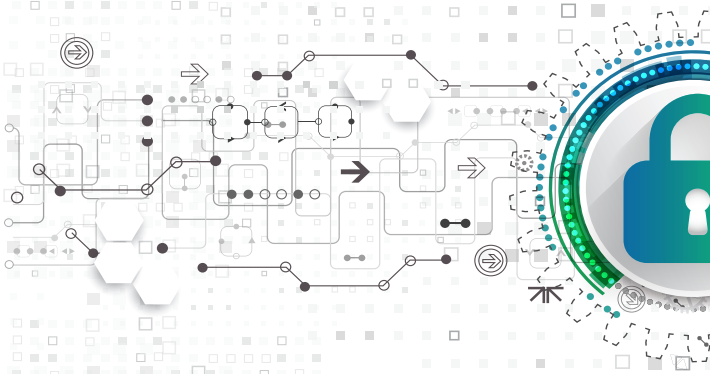
STIMSON

Demonstrating DUE CARE

Cyber Liability Considerations for Nuclear Facilities

by Kathryn Rauhut and Lovely Umayam



EXECUTIVE SUMMARY

Cyber security is the next frontier for nuclear risk managers. Cyber attacks continue to evolve in sophistication and stealth, making it challenging to develop an effective approach to risk management. Although there is consensus within the nuclear industry that it must bolster its capacity to "remain ahead of the dynamic cyber threat curve,"[1] it is important to clarify what this means in practice. What constitutes a *reasonable* application of cyber security measures such that they sufficiently reduce vulnerabilities and associated risks?

In November 2016, the Stimson Center, along with the Security Awareness Special Interest Group (SASIG) and the World Institute for Nuclear Security (WINS), hosted The *Nuclear Security Roundtable on Executive and Corporate Responsibility* in London. The day-long roundtable brought together fifty industry stakeholders and cyber security experts to discuss the challenges inherent in managing cyber security risks in the nuclear sector and ways to address them. During the roundtable, participants examined a hypothetical cyber attack scenario in a nuclear power plant that undermined the security posture of the facility. The cascade of events resulted in a major power outage and led to first-party property damage, reputational fallout, significant third-party business interruption losses, injury and death.

Under this scenario, participants considered potential negligence claims and corporate liability; they also considered how a model of accountability demonstrating compliance to high industry standards might be structured to mitigate such liability.

The exercise resulted in the following key findings:

Corporate decision-makers struggle to determine the *value proposition* of additional cyber security enhancements. Due to the dynamic nature of the threat, it is hard to ascertain when enough effort to reduce the risk has been taken. This is further complicated by the challenge of communicating risk management decisions to non-specialist board directors and executives, as well as to shareholders and the public. It is difficult to quantify the effectiveness of additional security since the most convincing evidence is the *absence* of a cyber incident or a successful mitigation of an incident in progress and/or management of the response. Therefore, it can be hard to justify additional spending and the reallocation of resources towards further voluntary cyber security measures.

Determining the proportionality to allocate towards cyber security measures vis-à-vis other risk considerations is challenging in a resource-constrained environment. Cyber security is just one of the variables considered in a risk portfolio along with other security-related risks including safety and emergency response.

Identifying the perpetrator of a cyber attack could have significant implications on insurance coverage. If the perpetrator of an attack turns out to be a state (as

1. Nuclear Industry Summit. Working Group 1. Managing Cyber Threats. (March 30, 2016). p.3. http://nis2016.org/wp-content/uploads/2016/02/Working-Group-1-Report-Managing-Cyber-Threats.pdf.

has occurred several times in recent years), the attack could be interpreted as an act of war. This changes the threat profile to a state-level concern, which could have implications for operators since their insurance cover might be voided due to force majeure clauses.

