EUROPEAN NUCLEAR SECURITY REGULATORS ASSOCIATION
ENSRA

Western European Nuclear Regulators Association
WENRA

2024

Image courtesy of Pixabay

Remarks on NUCLEAR CYBER SECURITY

ENSRA / WENRA – CYBER WORKING GROUP

In 2024 the following countries were members of ENSRA:

- Belgium
- Czech Republic
- Finland
- France
- Germany
- Hungary
- Lithuania
- The Netherlands
- Norway
- Poland
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom

Contents

Aim

This paper describes key principles of establishing an effective cyber security posture within the civil nuclear sector. Technical implementation of the programme is out of scope. However, there is a range of international/national and technical guidance available e.g. NIST, ISO, IEC to be considered as supportive material alongside this guide.

Introduction

A cyber security incident can not only impact public health, nuclear safety and the environment, but also have a prolonged impact on operations. This includes not only the operations of the nuclear facility but also the operations of industries dependent on the output of the nuclear facility. It might therefore have a significant economic impact.

As in physical security, accountability for cyber security fully lies with the top management and cannot be transferred. However, in contrast to a physical security incident, detection of a cyber security incident can be challenging and difficult to mitigate. In addition, tools facilitating cyberattacks are widely available to a broad range of adversaries which make the likelihood of a cyberattack increasingly probable. Distinguishing between state-sponsored adversaries and other adversaries is often not possible. The importance of holistic approaches to security are key to ensure that physical, personnel and cyber security can all work together to act as a compounding factor in both preventative and responsive requirements.

Therefore, it is necessary to develop, implement, and maintain an effective cyber security posture in accordance with national legislation and regulations.

Establishing Responsibilities and Capabilities

Establishing responsibilities and capabilities for cybersecurity involves defining clear ownership, roles and responsibilities for personnel involved in securing the organisation. Additionally, organizations within the sector should develop and maintain comprehensive cybersecurity capabilities. Collaboration with regulatory bodies, adherence to industry standards and regular training programs for personnel are essential components. By aligning responsibilities with capabilities and industry best practices, organisations can enhance their cybersecurity posture, safeguarding critical infrastructure from evolving cyber threats.

To facilitate cyber security, top management needs to demonstrate ownership, leadership and commitment with respect to information and cyber security. Therefore, it is necessary to

- allocate human and financial resources.
- identify and assign roles and responsibilities.
- establish and maintain awareness and competences.
- consider all stages of the facility lifetime and asset lifecycles from design to disposal.

To maintain cyber security, it is necessary to

- identify and keep track of all cyber assets and their configuration.
- keep asset information up to date.
- select, adapt and enforce cyber security measures with respect to all cyber assets.
- periodically perform self-assessment of all cyber security measures.
- support the self-assessment by independent assessments.
- consider all lifecycle phases of cyber assets.

Risk Management

Risk management in cybersecurity aims to understand the potential impact of threats and vulnerabilities, prioritize them based on their significance, and implement appropriate controls to manage and reduce the associated risks. This iterative process involves continuous monitoring and adaptation to evolving threats, ensuring that organizations can make informed decisions to safeguard their information and maintain resilience in the face of cyber challenges.

Risk assessments include

- **threat assessment**
  In conjunction with competent authorities, a facility tailored cyber threat statement takes into account the emergence of new adversarial capabilities and the applicability of existing capabilities to newly identified vulnerabilities.
- **vulnerability assessment**
  Vulnerabilities are be identified and actively tracked.
- **impact assessment**
  The impact of said vulnerabilities is analysed and their timely remediation is planned.

Cyber security risk assessment is renewed at regular intervals and immediately when something significant changes. This includes changes in threat characterization or the identification of new vulnerabilities.

Asset and Change Management

Cyber assets may be physical or digital systems, functions, persons and not necessarily located within the facility (this includes especially outsourced services such as cloud-solutions). By understanding the value and dependencies of these assets, cybersecurity professionals can implement tailored protection measures.

Change management focuses on systematically controlling modifications to the organization's environment. This includes assessing the impact of changes on security, conducting risk analyses, and ensuring that proper authorization processes are in place. Integrating these practices is essential for minimizing vulnerabilities, ensuring system availability, and facilitating a proactive response to emerging cyber threats.

Adhering to industry standards, helps organizations in implementing robust asset and change management processes, enhancing overall cybersecurity resilience. Alongside this, the integration of asset and change management processes with broader security controls will create a cohesive and proactive cybersecurity strategy.

An ***active inventory*** of all cyber assets is maintained.

A ***change management program*** for cyber assetsis maintained.

Supply chain risk management for specifying, monitoring and managing the supply of items, products and services that impact cyber security is established.

Protecting Against Compromise and Security by Design

The establishment of secure network architectures is paramount in safeguarding information systems. This involves implementing a defence-in-depth strategy, which advocates layering multiple security controls to protect against a variety of threats.

It is also important to consider a graded approach, tailoring security measures to the specific risk profile of an organization. The approach will include

- an identity and access management programme to establish and control authorized access to cyber assets.
- procedures for the identification, use, control, and protection of digital assets that interface or communicate with a system containing cyber assets.

A cyber security by design approach is applied in order to ensure the security of new facilities, systems and modifications.

Incident Preparedness and Response

Incident preparedness and response is a critical component of cybersecurity that focuses on efficiently and effectively managing and mitigating the impact of security incidents. This encompasses a systematic approach to identifying, analysing, and responding to incidents, including but not limited to cyberattacks, data breaches, and system compromises.

It is crucial to

- identify capabilities, organizational roles and responsibilities within a cyber security incident
- maintain a ***response plan*** establishing a graded approach to ensure response to cyber security incidents is consistent with the severity of the incident.
- Exercise the response plan periodically through assurance activities for response and recovery and testing the effectiveness of interfaces with other entities.
- Integrate lessons learned to enhance future incident preparedness and response.

Adhering to industry standards, ensures a structured and well-coordinated response, minimizing the impact of incidents and facilitating the restoration of normal operations in a secure manner.

Reporting and Notification

Reporting requirements play a crucial role in effective cybersecurity governance, encompassing both internal and regulatory dimensions. Internally, organizations must establish clear reporting mechanisms to promptly communicate cybersecurity incidents, vulnerabilities, and risk assessments to relevant stakeholders. This includes executive leadership, IT teams, and other key personnel.

Additionally, compliance with regulatory reporting requirements is imperative. Adhering to regulations ensures that organizations not only meet legal obligations but also contribute to a culture of transparency and accountability in managing cybersecurity risks.

By integrating both internal and regulatory reporting requirements, organizations can enhance their cybersecurity posture and demonstrate a commitment to safeguarding sensitive information and maintaining compliance with applicable laws and standards.

Annex

Supporting material :

The Cyber Security Body of Knowledge (CyBOK) v1.1.0 - The Cyber Security Body of Knowledge (cybok.org) CyBOK Version 1.1.0 © Crown Copyright, The National Cyber Security Centre 2021, licensed under the Open Government Licence: https://www.nationalarchives.gov.uk/ doc/open-government-licence/.