Cybersecurity in the Nuclear Industry

WINS Academy

CONTENTS

WHO THIS MODULE IS FOR

The audience for this module includes managers with responsibility for security as well as regulators, government departments and others who wish to better understand the background and implications of cybersecurity in the nuclear industry. The technical content is introductory, requiring no prior cybersecurity knowledge.

KEY ISSUES

Digital technologies are now integrated into nearly all aspects of nuclear facility operations. These technologies are incorporated into nuclear security systems, nuclear safety systems, nuclear material accountancy and control systems, and systems supporting emergency response services. Over recent years, individuals and groups with malicious intentions have recognised that this shift has increased the opportunity for cyberattacks.

Cybersecurity, at its foundation, is the protection of information technology systems and operational technology systems from cyberattack. This module introduces the importance of cybersecurity to the nuclear industry to help learners reflect on how cybersecurity could be improved in their own organisation. Cybersecurity is a strategic risk to be managed, and by completing this module you can assist your organisation increase its cybersecurity resilience.

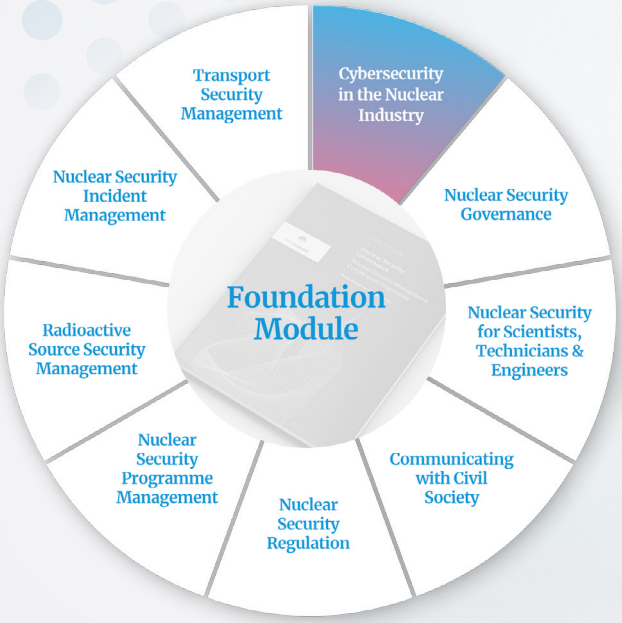
KEY LEARNING OBJECTIVES

The overall objective of this module is to provide you with an overview of cybersecurity in the nuclear industry, including its challenges, terminology, relevant best practice and standards. Successfully completing this module will help you communicate more effectively with specialist cybersecurity professionals and help you make informed decisions about cybersecurity in your organisation.

By the time you have completed this module you will understand:

- Cybersecurity in the context of the nuclear industry
- Cyberthreat actors (both insiders and external adversaries)
- IT and OT systems within nuclear facilities that may be the target of a cyberattack
- Vulnerabilities that may be exploited by a cyberthreat
- The types of cyberattacks that may be carried out by cyberthreats
- Cyberattack vectors
- The potential consequences of cyberattacks on an organisation and on wider society
- The nature of the different responsibilities within a State for cybersecurity, including regulatory bodies, operators and providers in the supply chain
- The key elements of, and importance of, developing an effective cybersecurity risk management strategy as part of a wider organisational or enterprise risk management strategy
- The need for cybersecurity to be incorporated as an essential component of the wider organisational culture and methods to establish this culture within your organisation
- Required cybersecurity competences in your organisation
- Ongoing and emerging issues related to cybersecurity in the working environment
- Essential organisational practices for planning, preparedness and response to a cybersecurity incident
- The importance of cybersecurity resilience for the nuclear industry

WINS Academy



OUTLINE

UNIT 1: CYBERSECURITY IN THE NUCLEAR INDUSTRY

1.1 Cybersecurity
1.2 Cyberthreats
1.3 Cyber Targets: Nuclear Facility Scenarios
1.4 Cyberattacks and their Consequences

UNIT 2: NATIONAL RESPONSIBILITIES FOR CYBERSECURITY

2.1 Responsibilities of the State
2.2 Responsibilities of Operating Organisations for Cybersecurity
2.3 Supply Chain Management

UNIT 3: CYBERSECURITY RISK MANAGEMENT

3.1 Risk
3.2 Cybersecurity Risk Reduction Strategy
3.3 Evaluating Cybersecurity Risk Management

UNIT 4: CYBERSECURITY CULTURE

4.1 Cybersecurity Culture
4.2 Cybersecurity Competence
4.3 Cybersecurity and the Working Environment

UNIT 5: CYBERSECURITY INCIDENT PREPAREDNESS AND RESPONSE

5.1 Cybersecurity Incident Response Planning and Preparedness
5.2 Responding to Cybersecurity Incidents
5.3 Communicating about Cybersecurity Incidents

UNIT 6: CYBERSECURITY SCENARIOS

6.1 Scenario 1: Digitisation of Systems and the Supply Chain
6.2 Scenario 2: Regulation and Threat Assessment
6.3 Scenario 3: Cybersecurity Risk Management
6.4 Scenario 4: Cybersecurity Culture
6.5 Scenario 5: Cybersecurity Incident Preparedness and Response

COURSE SUMMARY