Although cyber-related risks remain underinsured, many industry actors across all business sectors mistakenly believe that they would be sufficiently insured in the event of a cyber attack. This belief is further complicated in the nuclear sector because third-party liability coverage under the nuclear liability regime would only be triggered if the incident results in a radiological release to the environment. In the event of a cyber breach that leads to non-radiological damage (e.g., third-party business disruption from a power blackout), claims would have to be covered by conventional insurance. The cyber insurance market is currently engaging with the nuclear insurance market to try to tailor existing cyber coverage for nuclear power plants, but these discussions are still in process.

In the aftermath of a cyber security event at a nuclear facility, operators will have to demonstrate that they took all reasonable measures to protect against the attack. *Reasonableness* is currently determined by taking into account various factors including relevant standards, rules, any existing domestic regulations and industry norms. While these are effective measures to a degree, they do not encourage the adaptive mindset necessary when responding to a complex cyber environment. Furthermore, industry norms are not internationally agreed. Thus, it is in industry's best interest to develop internationally agreed cyber security norms that can be used to determine reasonableness. In the absence of an agreement, reasonableness will be decided by a judge or jury.

There is an emerging interest within the nuclear industry to develop and adopt a governance template that could demonstrate due care in either preventing or managing the response to a cyber security incident. Such a template could include criteria for good corporate governance, strong security culture, and cyber security best practices. If these criteria are met or exceeded, it could serve as a means to demonstrate that a given company or operator took all reasonable measures to mitigate its cyber security risks.

A well-developed governance template could provide evidence of duty of care following a cyber security incident which over time could become legally binding. Roundtable participants expressed support for the development of such a template in cooperation with civil society organisations and appropriate government entities. Defining what is unacceptable and acceptable behaviour in advance will encourage better risk reduction measures.

BACKGROUND

Technology has revolutionised business practices around the world as organisations have automated critical operations and engaged in the digitised economy. Although technological innovations have significantly streamlined operational processes and ushered in unprecedented productivity, they have come at a cost. Integration and reliance on complex digital components and systems expose businesses to ever-evolving and constantly multiplying cyber threats. Although governments and industry have sought to implement measures to prevent exploits and breaches, they have often failed to keep pace with the creativity and cunning of cyber adversaries.

In fact, the world is now experiencing a surge in cyberattacks, some of which are being operationalized by nation states. For example, the Ponemon Institute found that a sample of 237 organisations experienced a total of 465 discernible cyber attacks *each week* in 2016.[2] The US Department of Homeland Security reported that its Industrial Control Systems Response team addressed 295 cyber incidents in 2015, a 20% increase from the previous year.[3] It is consequently not far-fetched to worry about catastrophic cyber attacks on critical infrastructure, including nuclear installations.

2. Ponemon Institute. *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*. (February 6, 2017). http://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation.

3. US Department of Homeland Security. *NCCIC/ICS-CERT Year in Review*. (2015). https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

Indeed, the civil nuclear community, which has traditionally emphasised physical protection, has begun to view cyber security as a core component of the nuclear security architecture.

Although governments and nuclear industry players are now collaborating actively to improve cyber security through the development of frameworks, regulations and guidance documents, compliance with minimum standards alone is not enough to protect facilities and manage response to cyber attacks. It is in nuclear industry's self-interest to identify business incentives that encourage organisations to implement, embed and maintain effective cyber security practices within the security culture of their entire workforce.

Early in 2016, the Stimson Center nuclear security team launched a project exploring how market forces (economic incentives in insurance and financing) and intrinsic values (corporate social responsibility and accountability) could incentivise the nuclear industry to voluntarily adopt more robust nuclear security measures. Stimson's initial efforts have been very well received,[4] particularly the subset of work that examines how executive-level security risk assessments could frame nuclear security as a valuable component of a company's business operations and also lead to smarter security spending.

