Chatham House Report | Executive Summary

Caroline Baylon with Roger Brunt and David Livingstone

September 2015

Cyber Security at Civil Nuclear Facilities

Understanding the Risks

CHATHAM
HOUSE
The Royal Institute of
International Affairs

Executive Summary and Recommendations

Recent high-profile cyber attacks, including the deployment of the sophisticated 2010 Stuxnet worm, have raised new concerns about the cyber security vulnerabilities of nuclear facilities. As cyber criminals, states and terrorist groups increase their online activities, the fear of a serious cyber attack is ever present. This is of particular concern because of the risk – even if remote – of a release of ionizing radiation as a result of such an attack. Moreover, even a small-scale cyber security incident at a nuclear facility would be likely to have a disproportionate effect on public opinion and the future of the civil nuclear industry.

Notwithstanding important recent steps taken by the International Atomic Energy Agency (IAEA) to improve cyber security across the sector, the nuclear energy industry currently has less experience in this field than other sectors. This is partly due to the nuclear industry's regulatory requirements, which have meant that digital systems have been adopted later than in other types of critical infrastructure. In addition, the industry's long-standing focus on physical protection and safety has meant that while these aspects of risk response are now relatively robust, less attention has been paid to developing cyber security readiness. As a result, exploiting weaknesses in digital technology could be the most attractive route for those seeking to attack nuclear facilities without fear of interdiction.

The cyber security risk is growing as nuclear facilities become increasingly reliant on digital systems and make increasing use of commercial 'off-the-shelf' software, which offers considerable cost savings but increases vulnerability to hacking attacks. The trend to digitization, when combined with a lack of executive-level awareness of the risks involved, also means that nuclear plant personnel may not realize the full extent of this cyber vulnerability and are thus inadequately prepared to deal with potential attacks. There is a pervading myth that nuclear facilities are 'air gapped' – or completely isolated from the public internet – and that this protects them from cyber attack. Yet not only can air gaps be breached with nothing more than a flash drive (as in the case of Stuxnet), but the commercial benefits of internet connectivity mean that nuclear facilities may now have virtual private networks and other connections installed, sometimes undocumented or forgotten by contractors and other legitimate third-party operators.

Meanwhile, hacking is becoming ever easier to conduct, and more widespread: automatic cyber attack packages targeted at known and discovered vulnerabilities are now widely available; advanced techniques used by Stuxnet are now known and being copied; and search engines can readily identify critical infrastructure components that are connected to the internet.

In the light of these concerns, Chatham House undertook an 18-month project in 2014–15 on the nexus between cyber security and nuclear security. By drawing on in-depth interviews with 30 industry practitioners, as well as policy-makers and academics, and convening three expert roundtables, the project sought to assess the major cyber security challenges facing the wider nuclear industry; to identify international policy measures that could help to enhance cyber security in the sector; and to help increase knowledge of current concerns in this area. This report examines the major cyber threats to civil nuclear facilities, focusing in particular on those that could have an impact on industrial control systems, and suggests some potential solutions to these challenges.

Main findings

The research identified the following major challenges for civil nuclear facilities.

Industry-wide challenges

- The **infrequency of cyber security incident disclosure** at nuclear facilities makes it difficult to assess the true extent of the problem and may lead nuclear industry personnel to believe that there are few incidents. Moreover, **limited collaboration with other industries or information-sharing** means that the nuclear industry tends not to learn from other industries that are more advanced in this field.
- A **paucity of regulatory standards,** as well as limited communication between cyber security companies and vendors, are also of concern.
- This suggests that **the industry's risk assessment may be inadequate;** as a consequence, there is often **insufficient spending on cyber security.**
- **Developing countries may be particularly at risk,** because they have even fewer resources available to invest in cyber security.

Cultural challenges

- **Nuclear plant personnel, who are operational technology engineers, and cyber security personnel, who are information technology engineers, frequently have difficulty communicating,** which can lead to friction. In many cases the problem is exacerbated by the off-site location of cyber security personnel.
- **Nuclear plant personnel often lack an understanding of key cyber security procedures,**

finding that the procedures documents produced by cyber security personnel do not communicate this information in language that is clear to them.

- **Cyber security training at nuclear facilities is often insufficient.** In particular, there is a **lack of integrated cyber security drills** between nuclear plant personnel and cyber security personnel.
- **Reactive rather than proactive approaches to cyber security** contribute to the possibility that a nuclear facility might not know of a cyber attack until it is already substantially under way.
- This suggests that **nuclear plants may lack preparedness for a large-scale cyber security emergency,** particularly if one were to occur **outside normal working hours.**

Technical challenges

- **Many industrial control systems are 'insecure by design',** since cyber security measures were not designed in from the beginning.
- **Standard IT solutions such as patching are difficult to implement** at nuclear facilities, mainly owing to concern that patches could break a system and because of the commercial need to reduce plant downtime.
- **Supply chain vulnerabilities** mean that equipment used at a nuclear facility risks compromise at any stage.

