PRIORITIZING ACTIONS FOR MANAGING CYBERSECURITY RISKS

D. DECKER
Henry L. Stimson Center
Washington, D.C., United State
Email: ddecker@stimson.org

K. RAUHUT
Henry L. Stimson Center
Washington, D.C., United States

M. FABRO
Lofty Perch
Toronto, Canada

Abstract

Cyberattacks are the norm in every industry, and the nuclear industry is no different. However, the associated consequences of an attack are different in the nuclear sector, where fears of radiation releases and material diversion greatly influence how risk is analyzed and managed. In an era where erroneous and inaccurate news often spreads on social networks faster than accurate official reports, risk management and incident planning need to be prioritized and given a fresh look. That was just one finding from a workshop on nuclear cyber risks held in Vienna, Austria, in late 2018. The Fissile Materials Working Group (FMWG) - a coalition of 80 organizations from around the world working to keep the world safe from nuclear terrorism - in collaboration with the Stimson Center brought together cybersecurity experts and stakeholders to consider cyber risks in the civil nuclear industry and how to address them. The workshop report, Nuclear Cybersecurity: Risks and Remedies, detailed 10 findings. Since the time of that report, FMWG and Stimson have been working with expert stakeholders to further assess those risks, to consider new emerging risks, and to prioritize actions needed to better manage them. New approaches are needed to confront the quickly evolving landscape of risks. The paper will detail some work that needs to be done in the private sector and civil society as well as by States and international organizations to help pool expertise and better manage risks. The paper will also consider new technologies and their effects on risk. How can the nuclear industry, States, international organizations, nongovernmental organizations and other stakeholders work together to address and mitigate cyber risks?

1. INTRODUCTION

Cyber risks are omnipresent. Threat actors, using undetectable methods and techniques, have infiltrated the supply chain and inserted previously unseen vulnerabilities that can be exploited at will. Cybersecurity risks can be managed but never completely eliminated. The most dangerous consequences of a system-wide cyberattack on a nuclear power plant range from disruption of the power supply to radiation releases, harming both people and the environment over the short or long term. Given the special nature of the nuclear industry, more attention needs to be paid to establishing effective approaches to managing risks in cyberspace.

This paper will first review the history and evolution of nuclear cyber risks in terms of threats, vulnerabilities and consequences. It will also discuss some of the emerging risks from software and hardware as well as risks from next-generation communication infrastructures, artificial intelligence (AI) and "deepfakes." It will then look at approaches to managing these risks at an organizational level and at an international level based on recommendations from international stakeholders engaged over the last 1.5 years in roundtables and discussions.[1]

[1] For one of the initial discussions, see DECKER, D., RAUHUT, K., KUTCHESFAHANI, S., CONNOLLY, E., Nuclear Cybersecurity: Risks and Remedies (2019), https://www.stimson.org/content/nuclear-cybersecurity-risks-and-remedies

1. CYBER RISK TRENDS: THREATS, VULNERABILITIES, CONSEQUENCES

Some of the earliest cyberattacks involved criminal theft of data. Attacks resulting in a breach in confidentiality are important and still widespread, as are those that impact data integrity and availability. The concern involves not just loss of intellectual property that could give advantage to competitors but also theft, destruction or modification of sensitive information that could compromise nuclear safety and/or security. Plant blueprints and employee data stolen in a 2014 cyberattack on Korea Hydro and Nuclear Power Company caused fears and prompted impromptu emergency drills [1]. Most recently, malicious actors injected malware into administrative systems of a new Indian nuclear power plant where, in addition to other issues, a large amount of data was stolen [2] [3]. The contradictory public statements regarding the India incident recalls the initial confusion surrounding the 2011 cyberattack on the former French nuclear power group Areva [4].

Assurances that "air-gaps" can protect critical nuclear assets and systems from cyberattacks proved specious when the 2010 Stuxnet virus was able to destroy nuclear centrifuges. In 2018, the United States and the United Kingdom warned of very targeted infiltration of nuclear and other energy power operators and critical infrastructures using trusted networks, such as vendors; the potential for infiltration of vital operating platforms, applications and safety systems is real [5].