Complementing this project, the Stimson Center, the Security Awareness Special Interest Group (SASIG), and the World Institute for Nuclear Security (WINS) organised the *Nuclear Security Roundtable on Executive and Corporate Responsibility* in London on 22 November 2016 to explore potential drivers that could motivate organisations to implement additional cyber security practices beyond the baseline of regulatory compliance. The event highlighted, in particular, the underexplored topic of how to use tort liability[5] to address failure to adequately protect against a cyber security incident at a nuclear facility when no release of radioactive materials occurs. By looking at an incident that did not result to a radiological release, participants explored circumstances in which existing nuclear liability regimes did not apply but still produced catastrophic damage, such as disruption to the power supply.[6]

Internet vulnerabilities at a power plant extend well beyond privacy breaches; a cyber attack could cause physical damages that could in turn lead to property damages, loss of life and injuries. This fact raises a key question: What is a company's duty of care in its oversight and management of cyber security risks, and what does corporate accountability look like if it fails to uphold this duty? The following discussion helps nuclear industry actors, particularly executive-level managers, consider cyber-related risks in their overall risk-calculation and the possible ramifications that could ensue should a cyber security incident occur at a facility for which they have responsibility.

THE VALUE PROPOSITION OF SECURITY

One of the fundamental challenges that executives across business sectors face is how to manage security risks and determine the appropriate response measures. Executives must not only know when to take action to minimise security risk, but also to recognise when a certain action is enough. In an aggressive, outcome-focused environment with various financial constraints, it can be challenging for executive-level risk managers to ascertain the v*alue proposition* of security. In essence, this means determining the value of implementing certain security features in relation to other facets of the business such as operational efficiency and profitability.

The fact is that complete security can never be definitively achieved. There will always be some residual risk that cannot be prevented or is beyond the design basis threat. And as the nuclear business adapts to new technologies and emerging security threats in cyberspace, the dynamic nature of security makes it challenging to quantify which measures

4. Decker, D., & Rauhut, K.. *Nuclear Energy: Securing the Future: A Case for Voluntary Consensus Standards*. Stimson Voluntary Consensus Standard Report (2016). https://www.stimson.org/content/nuclear-energy-securing-future-case-voluntary-consensus-standards.

5. Tort liability is the legal obligation of a party to provide remedy to a victim of a civil, not criminal, wrong.

6. Note that international nuclear liability treaties generally cover damage from radiological releases or a precautionary action, such as an evacuation, related to a potential release.

are *reasonable*. Unfortunately, reasonableness is a social and legal construct, not a scientific one, and it does not lend itself easily to measurement. The challenge here is that (as one participant summarised) "You can't prove it if you can't measure it."

The artificial separation between safety and security also compounds the competition for resources. Although security is often included in general risk reduction considerations, safety is likely to receive priority because it is associated with high hazard risks that have the potential to incur considerable costs, including loss of life. Furthermore, because numerous safety-related accidents and incidents have occurred in the past, it is easy to understand their potential consequences. In contrast, few security incidents have taken place, and those that do occur are often not publicised. Although there are significant differences between safety and security, more needs to be done to identify their commonalities so that investments are not made in one at the expense of the other.

CYBER INSURANCE COVERAGE

The international nuclear liability regime was created to supplement national laws with international conventions that can address the potential cross-boundary consequences of a nuclear incident. A radiological release caused by a cyber attack would be covered by current nuclear liability policies. Liability in this case is strict and absolute, regardless of fault, which means that negligence does not need to be proven. It is channelled to the operator, who assumes complete responsibility; however, it is limited in amount and scope by legislation and conventions. The state accepts responsibility as the insurer of last resort.[7]

Thus, a purpose of the nuclear liability regime is to compensate victims from losses associated with trans-boundary exposure to radioactive contamination that could be so widespread and catastrophic it would be uninsurable in the conventional market. Non-radiological related losses such as personal injury, wrongful death, third-party business interruption and reputation may be covered under a company's commercial general liability, property or business interruption polices.[8]

Specialty cyber insurance policies were developed to cover losses associated with data privacy breaches, but they do not generally address cyber attacks that lead to large-scale physical damage. These policy limits are not intended to absorb catastrophic losses from a significant cyber terrorism event that causes, for example, disruption of the energy supply. Some recent policies in other industries have added the Institute Cyber Attack Exclusion Clause (CL 380),[9] and it is foreseeable that exclusions of this nature may also develop in the nuclear insurance market. Consequently, cyber insurance still needs to be developed to cover non-radiological—but potentially catastrophic—threats to nuclear power plants.