Recommendations

The cyber security threat requires an organizational response by the civil nuclear sector, which includes, by necessity, knowledgeable leadership at the highest levels, and dynamic contributions by management, staff and the wider community of stakeholders, including members of the security and safety communities. The nuclear sector as a whole, taking account of recommendations and guidance issued by the IAEA, should take a strategic approach that will:

- **Develop a more robust ambition** to match or overtake its opponents in cyberspace and thereby take the initiative, focusing its resources on critical elements of the nuclear fuel cycle.
- **Fund the promotion and fostering of cyber security** within the industry, aiming to encourage a sectoral-level approach, from the highest levels down to the individual.
- **Establish an international cyber security risk management strategy** designed to maintain momentum and agility, incorporating the necessary mechanisms for in-depth preparation to meet cyber security challenges, however these may arise, and a flexible and coordinated response.
- **Develop coordinated plans of action to address the technical shortfalls** identified, such as in patch management, and make the necessary investments.
- **Include all stakeholders** in the organizational response. This will require knowledgeable leadership at the highest levels, the free flow of information and dynamic contributions by management, staff and the wider community of stakeholders, including members of the security and safety communities.
- **Promote an environment that enables the appropriate balance between regulated and self-determined actions** to avoid any tendency for overall stagnation.

Specific recommendations

The report proposes a number of specific recommendations to address the challenges identified.

Assessing the risk – and attracting investment

- **Develop guidelines to measure cyber security risk in the nuclear industry,** including an integrated risk assessment that takes both security and safety measures into account. This will help improve understanding of the risk among CEOs and company boards and make cyber security in the nuclear sector more commercially attractive.
- **Promote cyber insurance,** which will require strong risk assessments, as an effective way to drive the process of implementing change.

Handling the 'human factor'

- **Engage in robust dialogue with engineers and contractors to raise awareness of the cyber security risk,** including the dangers of setting up unauthorized internet connections.
- **Establish rules where these are not already in place** – such as banning personal devices from control rooms and requiring nuclear plant personnel to change the default passwords on equipment – and enforce these rules through a combination of independent verification methods and technical measures, for example by blocking off USB ports.

Promoting disclosure and information-sharing

- **Encourage nuclear facilities to share threat information anonymously** (such as by revealing 'indicators of compromise') in order to promote greater disclosure, since the reluctance to disclose cyber attacks stems partly from concerns for damage to reputation.
- **Promote industry conferences and other measures to enhance interpersonal relationships** in order to encourage informal sharing initiatives, even if governments are dissuaded by national security concerns from sharing threat information at the international level.
- **Governments should lead the establishment of national Computer Emergency Response Teams (CERTs) specialized in industrial control systems,** particularly since they recognize that information-sharing at a national level is key.
- **The regulator should reassure owner-operators** that they will not be penalized for any information that they share, provided they show good faith.

Developing further international policy measures

- **Encourage all countries that have not yet done so to adopt an effective regulatory approach to cyber security at nuclear facilities.** Since a large number of countries follow IAEA guidance, allocating more resources to the IAEA to enable it to develop recommendations on responding to cyber security threats could generate significant benefit.
- **Provide technical and funding assistance to developing countries** in order to improve cyber security at their nuclear facilities.

Bridging communication gaps – including the need for cultural change

- **Establish integrated projects between nuclear plant personnel and cyber security personnel,** such as the preparation of cyber security training materials and undertaking of joint vulnerability analyses. This would also encourage IT personnel to visit the nuclear facility in person on a regular basis to aid mutual understanding.
- **Improve the frequency and quality of cyber security training at nuclear facilities,** potentially involving accreditation of training programmes by the IAEA, **and hold integrated scenario-led drills** between nuclear plant personnel and cyber security personnel to hone skills and develop common understandings and practices.
- **Promote the further creation of more cross-disciplinary university programmes** aimed at training cyber security specialists in the nuclear industry.
- **Foster partnerships between vendors and cyber security companies** to enable the development of more robust cyber security products.

Enhancing security – including the need for 'security by design'

- **Promote the importance of 'security by design',** so that future generations of industrial control systems incorporate security measures during the initial conception phase. This may mean **avoiding superfluous digital features** as well as **incorporating authentication and encryption technologies.**
- **Ensure that sufficient redundancy is retained** in digitlized systems.
- **Promote the use of 'whitelisting',** which restricts the unprecedented flexibility of digitized industrial control systems and also reduces the need to patch systems.
- **Implement intrusion detection systems such as network monitoring** of traffic for anomalous behaviour across the entire control system network, not just on the network perimeter.
- **Encourage the further adoption of secure optical data diodes.**
- **Ensure the integrity of the supply chain.**
- **Prioritize key areas for cyber security investment,** including identifying critical cyber assets at each nuclear facility.

Independent thinking since 1920

Chatham House, the Royal Institute of International Affairs, does not express opinions of its own. The opinions expressed in this publication are the responsibility of the authors.

Cover image © Korea Hydro and Nuclear Power, Handout/Getty Images

Typeset by Soapbox, www.soapbox.co.uk

Cover image: Workers of Korea Hydro and Nuclear Power Co. participate in an anti-cyber attack exercise at the Wolsong nuclear power plant on 22 December 2014 in Gyeongju, South Korea.

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223