More pernicious attacks are likely as well-developed hacking tools are leaked, copied and customized for a particular target. Information technology service providers have become a target for advanced persistent threats, thereby threatening the security of their clients. Cloud and managed service providers have access to the inner workings of clients; a compromised provider represents a compromised client [6].

In addition to facing new and increasing cyber capabilities possessed by the threat actor, the nuclear industry is facing increasing vulnerabilities. It is these vulnerabilities that ultimately provide the opportunities to the attacker. Next generation nuclear technologies, including small modular reactors, are highly digitized. Also, existing nuclear operators are often replacing legacy systems with digital ones. Increased digitization can also mean more users, more service providers and more trust in and amongst critical networks and the assets that are contained in them. That increases the surface area for an attack and the possible vectors of attack, including in some cases more personnel in the organization, business affiliates, suppliers, advisors and even its regulators. Credential protection, access authorizations, and good training are critical, as people often represent the highest vulnerability in an organization – through accidental, negligent or malicious behaviors.

Supply chain vulnerabilities are of increasing concern both for hardware and software, with vulnerabilities being discovered in everything from computer chips to safety systems. The International Atomic Energy Agency (IAEA) has produced guidance to help manage risks from counterfeit and fraudulent items in the nuclear industry but notes the continuing challenges, from original providers ending system updates to actors deliberately diverting and substituting fraudulent integrated circuits for espionage purposes [7].

New technologies need to be assessed for the vulnerabilities they may present to computer and related systems.

- The move to 5G systems means increased speed and resilience in communications but also means increased complexities and vulnerabilities [8]. The implications of this for the nuclear as well as other sectors is unclear, with the confidentiality, security and integrity of 5G/updated communication systems needing to be reassessed as well as the operating systems and functions, such as emergency response, that rely on those communication systems;
- AI may be used well in the nuclear and other sectors to decrease vulnerabilities, for example, with AI supporting biometric data to authenticate users and limit access and analyzing behaviors to detect anomalies. Threat actors, though, also can use AI to hone their approaches. Facilities may well be vulnerable to a blended attack using AI to disrupt plant operations while unmanned aerial vehicles disrupt communications further or assist attackers in surveillance for targeting physical protection systems;

- Distributed ledger technology (“blockchain”) may offer some opportunities for security, such as in possibly helping to ensure integrity and authenticity of control system applications used in nuclear operations. Over the longer-term, however, quantum computing may be able to thwart those advantages;
- Terrorists with lesser capability than State actors may also find fresh ways to exploit the nuclear enterprise with new electronic devices. Employees wearing digital devices can pose exploitable vulnerabilities for information security and potentially nuclear facility operations;
- Other new technologies such as robotics and remotely operated physical protection systems can assist in making security more cost efficient and could be an effective attack deterrent; however, these also present additional attack surfaces for cyber intrusion and can make nuclear operations more vulnerable.

These and other innovations, such as the use of augmented reality to assist in training, need to be assessed for their benefits, such as decreasing human error, as well as their potential to increase risks.

Consequence management is dependent on communications and availability of response mechanisms. Social media spreads information today faster than news from official channels can be released; false calls for evacuations can lead to highway deaths and social mayhem. Another fear stakeholders raise is that a malevolent actor will use AI to present false risk communications to the public and to targeted emergency responders in order to interfere with appropriate, planned actions. The advent of “deepfakes” with false audio and visual representation of trusted actors can compromise response functions and cause serious alarm among the public. This would greatly increase the consequences of any event.

The problems with the lack of agreed international norms and standards in cyberspace will be compounded by the uncharted terrain of new technologies, which is devoid of national or international standards. The potential for misuse of next-generation technologies and machine intelligence, which are so unknown, may well be unpreventable and beyond the design basis threat (DBT) of any nuclear facility. Any DBT that has a cyber-component will define the threat and associated characteristics/attributes against which a facility must reasonably defend itself. The facility should be tested and assessed as to its ability to manage that threat. However, at the end of the day, no one can predict what that cyber threat and associated vulnerabilities look like. If the consequence of this futuristic attack results in some kinetic impact related to sabotage, release or theft/diversion of materials, the facility is going to have to be responsible for protecting the systems that are related to that impact and for helping to mitigate consequences.