There are several barriers to this type of coverage. First, the potential loss from a catastrophic event would make the insurance premiums too costly. (Initial government financial backing could be used to stimulate a cyber insurance market similar to that found in the terrorism risk insurance markets.) Another problem with cyber risk is the under-reporting of incidents. Because many attacks are not disclosed, there is a lack of actuarial data to develop and inform more sophisticated cyber risk management products. Enhanced cyber incident data sharing and analysis could help provide insurers with the information they need to develop insurance coverage while advancing enterprise-wide cyber-risk management practices.

A HYPOTHETICAL SCENARIO

To challenge assumptions and stimulate thinking around cyber threats to nuclear facilities, roundtable participants were presented with a hypothetical scenario in which an unknown adversary carries out a cyber attack on a nuclear

7. World Nuclear Association. *Liability for Nuclear Damage* (Updated March 2017). http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/liability-for-nuclear-damage.aspx.

8. For an in-depth discussion about insurance coverage involving a cyber attack that resulted in physical damage, please see Lathrop and Stanisz. Hackers Are After More Than Just Data: Will Your Company's Property Policies Respond When Cyber Attacks Cause Physical Damage and Shut Down Operations? (June 2016). https://www.pillsburylaw.com/images/content/1/0/v2/104438/EnvironmentalClaimsJournal-LathropStanisz-June222016.pdf.

9. CL380 text. https://www.if.fi/web/fi/yritysasiakkaat/extra/vakuutusehdotsuomi/documents/tavarankuljetusvakuutusehdot/voimassaolevat/cse33900.pdf.

power plant. To do so, the adversary uses existing security vulnerabilities that are the result of poor management decisions that degrade the security posture of the facility. The attack shuts down the plant, overburdens the power grid, triggers severe blackouts in critical services such as hospitals and transportation hubs, and leads to numerous injuries and several deaths. In other words, the damage is severe even though it did not result in a radiological release.

This scenario is an example of a *black swan* event, which is low probability, unexpected and highly impactful at the time it occurs (although in hindsight demonstrates that it might have been predicted). After some discussion, roundtable participants agreed that the scenario was indeed possible. In fact, attacks on critical infrastructure have already occurred. Examples include hacks on the Ukraine power grid in 2015[10] and again in 2016,[11] which cut off electricity in major districts in Kiev. Indeed, the international community is already concerned about how similar attacks could be carried out on nuclear installations. For example, Yukiya Amano, Director General of the International Atomic Energy Agency (IAEA), said that known cyber attacks may only be "the tip of the iceberg."[12] Jan Eliasson, United Nations Deputy Secretary-General, addressed the growing likelihood of a hack on a nuclear power plant that could trigger a range of damages, including a radiological release.[13]

Participants noted that while they recognise cyber threats are real and on the rise, they find it difficult to fully grasp the complexity of the threat landscape and to determine what is technically feasible and what is improbable. Several roundtable participants raised concerns about the next frontier of cyber attacks in the nuclear sector, including the upsurge in zero-day vulnerabilities and attack vectors that manipulate or corrupt data as opposed to targeting industrial control systems directly. (A zero-day attack uses a vulnerability in a computer application to infect a computer; it occurs on the same day people become aware of it, so it is impossible to patch the vulnerability before the attack takes place.)

