Nuclear Industry Association

Cyber Security: In the Nuclear Supply Chain

The UK's Civil Nuclear Sector generates around 20% of the UK's electricity needs. It is the only low carbon generating source that can provide continuous electricity on this scale to homes, schools, business and hospitals, and is a crucial part of the UK's Critical National Infrastructure. Given its key role in maintaining our security of supply, it is essential it is protected from all forms of attack, and that public and political confidence is maintained.

Cyber security, ensuring the protection of devices, services, networks and the information on them from theft or damage, is key to all organisations. In the UK nuclear industry, computers and digital assets play a crucial part in all nuclear facilities. The nature of the cyber threat is dynamic, with attackers constantly developing new ways to achieve their objectives. This, together with changes to the regulatory process, means all organisations in the sector must work together to maintain security.

At the more prosaic level, many organisations are also vulnerable to simple low technology attacks that could be mitigated through the application of basic cyber hygiene measures. Nuclear industry suppliers have a pivotal role to play in ensuring the supply chain is not an easy target for those looking to cause disruption or to steal information.

The UK Government launched, in February 2017, a five year sector **Civil Nuclear Cyber Security Strategy (CNCSS)**.[1] The first sector specific cyber strategy for Critical National Infrastructure. The aim of this document is to provide clear information to the nuclear supply chain on how to prevent, recognise and respond to cyber-attacks.

WHAT ARE CYBER-ATTACKS AND CYBER SECURITY?

Cyber-attacks are malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.[2] **Cyber security** is the protection of devices, services and networks - and the information on them - from theft or damage.[1]

Six in ten (58%) critical national infrastructure companies have low confidence in maintaining all supply chain companies are secure against cyber-attacks.[3] While 50% have low confidence that their employees are aware of the part they play in protecting their organisation from cyber-attacks.[2]

Cyber-attacks can be linked to a variety of actors including: nation states, organised crime, hacktivists, disgruntled staff and terrorist groups. The **National Cyber Security Centre (NCSC)** provides a weekly **threat report** which highlights the key global cyber related incidents. The recent **Wannacry** and **NotPetya** malware demonstrates the heavy financial losses that organisations can suffer.

[1] Civil Nuclear Cyber Security Strategy, Department for Business, Energy & Industrial Strategy – https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591619/170213_-_Civil_Nuclear_Cyber_Security_Strategy.pdf

[2] National Cyber Security Centre Glossary, NCSC, 2016 – https://www.ncsc.gov.uk/glossary

[3] Atkins Cyber resilient infrastructure report, Atkins – http://explore.atkinsglobal.com/cyber/

TYPES OF CYBER-ATTACK

PHISHING

Attempt to obtain sensitive information (username, password etc) by disguising as a trustworthy entity in an email

MALWARE

Malicious software - includes viruses, trojans, worms or any code or content that could have an adverse impact on a system

SQL INJECTION

A code injection technique used to attack data-driven applications through its SQL database

PHARMING

An attack on a network infrastructure that results in users being redirected to an illegitimate website

RANSOMWARE

Malicious software that makes data or systems unusable until the victim makes a payment

TYPES OF ATTACKER

NATION STATE

State sponsored that aims to disrupt and damage infrastructure, spread propaganda, or manipulate opinion

CYBER CRIMINALS

Interested in making money through fraud or from the sale of valuable information

HACKTIVIST

Those who wish to attack companies for political or ideological motives

ESPIONAGE

Industrial competitors interested in gaining economic advantage for their companies

INSIDER

Employees, or those who have legitimate access, either by accidental or deliberate misuse

WHY IT IS IMPORTANT NOW AND FOR THE NUCLEAR INDUSTRY

a. There have been a number of well documented cyber-attacks on other national civil nuclear and energy industries.

b. Cyber attackers have quickly evolving tools and more sophisticated techniques to target IT systems.

c. Increased risk in the nuclear industry with a trend towards digitisation and use of ‘off the shelf’ IT systems.

d. Organisations can be targeted by actors to gain something of value. This can be anything from personal data to sensitive nuclear information. There is much intellectual property developed within supply chain that provides both competitive advantage and differentiation; it is vital to protect such valuable information from theft.

e. The nuclear sector is a key part of the UK’s Critical National Infrastructure.

