5 Days

Industrial Cyber Security

Reducing Cyber Risk, Operating Securely

Upcoming Sessions

22-26 Jul 2024	Dubai - UAE	$5,950
16-20 Dec 2024	Dubai - UAE	$5,950

Training Details

TRAINING COURSE OVERVIEW

The threat of Cyber Attacks is widespread and global, and effects individuals, commercial organisations and nation states alike. The ability to safeguard your organisation and technology from attacks, and more importantly understand how to identify, analyse, respond and investigate cyber-attacks as a security breach is paramount. The ability for an Information Security Breach resulting in the circumvention of operational technology controls can have disastrous effects, as we have seen with global documented case such as Ukraine Power Station attack.

Attacks are growing in number and sophistication. The networked control systems are often integrated and reliance with specialist strategic partners underpins your organisational risk and competitive ability. Furthermore, to effectively detect and deter any cyber-attack, you need to understand the nature, motive and ways of perceived cyber threat actors. In doing so and utilising appropriate countermeasures, best practice and management techniques will mitigate the risk of cyber-attack and enhance protection to your assets.

Boards of directors, corporate officers, chief engineers and frontline employees are starting to understand the implication of Cyber breaches within their organisation and their potential effect to their personal liability. Therefore, Cyber Security is a core value for leaders in today's digital economy environment.

This Anderson 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 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 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 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

The Certificate

Anderson Certificate of Completion will be provided to delegates who attend and complete the course

INFO & IN-HOUSE SOLUTION

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

Call us: +971 4 365 8363

Email: info@anderson.ae

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

Email: inhouse@anderson.ae

Anderson
Executive Development Centre

P.O Box 74589, Dubai, United Arab Emirates

Web: www.anderson.ae

Email: info@anderson.ae

Phone: +971 4 365 8363

Fax: +971 4 360 4759