In today’s world, it is not a matter of if but when there will be another major nuclear incident. The incident may not even start as a malicious act but could be due to negligence or oversight or accident. Yet, the question ultimately is how to prioritize actions to manage risks by appropriately addressing threats, vulnerabilities and consequences.

2. PRIORITIZING RISK MANAGEMENT ACTIONS – FOR LICENSEES

Understanding the threat vectors can help with prioritization of risk management. Some understanding of who is attacking may be needed in order to understand the more important “why” and the tactics, techniques and procedures of the adversary. The “why” can be much more useful because it maps directly to threat actor intent and associated consequences sought by the adversary. These characteristics do not have anything to do with probability and can actually be used to inform the defender with regards to how to focus efforts. An advanced persistent threat, however, is hard to understand let alone manage [9] [10]. States do not necessarily expect their licensees to prevent such threat actors targeting their facilities but do expect licensees to take steps to ensure good basic cyber hygiene to avoid being easy targets – and to avoid simple human errors.

Licensees should comply with their State’s regulations at a minimum – but States’ regulatory guidance is insufficient. Given the evolving nature of the threat and the continuing identification of new vulnerabilities, any cyber DBT that defines the threat a licensee must prevent would be outdated as soon as it is established. Prescriptive regulatory guidance becomes meaningless. A performance-based approach to regulation is better as it creates the opportunity for cyber to inform how consequence analysis is managed. This ultimately results in a graded approach that empowers the licensee to protect their assets according to functionality, criticality or other operational metrics.

Such an approach would encourage a licensee to be more proactive in continuously developing appropriate methods for identifying and responding to the actions of a threat actor, thereby avoiding potential consequences. However, from a licensee's perspective, this is also insufficient.

Regulators provide baseline requirements, but industry peers may have exceeded those requirements thus establishing new industry norms that a licensee should adopt. The Amended Convention on the Physical Protection of Nuclear Material (A/CPPNM), which came into force in 2016, notes the importance of security culture and defense in depth and recognizes that licensees have the "prime responsibility" for protecting their materials and facilities [11]. That means licensees have an obligation, beyond regulatory minimums, to understand threats as well as their vulnerabilities and consequences. Licensees, therefore, must learn from others, both in the nuclear industry and more broadly.

This is where good governance is important. Owners and managers must demonstrate that they value good security as a core value and can share good practices and require the same of their suppliers, contractors and others with whom they engage. In doing this, an organization not only reduces risks, it also reassures the regulators, investors, insurers and the public and garners reputational gains as well as reduced liability in the event of an incident [12]. The Stimson Center, World Institute for Nuclear Security (WINS) and Internet Security Alliance (ISA) are all working on good governance models with ISA focusing particularly on good governance for cybersecurity through its Cyber Risk Management Handbooks, which are being adopted around the world [13] [14].

Voluntary consensus standards/frameworks can help managers reinforce good security governance and provide a peer-developed approach to risk assessments [15]. The IAEA provides guidance for computer security self-assessments [16]. Industry and government organizations also provide guidance, e.g., on identifying and securing critical digital-dependent functions; and, good guidance comes from both inside and outside the nuclear industry [17] [18]. The United States' National Institute of Standards and Technology (NIST) worked with a broad group of industry stakeholders to develop the Cybersecurity Framework; NIST says Israel, Japan and other countries have successfully leveraged the Framework [19].

Licensees must decide among the plethora of frameworks, as there is yet little global consensus, and adopt a risk management approach that is right for them. They much allocate time for the then necessary risk assessments and invest in filling any gaps, including for appropriate cybersecurity training at all levels of operations as humans are the biggest contributors to cyber insecurity in organizations. The IAEA and WINS as well as others offer training and actual simulations [20].

Stakeholders note that good security culture with basic training and reinforcement of good cyber hygiene is necessary but not sufficient. More information sharing is needed across licensees (see next section) to ensure lessons get shared. Such detailed sharing would go beyond development of consensus standards or cyber frameworks; it would involve sharing of actual experiences. Response planning is key and needs additional work. Stakeholders note the importance of developing more scenarios and practices, including with emergency responders. Some of this work could be done by individual licensees but would be accomplished more cost effectively if done on a regional or industry-sector basis. International organizations and associations could well help with these tasks.

