

IT SECURITY IN THE OIL & GAS INDUSTRY FOR MANAGERS

“Safeguard digital operations and energy assets through strategic cybersecurity management.”

Schedule

Venue	Fees
In-House	ASK FOR THE QUOTATION

Introduction

As the oil & gas industry accelerates digitalization across upstream, midstream, and downstream operations, the risk of cyberattacks on critical infrastructure has never been higher. This 5-day manager-focused course empowers leaders to understand, evaluate, and mitigate IT and OT cybersecurity threats specific to the energy sector. Participants will explore key frameworks, attack surfaces, asset protection strategies, and regulatory compliance requirements relevant to industrial control systems (ICS), SCADA, and cloud-enabled infrastructure.

Objectives

Participants will:

- Understand cybersecurity fundamentals in the oil & gas context
- Identify vulnerabilities across IT, OT, and IoT environments
- Apply key standards (e.g., NIST, ISO/IEC 27001, IEC 62443)
- Develop response plans and incident management protocols
- Integrate cybersecurity into digital transformation strategies

Why Attend

Cyber incidents in oil & gas can lead to massive operational downtime, safety risks, financial loss, and reputational damage. This course enables managers to protect sensitive assets, ensure operational continuity, and meet compliance mandates with confidence.

Target Audience

- IT Managers & Cybersecurity Leads
- Plant & Operations Managers
- HSE, Risk & Compliance Officers
- Engineering, SCADA & Control System Managers
- Digital Transformation & Innovation Officers
- Vendor Managers & Project Managers in Tech Initiatives

Individual Benefits

- Gain working knowledge of cybersecurity standards and frameworks
- Learn to lead incident response and resilience planning
- Improve collaboration between IT, OT, and executive leadership

Organizational Benefits

- Prevent disruptions and protect critical operations
- Align cybersecurity with business and regulatory goals
- Reduce vulnerabilities in legacy systems and new tech deployments
- Enhance organizational resilience and cyber maturity

Instructional Methodology

- Expert-led sessions & real-world oil & gas cyber case studies
- Interactive workshops & tabletop simulations
- Group threat-mapping exercises
- Incident response and mitigation planning labs

Course Outline

DETAILED 5-DAY COURSE OUTLINE (CUSTOMIZABLE)

- Training Hours:** 7:30 AM – 3:30 PM
- Daily Format:** 3–4 Learning Modules | Coffee Breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00
- Day 1: Cybersecurity Landscape in Oil & Gas**
- Module 1:** Cyber Threats Targeting the Energy Sector (07:30 – 09:30)
- Module 2:** Attack Vectors – IT, OT, IoT & Cloud (09:45 – 11:15)
- Module 3:** Case Studies – Real Incidents in Oil & Gas (11:30 – 01:00)
- Module 4:** Introduction to Cybersecurity Standards & Risk Frameworks (02:00 – 03:30)
- Day 2: Cyber Risk Management & Governance**
- Module 1:** Risk Identification & Asset Classification (07:30 – 09:30)
- Module 2:** Cyber Risk Assessment Tools (09:45 – 11:15)
- Module 3:** Cyber Governance & Policy Development (11:30 – 01:00)
- Module 4:** Workshop: Creating a Cybersecurity Risk Register (02:00 – 03:30)
- Day 3: IT & OT Security Fundamentals**
- Module 1:** ICS/SCADA System Security Essentials (07:30 – 09:30)
- Module 2:** OT-IT Convergence & Risk Exposure (09:45 – 11:15)
- Module 3:** Network Segmentation, Firewalls & Endpoint Controls (11:30 – 01:00)
- Module 4:** Vulnerability Management and Patch Strategies (02:00 – 03:30)
- Day 4: Incident Response & Cyber Resilience**
- Module 1:** Threat Detection & SIEM Platforms (07:30 – 09:30)
- Module 2:** Developing Incident Response Plans (09:45 – 11:15)
- Module 3:** Business Continuity & Disaster Recovery (11:30 – 01:00)
- Module 4:** Simulation: Cyberattack on an Offshore Facility (02:00 – 03:30)
- Day 5: Compliance, Strategy & Future Trends**
- Module 1:** Global Standards: ISO/IEC 27001, IEC 62443, NIST (07:30 – 09:30)
- Module 2:** Regulatory Requirements (NERC CIP, GDPR, etc.) (09:45 – 11:15)
- Module 3:** Integrating Cybersecurity into Digital Strategy (11:30 – 01:00)
- Module 4:** Final Exercise: Cybersecurity Roadmap for a Gas Terminal (02:00 – 03:30)

Certification

Participants will receive a **Certificate of Completion – IT Security in the Oil & Gas Industry for Managers**, demonstrating their capability to lead cybersecurity initiatives and protect critical digital infrastructure in energy operations.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: +601116373203	EMAIL: info@mawaevents.net
--	---	---

© Material published by MAWA Events 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.