move away from lagging indicators, especially in environments where not many incidents happen. It is important to ask the right questions: For example, organisations should ask if they would be resilient to an attack and for evidence to be provided.

Participants also offered some advice for developing metrics for human reliability, cyber and physical protection:

- For PP, design metrics around people, equipment and performance. Measure the proficiency of your guard force. Assess the health status of your engineering systems.
- For HR, develop the *guilty person* concept. Also develop indicators that characterise an organisation's culture.
- For cybersecurity, develop metrics around confidentiality, integrity and availability issues. Assess your level of exposure and capabilities to respond (return to business as usual). Be clear on your assets. Protect your key information.

DAY 2: FRIDAY 15 FEBRUARY 2019

Before moving to the final session of the roundtable, participants were asked to reflect on what they had heard during the first day and to share their preliminary findings and take-aways. They were also asked to give their overall view of security in the nuclear sector and make suggestions for how it can be enhanced. Following are some of their comments:

- Many different stakeholders play a role in mitigating security risk. Organisations need to develop an integrated approach toward risk management.
- Risk profiles differ. Security needs and practices reflect these differences.
- Regulators have a role to play and need to work together to ensure comprehensive and complementary oversight.
- Too much attention sometimes goes to regulated areas, thereby short-changing other business areas. More focus should be given to investors, including developing specific metrics for them.
- We don't know whether we are quick enough at responding to emerging threats. We need to raise awareness, change the narrative and ensure that we recognise security as a business threat.
- We need flexibility to develop cost-effective security measures. We need creativity and good messaging/narrative. Regulatory compliance does not always mean effective security. Outcome-based regulations support flexibility and facilitate investment justifications.

- Language is very important. For instance, cost reduction requirements can be converted from a constraint to an objective. Do not emphasise cost reduction, but do highlight value added (e.g. sustainability, commercial imperative). Whenever possible, identify and communicate on the cost savings for the customer.
- We need to do a better job at security perception. We do not need to have visible guards to have good security.
- Nuclear industry investment in cybersecurity seems low. Are we slow to understand the risk? Do we have other priorities? Are costs reflected differently (corporate vs. facilities)?

SESSION 5: ESTABLISHING A BUSINESS CASE FOR SECURITY

The final session of the roundtable was designed to consolidate the key findings of the event and to explore how to develop a convincing business case for security investment. It also gave participants an opportunity to review the most effective communication methods between the executive team and the board.

To initiate the discussions, **Mr Mark Denn, Nehemiah Security, USA,** offered a perspective titled *The Business Case for Cybersecurity Investment.* He highlighted the importance of meaningful cybersecurity metrics and the challenges of extracting relevant information from the mass of collected data. He emphasised the need to put information in context and explained some options for providing the board with the information they need to take appropriate decisions.

During the E-voting questions that followed this presentation, a majority of participants disagreed with the statement that 'it is easier to justify investment in cybersecurity than in physical protection. They also disagreed with the statement that 'Chief financial officers and chief executive officers are easy to convince to allocate more resources to security'.

In a follow-up discussion on how to develop a convincing case for security, participants mentioned the importance of normalising language and adapting it to the board's business culture. Organisations are more and more viewing security risk as a normal risk; similarly, they believe that associated management practices should be the same as for any other risk. Trying to scare the board with potential consequences of a security incident is not usually a good practice. In general, board members start to develop a good understanding of security because they could be held liable should a security incident occur. (Insurance is a key driver of this evolution.)

Participants also discussed cybersecurity reporting and accountability lines and how to ensure optimal oversight and maximum benefit to the organisation. They had different perspectives about this issue, but generally said that cybersecurity should not report to the IT or PP heads and that a direct line to the C-level could be more appropriate. However, whatever the reporting lines, everyone agreed that it was important for the overall security programme to properly integrate cyber security and physical protection.

In the final task of the session and roundtable, participants were asked to form subgroups and prepare for a (fictional) investment justification meeting among the CSO, CFO and CEO of an organisation.

WAY FORWARD AND CONCLUSION

In conclusion of the event, participants shared some of their take-aways and key messages, in particular those for representatives of the nuclear industry. Examples of their comments include:

- Is there too much focus on satisfying the regulator? (i.e. actions taken are in order to achieve minimum compliance);
- We need to increase the role of industry bodies and to develop a common language, best practices and meaningful metrics. We also need to better engage the regulator;
- We can start thinking outcome-based for our security programmes well before the regulations evolve away from prescriptions;
- We need to embed security into business discipline and usual management and oversight practices. We also need to develop commercial arguments. Increasing competences within the group in charge will support such evolution;
- It is essential to harmonise/normalise security language. Do people understand what we say?
- Better integrating cybersecurity in the usual DBT frame will support this effort of normalisation;
- We need to share more examples of risk management methodologies and support the learning from experiences of successful changes.

In his concluding remarks, Dr Howsley, WINS, thanked participants for their active contributions to the roundtable, which had made the event a success. He said that the messages he had heard during the last two days were very important, and he committed WINS to sharing them with all of its members and beyond. He also emphasised the continuing need to ensure that organisations effectively include security matters in their overall risk management framework. In addition, Dr Howsley emphasised the importance of helping security departments acquire the necessary skill to develop business cases for security and to adapt their language so they can communicate their needs and priorities effectively. He also said that WINS will continue exploring the mechanisms involved in incentivising companies to report on their security governance and arrangements. Finally, Dr Howsley thanked SASIG for the opportunity to partner on this important topic and expressed the hope of continuing this successful collaboration to provide organisations with further risk management strategies and guidance.

In the final closing remarks, Martin Smith, SASIG, said it had been a privilege to meet new people and learn from different practices. He also said he would like to cooperate with WINS again in the near future.