3. PRIORITIZING RISK MANAGEMENT ACTIONS – FOR INTERNATIONAL ORGANIZATIONS AND OTHER ACTORS

Stakeholders note the need for broader international cooperation on cybersecurity, including fresh thinking on approaches. The United Nations has taken a leading role in supporting cyber cooperation, with the UN Secretary-General's High-level Panel on Digital Cooperation recommending coordination among the many different efforts. The Internet Governance Forum (IGF), a UN-supported platform for multi-stakeholder policy discussions, called for targeted collaboration that goes beyond national borders to evolve accepted best practices [21]. Nongovernmental organizations, industry associations, insurers, educational institutions and others also can play important roles to reduce cyber risks.

Stakeholders in the nuclear field suggest the following be done within their sector:

— Further development of emergency action best practices.

- Risk communication: What are the appropriate communications and communication channels to effectively reduce risk? This is likely to differ among countries. For a specific country, in the case of an actual event, what are the appropriate communications that reduce risk? This would entail joint development of prepared public emergency communications and pre-planned incident reporting for various scenarios. How does one ensure social media and "deepfakes" do not overtake reality?
- Emergency response: What could go wrong and how likely is it? This would entail analysis of actual incidents and additional scenario development based on evolving risks;[2]
- Table Tops and Other Exercises: Leveraging IAEA incident response work and above efforts, develop practice opportunities through both new and existing forums, such as GICNT exercises.

— More timely documentation of available best practices.

- Information exchanges: Explore having IAEA facilitate best practice information exchange more directly among licensees and with other organizations. This could be as a new initiative similar to the International Nuclear Security Education Network and as a complement to the State-sponsored work in the IAEA Global Nuclear Safety and Security Network (GNSSN). The IAEA will be exploring in 2020 development of an overarching framework to collect best practices from Nuclear Security Support Centers and should include the private sector in this, including cyber specialists. The IAEA could act as a convener, add special cyber elements to their information sharing – and collaborate with groups such as the World Nuclear Association and World Association of Nuclear Operators;
- Quick, timely updates: Institute a brief on evolving good practices. The IAEA takes a long time to publish its documents as most are consensus based. However, the IAEA or another entity could provide periodic short updates on evolving good practices, such as the EU Network and Information Security directive and evolving certification schemes, US supply chain requirements, as well as the earlier noted NIST Cyber Framework or ISA Cyber-Risk Oversight Handbook. State/industry regulatory guidance documents are not necessarily considered best practices or industry norms by other states – but voluntary sharing of good practices and lessons learned from others' experience can be facilitated;
- Responsible suppliers/contractor/vendors: Individual countries have approved vendor lists and some have outlawed the use of some suppliers. Can clear criteria be developed and shared for doing this? Is there some way the results of such analyses could be made public? How effective are new initiatives, such as the Global Cybersecurity Alliance? Can criteria be developed to guide contract terms that expand on the IAEA Contracting Toolkit?

— Information sharing regarding cyber incidents, including breaches involving those without consequences.

- Incident disclosures: What are the required information disclosures, for example trigger events, when to disclose, to whom, what type of communication to use, etc.? Research would look at incidents currently classified as "safety" events that also have a security aspect – and would look at the outcome of reporting. Consider also developing agreement around shared reporting of incidents using a cybersecurity incident scale to gauge how severe an event is to clarify context and significance, such as one developed by the IAEA. This could be a parallel to the IAEA Incident and Trafficking Database and could be done in a nongovernmental organization;[3]
- Lessons Learned: Compiling an anonymized database with lessons learned regarding nuclear and

[2] See, for example, the IAEA Safety standards on emergency preparedness and response: IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Standards on Emergency Preparedness and Response (2019), https://www.iaea.org/topics/emergency-preparedness-and-response/safety-standards-technical-guidance

