The National Skills Academy
NUCLEAR

Excellence in skills for nuclear

Cyber & Information Security Awareness Training for the UK Nuclear Industry

Individuals | Organisations | Assurance | Governance | Regulatory Requirements | Bespoke Training & Support

Increasing the knowledge, capability and agility of organisations to deal with all aspects of the cyber and information security challenges facing the nuclear industry in the UK.

Background and Context

Cyber security is a growing issue for all organisations, large and small. Across the UK, 65% of companies have had cyber-related incidents in the last 12 months; the reparation of which is becoming increasingly costly. The growing number of breaches have the potential to cause serious financial, operational and reputational damage.

In February 2017 the Government launched *"The National Cyber Security Strategy."* This strategy sets out what cyber risks will be addressed, by whom, when, and how success will be measured. The strategy sets out a path to keeping the UK civil nuclear sector ahead of rapidly evolving threats to, and vulnerabilities in, software and equipment in the next five years. It sets out clear expectations, and the roles that the industry, Government and Regulators need to play.

"Success will be an increasing capability, capacity and agility of stakeholders to deal with all aspects of the cyber security challenges faced by the UK civil nuclear sector."

The government's strategy includes a commitment from the UK civil nuclear duty holders to:

- Establish and sustain robust, effective, agile and assurable cyber security governance arrangements;
- Undertake appropriate risk management processes that pre-emptively reduce the associated risks;
- Increase the sector's capability and capacity to understand and manage cyber security risks where required;
- Ensure that known cyber security vulnerabilities are mitigated, so far as is reasonably practicable;
- Ensure that they are resilient to, and defend themselves against, evolving cyber threats; and
- Work with their supply chain to support and encourage them to manage and mitigate their cyber vulnerabilities.

For the supply chain, the expectation is that it will:

- Increase its capability and capacity to understand and manage cyber security risks where required;
- Ensure that they have processes in place to notify duty holders of cyber incidents or vulnerabilities;
- Ensure that known cyber security vulnerabilities are mitigated, so far as is reasonably practicable; and
- Undertake appropriate risk management processes that pre-emptively reduce the associated risks.

What is the training need for individuals?
Given the above context, and the fact that 50 % of the worst security breaches are caused by human error, it is recommended that all employees are educated in the essentials of cyber security.

Businesses need to consider both initial and refresher training to ensure that all staff understand the risks, and actively seek to protect themselves, both professionally and personally, from cyber and other security-related threats. This should include the latest in good practice in relation to ransomware, phishing, passwords, social engineering, malware, USB sticks, plus security at home and on the move, as well as in the workplace. This is covered in Part A of the NSAN course.

What is the training need for organisations?
Senior Managers and leaders will benefit from high level awareness of cyber security and the requirement for an effective information security management strategy and system. Organisations need to identify the relevant legal and regulatory requirements, such as those emanating from the Office for Nuclear Regulation, and understand what good looks like in terms of governance and compliance.

"Part A is clearly aimed at individuals and part B is focused on the organisation so considered more relevant to company management teams. Links to nuclear context is good with regulatory guidance information."

Comment from a course pilot attendee, June 2017.

Learning Outcomes

Our courses aim to achieve the following learning outcomes:

Part A: Nuclear Cyber & Information Security Awareness for Individuals

- Identify the main types of cyber security threats
- Understand how to counter those threats
- Understand the implications to both individual and companies of not complying with security protocols
- Have the required knowledge to identify what additional training they may need to reduce their own and company's security risk profile.

Course outline:

- Putting cyber security into context for the individual
- Identifying the damage to a business that a cyber security attack could cause
- Cyber security attack methods
- Strategies to counter the attack

"Great engagement, the tutor brought the topic to life."

"I think this course would be good for introducing good behaviours in IT. Not necessary knowledge of IT, but explaining good practice in human behaviour and that the potential cost to the company can be high. This must be backed up with good policies, which the company must create."

"A cyber security awareness course of great value to all employees. The full 1/2 day is a big investment, so the shorter e-learning package for inductions and refresher training is also an attractive option so that we can roll out the training to all staff."

Part B: Nuclear Cyber & Information Security Awareness for Organisations

- Understand how an information security management framework can enable compliance
- Understand the implications to both individuals and companies of not having an information security strategy
- Identify legal & regulatory requirements relevant to the nuclear industry
- Learn the importance of developing risk, recovery & incident plans, monitoring, testing and continuous improvement activities.

Course outline:

- Cyber & information security in the context of the nuclear industry
- Civil Nuclear Cyber Security Strategy
- ONR Security Assessment Principles (SyAps)
- International regulation (e.g. GDPR) and standards (e.g. ISO27001)
- Activities required to reduce cyber risk
- Good governance, policies & procedures
- Strategies for ongoing improvement

"The right depth of topic suitable for SME business leaders."

"This one is certainly aimed more at people within the governance functions, company managers, and people working in C&I. I really enjoyed the risk management aspect, and it certainly got me thinking about vulnerabilities I have at work."

"Excellent training for SIROs, which every nuclear company must have. Also, all information security professionals, IT or OT managers, CISO, supply chain security, and possibly HR and procurement managers. Thank you for an excellent and thought provoking course."

Training Formats

NSAN offers a range of remote and face-to-face formats that can be used alone or blended to provide a tailored programme to meet your requirements in terms of preferred learning method, staff numbers, availability and budget. A description of these formats and a guide to how they could be applied to the different "user groups" within your business is shown in the following table:

Format → / Level ↓	1 hour elearning module (awareness level knowledge of cyber security and the threats and mitigations specific to the nuclear industry)	1 hour Webinar (covering Part A or B headline topics, or a mix of both. Can be delivered "open" for all companies or "closed" format for single clients)	Face-to-face courses (½ day awareness up to 2 days or more for more in depth/advanced training bespoke to individual client's needs)
All/general users	√	√	
Admin users/controllers	√	√	√
Leaders & Managers		√	√
Specific functions e.g. C&I, procurement, project management, etc.		√	√

Webinar and face-to-face formats are subject to demand

Advanced Training & Further Support

In addition to the awareness training described in this leaflet, we can provide advanced training in cyber & information security to provide a greater level of depth and granularity in knowledge.

In addition, NSAN's Consultancy Service can provide hands-on support to help you achieve the following:

- Implementing & Certifying to ISO 27001 – Information Security Management
- Implementing & Certifying to ISO 22301 – Business Continuity
- Cyber Essentials & Cyber Essentials Plus Certification – HMG baseline cyber controls
- IASME Governance Certification – For SMEs and supply Chain
- Risk Management Planning – Risk identification, assessment & treatment
- Audit & Assessment provision

Next Steps

To register your interest, discuss your specific cyber security training needs and for prices, dates and NSAN member discounts, please contact your NSAN Operations Manager.

Alternatively contact…

T 01900 898120
E enquiries@nsan.co.uk
W nsan.co.uk