ICS Managers Security course outline (4 hours)

The NCSC and CIISec certified **ICS Managers Security Course** is designed to provide those at Managerial level (or equivalent) with an understanding of today's cyber security challenges facing their environments. This knowledge is vital when managing the day to day running of all aspects of security risk for those environments.

The course will show how to best identify and support their organisations' cyber security and risk mitigation/reduction strategies for their ICS environments.

Siker have worked in partnership with the National Cyber Security Centre (NCSC) the Centre for the Protection of National Infrastructure (CPNI) in the UK and leading Critical National Infrastructure (CNI) organisations.

Who should attend?

If you are a manager responsible or accountable for any ICS environment and/or people working on securing these systems including:

- Business Technical/Engineering/Procurement Lead
- ICS Policy/Decision maker
- Site/Asset Single Point of Accountability (SPA) for security and/or incident response
- Site/Asset IT Manager
- Site/Asset Physical security/Facilities Management professional

….**then this course is for you!**

It provides a high-level understanding of what the current and emerging cyber security risks are and the threats that your ICS environments face. In addition, it discusses how to forward plan to help mitigate and reduce these risks.

Pre-Requisites

There are no pre-requisites for this course and no laptop is required. A handbook of supporting material is provided.

What you will learn on this course

By the end of the course, you will be familiar with:

- How to identify what current and emerging threats your ICS environments face
- Where your ICS environments may be vulnerable
- What actions you need to take to secure those environments and help reduce the risk
- How to prepare for and manage a cyber security incident in those environments

Course Duration

The course consists of 4 hours of classroom training. Part one covers the current and emerging ICS risk landscape and Part 2 covers risk reduction planning and Incident Response.

Course Contents

Part 1: Background (what is an ICS, what are the threats and vulnerabilities)

- ICS description and terminology
- ICS Vs IT. Differences and similarities
- ICS Attack Surface
- Introduction to ICS Security Risk
- Known ICS security incidents

Part 2: Securing ICS (what can be done to secure an ICS)

- Planning to reduce the security risk
- Introduction to Cyber Incident Response
- Operational security
- Vendor management
- Building security into the procurement processes

Accreditation

This course has been accredited under the NCSC Certified Training scheme and the Chartered Institute of Information Security (CIISec) Accredited Training scheme. Attendees can earn 4 CPE credits.

What training should follow on from this?

This course is an awareness level course but it can be used as preparation for more advanced training such as the Siker ***ICS203: ICS Practitioners Security*** course and ***ICS405: Securing ICS*** course and the GIAC Global Industrial Control Systems Professional (GICSP) certification.

For more information go to www.sikercyber.com

Certified Training

in association with National Cyber Security Centre

iisp Accredited Course.