CONCERNS FOR THE NUCLEAR SUPPLY CHAIN

The supply chain is essential to the overall cyber and physical security of the nuclear industry. Its security therefore needs to be carefully managed.

Supply chain companies need to take measures proportionate to the risks they face. The robust physical security in the nuclear sector that has been developed may make cyber the preferred attack vector, and therefore more likely.

All sectors in the supply chain (including those beyond the regulator’s relationship with licensed nuclear sites) are required to engage with cyber security measures, to ensure successful delivery. This will require relationships with partnering companies, contractors and suppliers to provide the proportionate risk ownership, understanding and mitigation (even at the most basic level).

Through demonstrating good cyber security, relationships can be improved between contract companies and dutyholders, and this can even lead to the possibility of new contracts.

CYBER REGULATION IN THE NUCLEAR SECTOR

Security regulation in the UK nuclear industry has undergone a transformation, following the publication of the **Security Assessment Principles (SyAPs)** in 2017.

The Office for Nuclear Regulation (ONR) use these SyAPs, together with supporting **Technical Assessment Guides (TAGS)**, to guide regulatory judgements and recommendations when undertaking assessments of duty holders' security submissions such as site security plans and transport security statements.

Key regulation for the nuclear supply chain falls under Regulation 22 of the **Nuclear Industries Security Regulations (NISR) 2003.** This requires duty holders to maintain such security standards, procedures and arrangements as are necessary for the purpose of minimising the risk of loss, theft or unauthorised disclosure of, or unauthorised access to, any **Sensitive Nuclear Information (SNI).** Whilst not taking precedent over these legal definitions, a simple, working definition of SNI can be described as information relating to activities carried out on or in relation to civil nuclear premises; and deemed to be of value to an adversary planning a hostile act. This definition and further guidance can be found within ONR's Classification Policy.

For a dutyholder to demonstrate evidence of effective arrangements in this area and noting that SNI always accompanies a Government Security Classification (GSC), ONR considers the expectations and requirements articulated within the HMG Security Policy Framework (SPF) to be relevant good practice. As such ONR have directly mapped five of the 10 **Fundamental Security Principles (FSyP)** from the SyAPs to SPF in order to provide a framework for dutyholders to evidence their arrangements and for regulators to make judgements on their adequacy.

FSyP 1 - Leadership and management of security: The need to implement and maintain organisational security capability underpinned by strong leadership, or a robust governance process.

FSyP 2 - Organisational Culture: The need to encourage and embed an organisational culture that recognises and promotes the importance of security.

FSyp 3 - Competence Management: The need to implement and maintain effective arrangements to manage the competence of those assigned security roles and responsibilities.

FSyP 7 - Cyber Security and Information Assurance: The need to implement and maintain effective security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.

FSyP 8 - Workforce Trustworthiness: The need to implement and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity.

Further guidance is available on the ONR's List N webpage or by contacting ONR directly at listn@onr.gov.uk.

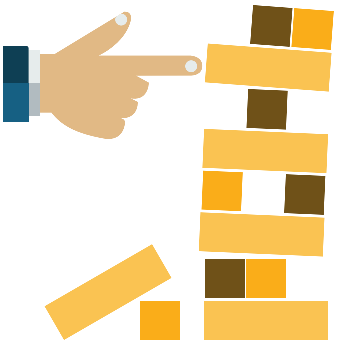
KEY PRINCIPLES OF SUPPLY CHAIN SECURITY

In January 2018, NCSC and the **Centre for the Protection of National Infrastructure (CPNI)** issued new guidance to help organisations establish effective control and oversight over their supply chains.

The guidance proposes a series of 12 key principles, divided into four sections, each representing a stage in the process.

Implementation of these recommendations will improve overall resilience, reduce the number of business disruptions companies suffer and the damage they cause. It will also help suppliers demonstrate compliance with the General Data Protection Regulation 2018 (GDPR), which builds upon the **Data Protection Act 1998 (DPA)** and the **Privacy and Electronic Communications Regulations 2003 (PECR).**

WHAT ARE THE RISKS TO ORGANISATIONS?



Cyber threats may impact on an organisation's safety–related functions and could also have financial consequences.

A cyber-attack could have a disproportionate reputational effect on businesses within the nuclear industry. From a national perspective a cyber security breach could damage the public's perception of nuclear even if the attack does not affect a nuclear specific activity.

