Tel No:+97126654546 | Fax No:+97126654182 | Email: aisha@cmc-me.com | www.cmc-me.com

IT175:

Industrial Cyber Security:

Reducing Cyber Risk, Operating Securely

Training Description:

The threat of Cyber Attacks is widespread and global and it effects individuals, commercial organisations and nation states alike. The ability to safeguard your organization 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.

The training course will highpoint:

- 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 Objectives:

By the end of the training, 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

Training Designed for:

This course is intended for Legal Professionals, System Engineers, Security Administration, Operational Staff and those who have involvement with, and responsibility for operational technology, information technology, & risk assessment.

Training Program:

DAY ONE:

- ❖ Pre-Test

- ❖ 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
- ❖ Course Conclusion
- ❖ Final Examination and EVALUATION

Training Requirement:

"Hand's on practical sessions, equipment and software will be applied during the course if required and as per the client's request."

This training course is available upon request in English or Arabic. Content, location and duration can be adapted to your specific wishes. It is therefore possible to focus on specific modules of the training course

as per client's learning needs and objectives. Further, it should be forwarded to us a month prior to the course dates.

Training Methodology:

This interactive training course includes the following training methodologies as a percentage of the total tuition hours:-

- 30% Lectures, Concepts, Role Play
- 30% Workshops & Work Presentations, Techniques
- 20% Based on Case Studies & Practical Exercises
- 20% Videos, Software & General Discussions
- Pre and Post Test

Training Certificate(s):

Internationally recognized certificate(s) will be issued to each participant who completed the course.

Training Fees:

As per the course location - This rate includes participant's manual, hand-outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Note: The 5% VAT (Value Added Tax), will be effective starting 01st of January 2018 as per the new regulation from the UAE Government. The VAT applies for all quotation both for local and abroad.

Training Timings:

Daily Timings:

07:45 - 08:00	Morning Coffee / Tea
08:00 - 10:00	First Session
10:00 - 10:20	Recess (Coffee/Tea/Snacks)
10:20 - 12:20	Second Session
12:20 - 13:30	Recess (Prayer Break & Lunch)
13:30 - 16:00	Last Session

For training registrations or in-house enquiries, please contact:
aisha@cmc-me.com / training@cmc-me.com
Tel.: +971 2 665 3945 / 643 6653 | Mob.: +971 52 2954615
Training & Career Development Department