[3] For example, the James Martin Center for Nonproliferation Studies puts together a more detailed trafficking database than IAEA's, which requires confirmation from States. See: CNS- JAMES MARTIN CENTER FOR NONPROLIFERATION STUDIES, The CNS Global Incidents and Trafficking Database (2019), https://www.nti.org/analysis/articles/cns-global-incidents-and-trafficking-database/

cybersecurity to create an "operator's database" resource, including of industrial control system incidents. This could be based on open source reporting and voluntary sharing and may include safety incidents.[4] Some countries have started to figure out ways to expand information sharing among government, private sector, insurers and cyber specialists within their own jurisdiction; documenting such efforts, the process for effecting them (including legislation to allow and protect shared information) and sharing success stories would be useful to replicating such models.

Stakeholders in the nuclear sector recognize that their issues and concerns regarding cyber security are not totally unique. Except for the potential for radiation release and accompanying fears of such, other enterprises and individuals have similar cybersecurity concerns. Stakeholders support broader initiatives. As a result of recent UN General Assembly Resolutions, discussions are continuing on cyber norms, the rule of law, and related issues [22]. Advances may well be forthcoming to support better hardware and software security. But the importance of cyber risks in the nuclear sector spurred calls for more initiatives.

Additional ideas to reduce risks that should be explored include:

— Consideration of new forums/ways in which to develop agreements and support implementation.
  - Discussions in Organization for Security and Cooperation in Europe supporting more confidence-building measures;
  - Discussions on cyber issues in the trilateral South Korea/Japan/China Safety and Security Forum;
  - A protocol including cyber in the Convention on Nuclear Safety or the Amended Convention on the Physical Protection of Nuclear Material;
  - Establishing a connection between the obligations under CPPNM/A, national regulations and the transformation of those obligations into a set of norms among industry. Uncover those norms already existing and look to norm establishment as a goal moving forward in the context of these and other treaty/UN Security Council resolution obligations;
  - More formalized agreements not to target critical infrastructures, including nuclear facilities.

— Evaluation of what works to reduce incidents.
  - Review of agreements that may have worked, such as the Obama-Xi 2014 agreement to reduce economic espionage or India-Pakistan's agreement not to attack nuclear facilities, which would include an assessment of how well they have or could work and be replicated;
  - The role of incentives and/or negative reporting in supporting adoption of voluntary good practices.[5]

— Consideration of enforcement mechanisms to reduce cyberattacks.
  - Review of State and international approaches to cybercrimes: Although the UN's Cyber Policy Portal has information on some professed policies, how are these being enforced? A think tank or academic institution could assess selected States' approaches to investigation, prosecution, and penalties for cybercrimes, e.g., cyberattacks, cyber terrorism, etc.;
  - Review of cooperation challenges in enforcement: If cybercrimes are to be reduced, good enforcement is needed – and collaborative approaches. Europol and Interpol have started good engagement with other stakeholders and need to further pursue such efforts;
  - Review of attribution challenges in cyberattacks: Attribution is important for deterrence. The challenge will come in identifying State attacks or State-supported attacks. Lessons might be learned from

[4] See: SLOWIK, J., "Evolution of ICS attacks and the prospects for future disruptive events." For past examples, see RISI Online Incident Database: RISI- REPOSITORY OF INDUSTRIAL SECURITY INCIDENTS, RISI Online Incident Database (2015), https://www.risidata.com/Database

[5] See, for example: JEWELER, M. G., LENTCHNER, C., ROSS, R. B., HOGAN, B., MROZ, R., Name-and-Shame Proposal of Electric Regulators Highlights Need for Cyber Insurance (2019), https://www.pillsburylaw.com/en/news-and-insights/name-and-shame-proposal-of-electric-regulators-highlights-need-for-cyber-insurance.html

studying other areas where collaboration on forensics and attribution methods have been tried, e.g., nuclear, chemical weapons. The collaborations can be through a new international organization or through a network of cooperating States, private sector cyber specialists/organizations, universities, and/or individuals. Much might be learned from the development of GICNT and the work of the Nuclear Forensics International Technical Working Group, which consists of experts working internationally to advance the discipline of forensics and to develop common approaches – including in law enforcement.