On a larger scale, an attack could disrupt supply, damage facilities, delay hazard and risk reduction, and risk adverse impacts sites, the public or environment.[4]

NCSC/CPNI guidance focuses on key questions organisations should ask their supply chain to understand the risks.

CASE STUDIES IN NUCLEAR (AND ENERGY) SUPPLY CHAIN CYBER SECURITY ATTACKS

In the supply chain there have been problems globally with counterfeit and compromised software:

- Since 2011, the cyber-espionage group known as Dragonfly has allegedly been targeting energy sector companies across Europe and North America. In their latest campaign, Dragonfly successfully **"trojanised"** legitimate **industrial control system (ICS)** software. Subsequently, when the ICS software was downloaded from the suppliers' websites it would install malware alongside legitimate software. The malware included additional remote access functionalities that could be used to take control of the systems on which it was installed.

- **Stuxnet**, a malicious computer worm, was responsible for causing substantial damage to the Iranian nuclear program. Hackers attacked the plant of Natanz in Iran in 2010, interfering with the nuclear program.[5] It is one of the clearest examples of how the use of a malicious code can significantly interfere with operations at a nuclear plant through its supply chain.

- In 2014 the Monju Nuclear Power Plant in Japan was attacked by malware which resulted in 42,000 emails and staff training reports lost.

- A series of powerful cyberattacks using the **Petya malware** swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms in 2017. Similar infections were reported across Europe, the United States and Australia. It is estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany second hardest hit with about 9%.

- The **WannaCry** ransomware attack, a worldwide cyberattack by a **cryptoworm**, targeted computers running Microsoft Windows by encrypting data and demanding ransom payments. WannaCry largely affected organizations that had not applied updates or were using older Windows systems past their end-of-life. Whilst it was not strictly an energy sector attack, this shows how important basic software and hardware updates can be.

