



## Industrial Cyber Security

Reducing Cyber Risk, Operating Securely

### ► Upcoming Sessions

19-23 Aug 2024	Online	\$3,950
11-15 Nov 2024	Online	\$3,950
17-21 Feb 2025	Online	\$3,950

### ► Training Details

#### TRAINING COURSE OVERVIEW

The threat posed by cyber attacks is pervasive and global, impacting individuals, commercial organizations, and nation states alike. Safeguarding your organization and technology from such attacks, and understanding how to detect, analyze, respond to, and investigate cyber incidents, is crucial. The repercussions of an information security breach, such as the documented case of the Ukraine Power Station attack, underscore the importance of robust defenses.

Cyber attacks are increasing both in frequency and sophistication. Integrated networked control systems and reliance on strategic partners further underscore organizational risks and competitive vulnerabilities. To effectively combat cyber threats, it is essential to comprehend the motives and methods of cyber threat actors. Implementing best practices, management techniques, and appropriate countermeasures can mitigate these risks and bolster asset protection.

Leaders across organizations—from boards of directors to corporate officers, chief engineers, and frontline employees—are increasingly aware of the implications of cyber breaches. Recognizing the potential personal liability involved, cyber security has become a cornerstone value in today's digital economy environment.

#### **This Anderson online training course will feature:**

- ▶ An understanding of Cyber Security issues
- ▶ Approaches to Cyber Security within an Operational Technology environment.
- ▶ An introduction to Cyber Security Frameworks
- ▶ Current Best Practices for Cyber Security Response
- ▶ Approaching Cyber Security Response Plans

#### TRAINING COURSE OBJECTIVES

#### **By the end of this online training course, participants will be able to:**

- ▶ Understand Information Security, and how this is deployed in an Operational Technology Environment
- ▶ Understand a range of Cyber threats and assess a security posture within an Operational Technology environment
- ▶ Appreciate the leading legislation, International Standards and Governance models for Cyber Security and current best practice
- ▶ Understand the approaches for Crisis and Incident Management for Cyber Security Breaches

## DESIGNED FOR

**This Anderson online training course is suitable to a wide range of professionals but will greatly benefit:**

- ▶ Legal Professionals
- ▶ System Engineers
- ▶ Security Administration
- ▶ Operational Staff
- ▶ Those whom have involvement with and responsibility for operational technology, information technology, & risk assessment

## LEARNING METHODS

This Anderson online training course will use a variety of proven adult learning techniques to ensure maximum understanding, comprehension and retention of the information presented. The training course is highly interactive and is carefully designed to provide the best mix of experience, theory and practice in a professional learning environment. The emphasis is on real case studies, and practical applications through “hands-on” action learning.

## ▶ Training Details

### Day One: What is Cyber Security?

- ▶ Overview of Cyber Security for Industries
- ▶ Cyber Crime and Attacks
- ▶ Technology, Policing, and Investigation of Electronic Crime
- ▶ Ethical Hacking and Cyber Crime
- ▶ Civil and Criminal Considerations

### Day Two: Assessing Your Cyber Security Posture

- ▶ Cyber Security and Risk Assessment
- ▶ Information Security and Standards
- ▶ ISO7799 - Information Security Management - Code of Practice
- ▶ ISA99 - International Standards for Automation Cyber Security Standard
- ▶ Reducing Your Security Risk and Increasing Your Security Capabilities

### Day Three: Cyber Security and Industrial Control Systems Management

- ▶ Information Security and Operational Technology
- ▶ Emerging Industrial Technology Trends
- ▶ Metcaf's Law
- ▶ Moore's Law
- ▶ Mirrors World

### Day Four: Cyber Security Controls

- ▶ Selecting Security Controls and Best Practice
- ▶ Considerations for Enhancing Security
- ▶ Detection, Prevention and Offensive Responses
- ▶ Securing and Assessing OPERATIONAL TECHNOLOGY Environments (OTE)
- ▶ OTE User Management, System Integrity, Data Confidentiality & Restricted Data Flow

### Day Five: Building a Cyber Response Plan

- ▶ Defining a Cyber Response Strategy
- ▶ Composing Cyber Response Plan
- ▶ Cyber Response Team Compilation and Service Vendor Support
- ▶ Cyber Preparedness and Corporate Governance
- ▶ Operational Security Centers

## ▶ Preview

10:30 - 11:00	:	Welcome, Setup, Registration
<b>11:00 - 12:30</b>	:	<b>First Session</b>
12:30 - 12:45	:	Break (15 minutes)
<b>12:45 - 14:15</b>	:	<b>Second Session</b>
14:15 - 14:30	:	Break (15 minutes)
<b>14:30 - 16:00</b>	:	<b>Third Session</b>

## ▶ The Certificate

An Anderson e-Certificate will be provided to delegates who attend and complete the online training course

### ▶ INFO & IN-HOUSE SOLUTION

For more information about this course, call or email us at:

Call us: [+971 4 365 8363](tel:+97143658363)

Email: [info@anderson.ae](mailto:info@anderson.ae)

Request for a Tailor-made training and educational experience for your organization now:

Email: [inhouse@anderson.ae](mailto:inhouse@anderson.ae)

**Anderson**  
Executive Development Centre

P.O Box 74589, Dubai, United Arab Emirates

Web: [www.anderson.ae](http://www.anderson.ae)

Email: [info@anderson.ae](mailto:info@anderson.ae)

Phone: +971 4 365 8363

Fax: +971 4 360 4759

©2024. Material published by Anderson  
shown here is copyrighted.

All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.