Published on *The National Law Review* https://natlawreview.com

Cybersecurity in the Nuclear Industry: US and UK Regulation and the Sellafield Case

Article By:

Andrew Parsons

Andrew Tuggle

Lisa Rushton

Key Points:

- Real-world examples from both the U.S. and U.K. demonstrate that nuclear facilities are being targeted by sophisticated cyber attackers, including state actors. This isn't just a theoretical risk—it's happening now, and facilities must take it seriously.
- The successful prosecution of Sellafield with significant fines (£332,500) shows that regulators are now willing to take strong enforcement action, even when no actual breach has occurred. Nuclear facilities cannot afford wait for an incident before improving their cybersecurity—they must be proactive.
- With both the U.S. and U.K. strengthening their regulatory frameworks and increasing enforcement powers, nuclear facilities should take steps now to review and upgrade cybersecurity measures. This includes not just updating technical controls, but also ensuring compliance with security plans, auditing systems, and maintaining proper documentation.

National security regulators are particularly concerned about the vulnerabilities of nuclear facilities to cyberattacks. In March 2022, the U.S. Justice Department unsealed criminal indictments against four agents of the Russian government, charging them with offenses related to cyber “spearfishing attacks” which compromised the business network of the Wolf Creek Nuclear Operating Corporation (WCNOC) in Burlington, Kansas. Also of note is the October 2024 prosecution and conviction of Sellafield Ltd in the U.K. for three offenses involving inadequate cybersecurity controls. In that case, the company (rather than the hacker) was charged by the Office for Nuclear Regulation (ONR) for failing to protect sensitive nuclear information and for failure to follow its own cybersecurity plan between 2019 and 2023.

Fortunately, the nuclear facilities in both cases were not materially compromised in these attacks.

The targeting of nuclear facility operators demonstrated that malicious actors intended to exploit cyber vulnerabilities within the nuclear industry.

U.S. Regulatory Framework

The Nuclear Regulatory Commission ("**NRC**") has been active in establishing rules and guidelines to enhance the cybersecurity of U.S. nuclear facilities:

1. **10 CFR Part 73.54**: One of the NRC's key regulatory frameworks that includes cybersecurity requirements, the regulation mandates that nuclear facilities establish and maintain a cybersecurity program to protect digital assets critical to safety, security, and emergency preparedness.
2. **Regulatory Guide 5.71**: In February 2023, the NRC revised its regulatory guide to provide detailed guidance on implementing cybersecurity measures. It outlines a defensive strategy that includes the identification of critical digital assets, continuous assessment of threats, and implementation of protective measures.
3. **Nuclear Energy Institute (NEI) 08-09 (2018 Addendum)**: This document, developed by the nuclear industry with NRC's endorsement, offers a comprehensive framework for cybersecurity programs. It emphasizes a risk-informed approach, allowing facilities to tailor their cybersecurity measures based on specific threats and vulnerabilities.

In 2013, the NRC's Office of Nuclear Security and Incident Response established a Cyber Security Branch (CSB) to strengthen internal governance of the agency's regulatory activities. Today, the NRC actively monitors threats associated with cybersecurity against NRC-licensed facilities. The CSB maintains a dedicated cyber assessment team responsible for analysing and evaluating real-world cyber incidents.

Today, the Nuclear Regulatory Commission (NRC) actively monitors threats associated with cybersecurity against NRC-licensed facilities. The Cyber Security Branch maintains a dedicated cyber assessment team responsible for analysing and evaluating real-world cyber incidents.

The team evaluates whether an identified threat could impact licensed facilities and makes recommendations for NRC actions and communications to the licensees. The NRC also coordinates with other intelligence and law enforcement communities including the National Counterterrorism Center, the Department of Homeland Security's U.S. Computer Emergency Response Team, and the Federal Bureau of Investigation in working to prevent cyberattacks.

U.K. Regulatory Framework

The U.K. Nuclear industry is subject to a range of different cybersecurity regulations that all have at their heart the concept that effective cybersecurity is a mandatory requirement. These rules have existed in various forms over the years, but there is now increasing activity by regulators to strictly enforce them.

The U.K. Nuclear industry is subject to a range of different cybersecurity regulations that all have at their heart the concept that effective cybersecurity is a mandatory requirement.