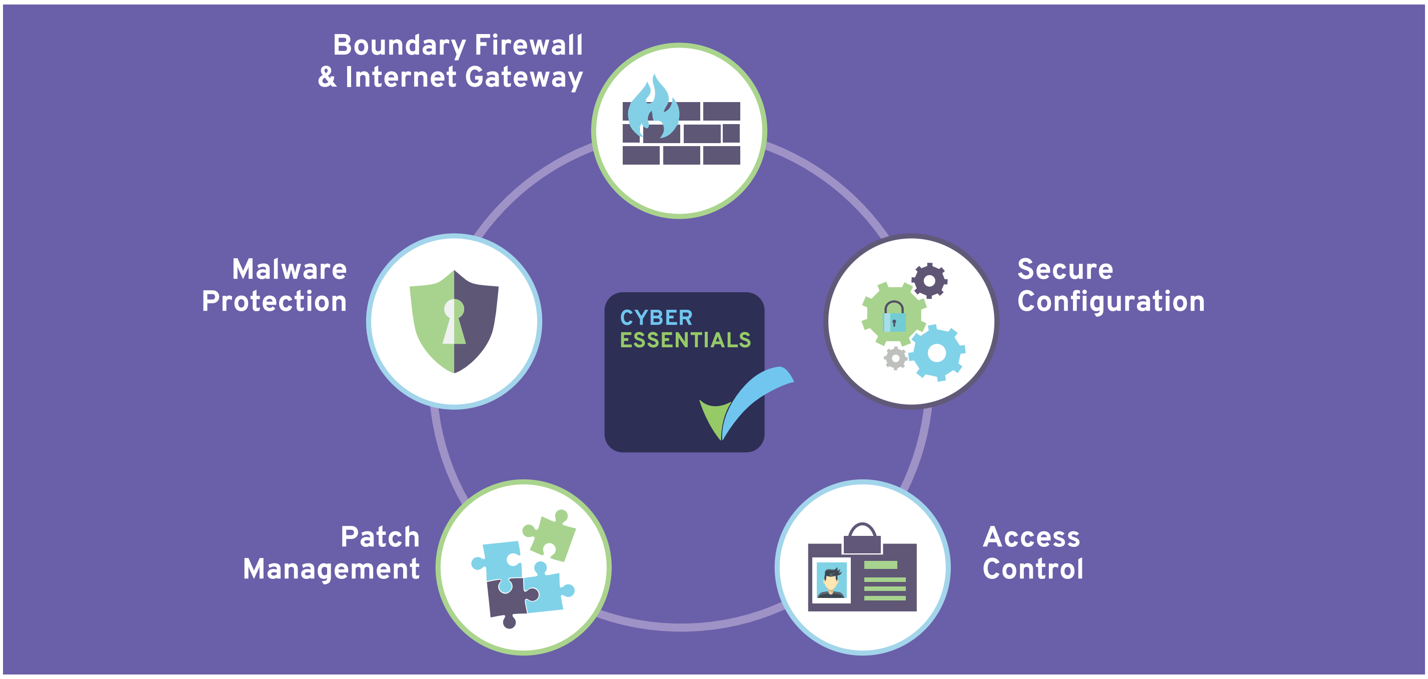
CYBER ESSENTIALS

Cyber Essentials is a Government backed industry scheme that helps organisations protect themselves against common online threats. It is suitable for organisations of any size and in any sector. The Nuclear Decommissioning Authority already requires all suppliers bidding for certain contracts, which are assessed to pose an element of information risk, to meet the requirements of the Cyber Essentials scheme.

It defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet.

[4] Civil Nuclear Cyber Security Strategy, Department for Business, Energy & Industrial Strategy – https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591619/170213_-_Civil_Nuclear_Cyber_Security_Strategy.pdf

[5] The Vulnerability of Nuclear Facilities to Cyber Attack, Brent Kesler, Strategic Insights, 2011 – https://calhoun.nps.edu/bitstream/handle/10945/25465/The_Vulnerability_of_Nuclear_Facilities_to_Cyber_Attack.pdf?sequence=1&isAllowed=y



Cyber Essentials covers the basics of cyber security in an organisation's enterprise or corporate IT system. There are two levels of certification – Cyber Essentials and Cyber Essentials Plus. Cyber Essentials Plus is more rigorous as it requires vulnerability tests to be performed as part of the certification.

Government widely encourages its adoption and made it mandatory for Central Civil Government contracts advertised after October 2014 for those contracts which feature handling personal information and provision of certain ICT products and services.

There is no direct correlation between ISO27001 (Information Security Management) and the Cyber Essentials scheme; being certified to ISO27001 does not provide an equivalent level of assurance unless the Cyber Essentials requirements have been included in the scope of ISO27001 and verified as such.

Cyber Essentials standards have been achieved by key organisations such as the Nuclear Decommissioning Authority, Radioactive Waste Management and International Nuclear Services. Private sector and local government organisations can also apply Cyber Essentials in their dealings with private sector supply chain providers.

Further reading can be found at www.gov.uk/government/publications/cyber-essentials-scheme-overview and www.cyberessentials.ncsc.gov.uk.

WHO TO CONTACT ?

In the case of a cyber-attack contacting the NCSC is an essential first step. This should also be the first step in the case of ransomware, contact should also be made with Action Fraud. The ONR would also need to be notified of any security breaches, this can be done through their incident notification form.

For supply chain organisations, if a breach has been detected and where appropriate, it may also be important to inform their contract holder/duty holder.

One of the most useful tools to get up to date cyber security information is to become a member of Cyber Security Information Sharing Partnership (CiSP). This platform allows you to share information securely with government and other members and access free network monitoring reports.

Organisations may benefit from developing an incident response plan, for confirmed breaches which require a proportionate response. This may include contacting the above suggested bodies but could also include an action for what comes next.

Further guidance and examples for a good incident response plan can be found on the NCSC Incident management page or in the Crest Cyber Security Incident Response guide.

The Nuclear Industry Association (NIA) is the trade association for the civil nuclear industry in the UK, representing more than 250 companies across the supply chain. The diversity of NIA membership expertise in new build, management and decommissioning enables effective and constructive industry-wide interaction.

Nuclear Industry Association
is a company limited by guarantee
registered in England No. 2804518

Registered Office:
5th Floor, Tower House
10 Southampton Street
London WC2E 7HA
TEL +44(0)20 7766 6640
EMAIL info@niauk.org

NIAUK.ORG

Follow us: @NIAUK

With support of:

Department for
Business, Energy
& Industrial Strategy

National Cyber
Security Centre
a part of GCHQ

NDA
Nuclear
Decommissioning
Authority

ONR
Office for
Nuclear Regulation