Cybersecurity in the Nuclear Industy

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.

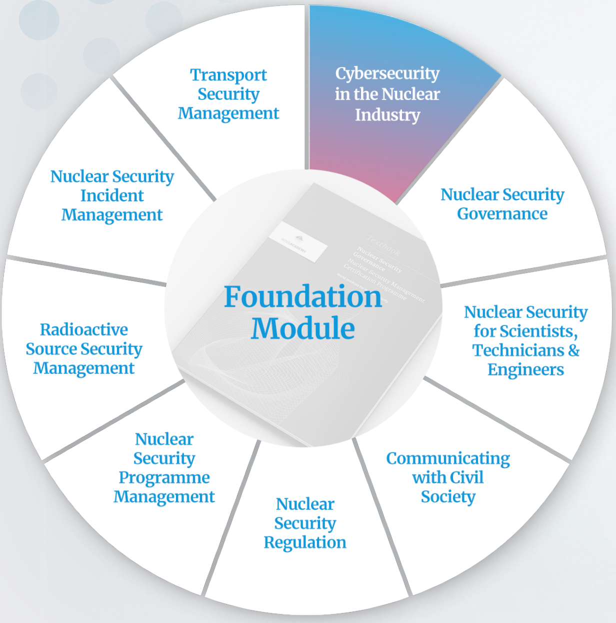
KEY ISSUES

In recent decades improvements in computer technology have changed the way people around the world live and work. Once digitisation was demonstrated to have clear benefits for the safety, security and economics of the nuclear industry, operators began to digitise operations and replace analogue equipment with digital systems. The supply chain has embraced the trend of digitisation, and many previously analogue components are now digital.

However, the benefits of digitising systems come at a cost. Cyberthreats working within an organisation (insider) or remotely from any location in the world (external adversary)—can launch a *cyberattack* that enables them to steal, alter or destroy sensitive information. Loss of such information can have harmful consequences, especially if the cyberattack alters the computerised instructions that control systems inside nuclear facilities. In the nuclear industry, one of the most concerning consequences would be damage leading to the uncontrolled release of radioactivity offsite.

KEY LEARNING OBJECTIVES

By the end of the course, participants will better understand the information technology (IT) and operational technology (OT) systems that could be the target of a cyberattack; who the cyberthreats might be, including their motivation, intention and capability; and steps that nuclear organisations can take to effectively prepare for and respond to a cybersecurity incident.


Foundation Module
Cybersecurity in the Nuclear Industry
Nuclear Security Governance
Nuclear Security for Scientists, Technicians & Engineers
Communicating with Civil Society
Nuclear Security Regulation
Nuclear Security Programme Management
Radioactive Source Security Management
Nuclear Security Incident Management
Transport Security Management

WINS Academy
Textbook
Cybersecurity in the Nuclear Industry
Nuclear Security Management Certification Programme
World Institute for Nuclear Security

OUTLINE

UNIT 1: CYBERSECURITY IN THE NUCLEAR INDUSTRY

1.1 Cyberthreats: Insiders and External Adversaries

1.2 Cyber Targets: Nuclear Facility Systems

1.3 Cyberattacks and their Consequences

UNIT 2: ROLES AND RESPONSIBILITIES FOR CYBERSECURITY

2.1 Roles and Responsibilities of the State, Including Regulatory Bodies

2.2 Roles and Responsibilities of Operating Organisations

2.3 Roles and Responsibilities in the Supply Chain

UNIT 3: CYBERSECURITY RISK MANAGEMENT

3.1 Cybersecurity Risk Assessment

3.2 Cybersecurity Risk Management Strategy

3.3 Performance Evaluation of 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 Preparing to Respond

5.2 Responding to Cybersecurity Incidents

5.3 Communicating about Cybersecurity Incidents

UNIT 6: SCENARIOS

COURSE SUMMARY