Acts of War

Cyber adversaries include both non-state and state actors and can be extremely challenging to identify. If an attack is traced to a state-sanctioned entity, it might be considered an *act of war*. Under this scenario, nuclear liability regimes would exclude losses, damage or liability, which would consequently shift responsibility from the operator and insurer to the state. The burden of proving that the cyber attack is an act of war would fall on the insurance company. What constitutes a digital act of war has been the subject of rigorous scholarly debate for the past twenty years, but it is still unresolved.[14]

Given the difficulties associated with attribution, the lack of consensus on what constitutes a digital act of war, and political and policy considerations associated with a sovereign state that makes an accusation public, this issue is likely to remain ambiguous and untested in the context of nuclear-related insurance. However, should a cyber incident eventually be deemed an act of war, it could lead to the exclusion of insurance coverage under force majeure clauses.[15] If cyber incidents are eventually determined not to be an act of war, operators could face litigation and be called upon to demonstrate that they had applied sufficient measures to thwart, mitigate or manage the response to an attack. Clearly, further study of this issue is required because of the potential impact on operators and their liabilities. (Insurance industry representatives

10. SANS Industrial Control Systems and E-ISAC. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case.* (March 2016) https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

11. Condliffe, Jamie. *Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks*. MIT Technology Review (December 22, 2016). https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

12. Shalal, Andrea. *IAEA chief: Nuclear power plant was disrupted by cyber attack*. Reuters (October 10, 2016). http://www.reuters.com/article/us-nuclear-cyber-idUSKCN12A1OC.

13. United Nations, Deputy Secretary General. Press Release (December 15, 2016). https://www.un.org/press/en/2016/dsgsm1035.doc.htm.

14. United States Congressional Hearing. Digital Acts of War: Evolving the Cybersecurity Conversation. (July 13, 2016). https://oversight.house.gov/hearing/digital-acts-of-war-evolving-the-cybersecurity-conversation/.

15. Paganini, Pierluigi."NATO Officially Recognizes Cyberspace a Warfare Domain." *Security Affairs* (June 18, 2016). http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html.

noted that they are interested in learning more about the coverage that is needed.[16])

NEGLIGENCE AND TORT LAW

When nuclear power plants are privately owned and operated, the private sector has primary responsibility for implementing cyber security and coordinating prevention and response with the government. Failure to adequately protect against reasonably foreseeable harm will give rise to liability. The most likely form in which it could be tested is in a tort suit alleging that the entity acted negligently by failing to exercise reasonable or due care in the prevention of a foreseeable risk. It is important to understand that the purpose of tort liability is not only to compensate victims but also to provide an economic incentive for good practice. Holding industry accountable for potential economic exposure serves as a strong and positive deterrent, provides predictability, and encourages safer and more secure behaviour.

Cyber security in the nuclear sector presents unique issues since most countries with nuclear power cap operators' liability; the state assumes responsibility for any financial consequences over and above the capped amount. These liability systems are triggered only when an incident occurs that results in radiological consequences. Because a cyber attack against a nuclear power plant could result in many other types of harm, operators could be vulnerable to potentially serious financial exposure.

In 2015, Lloyd's released a report titled *Business Blackout* that analysed a hypothetical cyberattack against power generating utilities that caused a major blackout on the American East Coast.[17] The report notes that uncertainty exists regarding whether certain losses would be insured. If there is no release of radiation, nuclear power operators are no different from any other energy supplier, all of whom are vulnerable targets for future terrorist attacks.

Used as a threat weapon, a widespread electricity blackout could trigger the collapse of a city's infrastructure. For example, an electricity blackout that occurred in North America in 2003 caused nearly a dozen deaths and cost more than $6 billion.[18] At a nuclear facility, such an attack could weaken the operator's ability to defend the perimeter; this literally and figuratively opens the door for terrorist access to nuclear materials. Under tort law applicable in most countries, the operator must prove that it took all reasonable measures to protect against a foreseeable cyber attack.