The overarching framework is set out in the Civil Nuclear Cyber Security Strategy 2022. This strategy aims to strengthen the cybersecurity posture of the U.K. civil nuclear sector over five years. It focuses on four key objectives:

1. **Risk Management:** Prioritizing cybersecurity as part of a holistic risk management approach.
2. **Risk Mitigation:** Proactively addressing cyber risks, including those from legacy systems and new technologies.
3. **Incident Management:** Enhancing resilience by preparing for and responding to cyber incidents collaboratively.
4. **Culture and Skills:** Promoting a positive security culture and developing cyber skills within the sector.

Underpinning this strategy are an overlapping (and growing) regime of cybersecurity laws:

- The Nuclear Industries Security Regulations 2003 ("**the NISR**") governs a wide range of security issues, including obligations to ensure that "sensitive nuclear information" is kept secure.
- The Network and Information Security Regulations ("**NIS 1**") designates nuclear sites as critical infrastructure and imposes an obligation to implement "*appropriate technical and operational measures*" to protect IT systems and to ensure continuity of service.

Whilst these regimes have been in place for some time, regulators recently stepped up enforcement to ensure compliance with these laws as was evidenced by the recent prosecution of Sellafield.

The Sellafield Case

Sellafield Ltd, the company licensed to operate the Sellafield nuclear decommissioning and waste site, received a fine in October 2024 of £332,500 after pleading guilty to three offences relating to inadequate cybersecurity controls and procedures that it had in place across a four-year period.

The prosecution was brought by the U.K.'s independent nuclear regulator (the Office for Nuclear Regulation ("**ONR**")) following its investigation where it had identified that Sellafield Ltd had failed to meet the requisite standards, procedures and arrangements set out in its own approved plan for cybersecurity as required under the NISR.

The ONR's case was not brought on the basis that there had been an actual exploitation of the security failings (seemingly because there was a lack of evidence that attacks had been successful, rather than conclusive proof that the attacks were stopped). The basis of the prosecution was Sellafield's unsatisfactory performance in relation to the management of its IT systems, and that had the vulnerabilities been exploited by attackers, it could have led to the unauthorised access to critical systems and loss of key data resulting in disrupted operations, damaged facilities and the delay of

important decommissioning activities. In particular, Sellafield failed to comply with its own cybersecurity plan and failed to undertake annual checks on the security of its operational and information technology systems.

Following its guilty plea to three offences under the NISR, Sellafield Ltd was ordered to pay a fine of £332,500, along with prosecution costs of £53,253.20. Despite the successful prosecution, the ONR has reported that the cybersecurity failings have yet to be fixed and are subject to ongoing required improvements.

Going forward, the U.K. legal regime is only going to get stronger. The Government has announced that it plans to introduce a new Cyber Security and Resilience Bill which intends to strengthen the U.K.'s operational resilience to cyber threats by, amongst other things:

- Updating the existing (NIS1) regime to ensure that more essential services are protected, including by increasing the scope of digital services and supply chains within the regime;
- Increasing regulators' powers through introducing new cost recovery mechanisms and the ability to proactively investigate potential vulnerabilities (similar to the U.S.'s 2022 update to inspection procedure 71130); and
- Expanding reporting requirements.

It is worth noting that the European Union's transition from NIS 1 to NIS 2 demonstrates a strengthened approach to cybersecurity, featuring expanded scope, more detailed requirements, and enhanced enforcement measures. This update emphasizes the EU's dedication to protecting critical infrastructure and extends security obligations to equipment suppliers and service providers. The U.K. Government is likely to use NIS 2 as a model when developing its own Cyber Security and Resilience Bill.

Going forward, the U.K. legal regime is only going to get stronger. The Government has announced that it plans to introduce a new Cyber Security and Resilience Bill which intends to strengthen the U.K.'s operational resilience to cyber threats.

Looking Ahead

U.S. and U.K. regulators are focused on ensuring that organisations providing essential services, and their related key digital suppliers, implement sufficient technical controls to enhance the level of cybersecurity and help protect critical infrastructure. Those in the nuclear industry will be at the sharp edge of these changes and should take the opportunity to review their operational and technical cybersecurity measures now to ensure they are fit for purpose.

National Law Review, Volume XV, Number 65