Many efforts are desirable for reducing cyber risks in the nuclear sector, but prioritization is key. Licensees may be guided by regulators but have a responsibility to make risk management judgments beyond regulatory minimums. International institutions including non-governmental organizations should look to the above list and decide where they have the capacity and capability to be effective in their efforts to reduce risk. An organized meeting to consider these recommendations among stakeholder groups would help inform that work.

REFERENCES

[1] TRENDMICRO, Korean Nuclear Plant Faces Data Leak and Destruction (2014), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/korean-nuclear-plant-faces-data-leak-and-destruction

[2] MONKEY CAGE, An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What You Need to Know (2019), https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

[3] THE ECONOMIST, A Cyber Attack on an Indian Nuclear Plant Raises Worrying Questions (2019), https://www.economist.com/asia/2019/11/01/a-cyber-attack-on-an-indian-nuclear-plant-raises-worrying-questions

[4] BROOK, C., Report: French Nuclear Company Areva Hit by Virus (2011), https://threatpost.com/report-french-nuclear-company-areva-hit-virus-103111/75825/2/

[5] DECKER, D., RAUHUT, K., Cyber Risks Go Nuclear (2018), https://www.stimson.org/content/cyber-risks-go-nuclear

[6] CISA- CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, APTs Targeting IT Service Provider Customers, https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers

[7] Managing Counterfeit and Fraudulent Items in the Nuclear Industry, Nuclear Energy Series nº NP-T-3.26, IAEA, Vienna (2019).

[8] EUROPEAN COMMISSION, EU-wide Coordinated Risk Assessment of 5G Networks Security (2019), https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[9] CAPEC- COMMON ATTACK PATTERN ENUMERATION AND CLASSIFICATION, ATT&CK Comparison (2019), https://capec.mitre.org/about/attack_comparison.html

[10] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, "A common cyber threat framework" (2017).

[11] Unofficial Consolidated Text of the Convention on the Physical Protection of Nuclear Material, As Amended on 8 July 2005, IAEA, Vienna (2005).

[12] DECKER, D., KEMPFER, J., RAUHUT, K., UMAYAM, L., Nuclear Security Governance Template (2017), https://www.stimson.org/nucleargovernance

[13] WINS- WORLD INSTITUTE FOR NUCLEAR SECURITY, 1.7 Corporate Governance and Legal Liability for Nuclear Security (2019), https://wins.org/document/1-7-corporate-governance-and-legal-liability-for-nuclear-security/

[14] ISA- INTERNET SECURITY ALIANCE, International Cyber-Risk Management Handbooks, https://isalliance.org/isa-publications/international-cyber-risk-management-handbooks/

[15] DECKER, D., RAUHUT, K., Nuclear Energy: Securing the Future – A Case for Voluntary Consensus Standards (2016), https://www.stimson.org/content/nuclear-energy-securing-future-case-voluntary-consensus-standards

[16] Conducting Computer Security Assessments at Nuclear Facilities, IAEA, Vienna (2016).

[17] Nuclear Sector Cybersecurity Framework Implementation Guidance: For U.S. Nuclear Power Reactors, DHS, Washington (2015).

[18] EPRI- ELECTRIC POWER RESEARCH INSTITUTE, EPRI Cyber Security Metrics Operationalization and Benchmarking Pilot (2019), https://www.epri.com/#/pages/product/000000003002016796/?lang=en-US&lang=en-US

[19] NIST- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Success Stories (2019), https://www.nist.gov/cyberframework/success-stories

[20] LYNGAAS, S., Hacking Nuclear Systems is the Ultimate Cyber Threat. Are We Prepared? (2018), https://www.theverge.com/2018/1/23/16920062/hacking-nuclear-systems-cyberattack

[21] IGF- INTERNET GOVERNANCE FORUM, "IGF 2018 WS#75 Approaches to a Wicked Problem: Stakeholders Promote Enhanced Coordination and Collaborative, Risk-Based Frameworks of Regional and National Cybersecurity Initiatives," 2018.

[22] VAVRA, S., World Powers are Pushing to Build Their Own Brand of Cyber Norms (2019), https://www.cyberscoop.com/un-cyber-norms-general-assembly-2019/