Roundtable participants discussed the nuclear owner/operator's duty to protect the public from a reasonably foreseeable terrorist act, especially one that does not include a release of radiation. The discussion focused on the issue of reasonableness and how senior managers could demonstrate due care in defense of negligent security claims. Understanding that an operator cannot defend against *all* threats, participants focused on the kinds of cyber threats nuclear operators should be reasonably expected to defend against.

REASONABLENESS AND CORPORATE ACCOUNTABILITY

Given the challenges in defining reasonableness, participants considered potential ways an organisation could demonstrate that it had taken all reasonable measures to mitigate vulnerability to and the effects of a cyber attack. Some challenges in this regard include the fact that reasonableness varies with the standards and expectations of a given community, so what is reasonable in one state may not be reasonable in another.

For example, the United Kingdom (UK) requires nuclear licensees to demonstrate they have done everything reasonably practicable to reduce risks by balancing the risk posed to the plant against the measures needed to control the risk in terms of money, time or trouble. Thus *reasonably practicable* implies a

16. The cyber insurance market has been engaged with the nuclear insurance market in attempts to tailor existing cyber coverage. For instance, steps are being taken by insurers to address coverage for onsite radiological damages resulting from a cyber attack.

17. Lloyd's. Business Blackout. (July 6, 2015). https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout.

18. Minkel, J.R. . The 2003 Northeast Blackout—Five Years Later. *Scientific American* (August 13, 2008). https://www.scientificamerican.com/article/2003-blackout-five-years-later/.

computation of risk has been made.[19] The UK's Office of Nuclear Regulation defines *reasonable conduct* by reviewing and approving the operator's facility security plan. Consequently, the security plan, which meets the UK's performance-based regulations, becomes the baseline goal-setting measure for demonstrating reasonable nuclear security. Although compliance with a regulation influences liability and provides strong evidence in an operator's favour, it is not definitive. On the other hand, non-compliance with a regulation is negligence per se, which means that it is inherently considered unreasonable.

Irrespective of the regulatory framework, participants noted that more could be done to encourage the industry to implement best practices that exceed regulatory compliance criteria rather than settling for the bare minimum required under a compliance-based approach. The concept of reasonableness changes over time, especially in the face of emerging technologies. Therefore, participants also agreed that leadership should constantly question whether specific practices are still reasonable in the dynamic cyber threat environment. The key question is: Are we confident we can defend ourselves effectively from a cyber attack and manage the consequences? Answering this question requires a focus on metrics.

The Nuclear Security Governance Reporting Template

During the final Nuclear Industry Summit (NIS) in 2016, participants produced a report titled *The Role of the Nuclear Industry in the World: And How It Manages the Security of Its Materials and Technologies*.[20] This document contains an Appendix that presents a Nuclear Security Governance Reporting Template consisting of broad, but modifiable, governance questions. These questions form a framework that prompts industry organisations to address certain topics in their annual reports, such as how they approach risk management, review their security performance, and promote a strong security and cyber risk management culture. Addressing such questions holds them accountable so that commercial pressures do not take precedence over either safety or security; it also enables them to demonstrate that they take corporate oversight arrangements for nuclear security seriously.

Roundtable participants agreed that an organisation's use of a well-developed template could become a valuable narrative that demonstrates sufficient duty of care for insurers and lawyers in the aftermath of a security incident. They also agreed that developing a governance template like this would be much more beneficial than another regulation or a standard which could take years to agree to and would not have the agility to meet the rapidly changing cyber threat.

BUILDING A MODEL OF ACCOUNTABILITY

It is incumbent on industry to demonstrate its ownership and commitment to a safe, secure and profitable nuclear future. As one participant noted:

You can outsource operations,
but you can't outsource responsibility.

Building on the outcomes of this roundtable, Stimson and WINS will continue to work with industry stakeholders to develop a draft governance template, drawing from the NIS Nuclear Security Governance Reporting Template and participant feedback. Methodologies used by other industries to gauge executive accountability will form an important part of the analysis, as will work already conducted by WINS on the quality of corporate governance arrangements.[21] The goal is to encourage nuclear industry stakeholders to adopt a governance template or similar model that showcases their executive decision-making processes in prioritising and promoting nuclear security in their workforce and that exceed basic regulatory requirements.

