



Demonstrating Due Care: Cyber Liability Considerations for Nuclear Facilities

Executive Summary

Cyber security is the next frontier for nuclear risk managers. Within a short span of time cyber attacks have evolved in sophistication and stealth, making it difficult to develop an effective and adaptive risk management approach. While there is consensus within nuclear industry that it must bolster its capacity to “remain ahead of the dynamic cyber threat curve,” it is important to determine what this looks like in practice: what constitutes a reasonable application of cyber security measures such that it sufficiently attempts to 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, bringing together fifty industry stakeholders and cyber security experts to discuss the inherent challenges in managing cyber security risks in the nuclear sector. Participants examined a hypothetical cyber attack scenario in a nuclear power plant that undermined the security posture of the facility, cascading into a major power outage and consequently resulting in first-party property damage, reputational fallout, and significant

third-party business interruption losses. Under this scenario, participants considered potential negligence claims and corporate liability, and how a “model of accountability” – demonstrating compliance to high industry standards – might be structured in order to mitigate such liability.

This 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 difficulty in communicating risk management decisions to non-specialist Board Directors and Executives, as well as shareholders and the public. Since it is difficult to quantify the effectiveness of added security (the only evidence would be the absence of a cyber incident or a successful intervention of an incident in progress), it is hard to justify added spending and reallocating resources towards cyber security measures.

✧ Cyber security is one of many variables considered in a risk portfolio among other security-related risks, as well as safety-related risks, which are customarily handled separately. Thus, determining the proportionality that needs to be given to cyber security measures vis-à-vis other risk considerations is challenging in a resource-constrained environment.

✧ Attribution of a cyber attack could have significant implications on insurance coverage. Increasingly, there is discussion on the implications for those with cyber security insurance if the attack is positively linked to a state-sponsored group. Thus, the attack could be interpreted as an “act of war,” which changes the threat profile to a state-level concern. In this scenario, there could be significant implications for the operator if their insurance cover is voided due to force majeure clauses.

✧ Although cyber-related risks remain under-insured, many industry actors across all business sectors mistakenly believe that they would be sufficiently insured in the event of a cyber attack. This is further complicated in the nuclear sector, where third-party liability coverage under the nuclear liability regime is triggered if the incident results in a radioactive 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 domestic regulations, if they exist, and industry “norms.” While these are effective measures to a degree, they do not encourage the adaptive mind set 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 upon cyber security norms that can be used to determine reasonableness. In the absence of an agreement, it 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 would demonstrate “due care” in the wake of 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 has taken all “reasonable” measures to mitigate its cyber security risks.

✧ Participants agreed that a well-developed governance template has the potential to be a useful narrative in the aftermath of a cyber security incident as evidence supporting “sufficient” duty of care. Industry participants during the roundtable expressed support for the development of a template in cooperation with civil society and appropriate government entities.

1 Nuclear Industry Summit, Working Group 1: Managing the Cyber Threat (2016), page 3: <http://nis2016.org/wp-content/uploads/2016/02/Working-Group-1-Report-Managing-Cyber-Threats.pdf>

**For more information on this project, contact:
Maria Lovely Umayam at lumayam@stimson.org
and Kathryn Rauhut at krauhut@stimson.org**



WORLD INSTITUTE FOR
NUCLEAR SECURITY

STIMSON

Special thanks to
The Security Awareness Special Interest Group