19. According to the definition set out by the Court of Appeal (in its judgment in Edwards v. National Coal Board, [1949] 1 All ER 743), the affordability of a specific measure is based on a broader social judgement that looks at what might be generally affordable across the sector (Edwards v NCB [1949] 1 KB 704, [1949] 1 ALL ER 743). UK Health and Safety Executive. ALARP at a Glance. http://www.hse.gov.uk/risk/theory/alarpglance.htm; Burges Salmon. Briefing: Health and Safety. (December 2013). https://www.burges-salmon.com/-/media/files/publications/open-access/health_and_safety_reform_the_not_very_proportionate_elephant_in_the_room.pdf.

20. Nuclear Industry Summit. *The Role of the Nuclear Industry in the World*. Working Group 3. (March 30, 2016). http://nis2016.org/wp-content/uploads/2016/02/Working-Group-3-Report-The-Role-of-the-Nuclear-Industry-in-the-World.pdf.

21. WINS has conducted analysis in this area. See WINS, Corporate Governance Arrangements for Nuclear Security: Analysis of Annual Reports from Companies and Regulations. (March 2014). https://www.wins.org/index.php?article_id=263&id=181&bid=262&source=1.

Special Thanks

This paper is funded by the **John D. & Catherine T. MacArthur Foundation**. Additional partners include the Government of Finland, the U.S. Department of State Partnership for Nuclear Security, and the Carnegie Corporation of New York. We would like to thank the law offices of Burges Salmon for generously hosting the roundtable upon which this paper is based. The event could not have been done without the organizational support provided by Nadia Kahn of the Security Awareness Special Interest Group. We are grateful for the contributions of the following individuals for sharing their expertise and facilitating substantive discussions summarised in this report. Their support was a critical component to the event's success:

- Lucas Bergkamp, Hunton and Williams
- Sam De Silva, Nabarro LLP
- Fred Gatte, Nuclear Risk Insurers
- Jim Griffiths, Kier Group
- Roger Howsley, WINS
- Ian Maciulis, JLT Energy France
- Mark Neate, Security and Resilience, Sellafield Ltd
- Mark Pollard, Director, Marsh LLC
- George Pyk, Nordic Nuclear Insurers
- Martin Smith, Security Awareness Special Interest Group
- Ian Truman, Burges Salmon
- Maria Lovely Umayam, Stimson Center

Finally, we are grateful for the hard-working editorial support provided by Clarice Dankers at WINS, the help on our hypothetical provided by MITRE Corporation, as well as the outstanding suppport of Debra Decker and Jacqueline Kempfer of the Stimson Center.

Roundtable Sponsors

- Roger Howsley, WINS
- Kathryn Rauhut, Stimson Center
- Martin Smith, Security Awareness Special Interest Group

About the Authors

Kathryn Rauhut is a nonresident fellow practicing international security law in Vienna, Austria. Lovely Umayam is a research analyst and program manager for the Stimson Center WMD Nonproliferaion/ Nuclear Security program. For any inquiries about this study, they can be reached at krauhut@stimson.org and lumayam@stimson.org.

About Stimson

The Stimson Center is a nonpartisan policy research center working to solve the world's greatest threats to security and prosperity. Think of a modern global challenge: refugee flows, arms trafficking, terrorism. These threats cannot be resolved by a single government, individual, or business. Stimson's award-winning research serves as a roadmap to address borderless threats through collective action. Our formula is simple: we gather the brightest people to think beyond soundbites, create solutions, and make those solutions reality. We follow the credo of one of history's leading statesman, Henry L. Stimson in taking, "pragmatic steps toward ideal objectives." We are practical in our approach and independent in our analysis. Our innovative ideas change the world.