P. O. Box. 74693, Dubai, U.A.E.
Tel: +971 4 4571 800
Fax: +971 4 4571 801
E-mail: info@euromatech.com
Web: www.euromatech.com

IT Security Cyber Attack

Introduction

Cybercrime and attacks are becoming more organized and established as a transnational business. High technology online skills are now available for rent to a variety of customers, possibly including nation states, or individuals and groups that could secretly represent a terrorist interest. You need only read the media to appreciate the current state of affairs of incidents which are made public, let alone those which go undisclosed. The increased use of automated attack tools by cybercriminals has overwhelmed some current methodologies used for tracking Internet cyber attacks, and vulnerabilities of a nations critical infrastructure, could possibly attract cyber attacks to extort money, or damage a commercial or national interest.

The threat is widespread and global, and effects individuals, commercial organisations and nation states alike. The ability to safeguard from attacks, identify, analyse and investigate cyber attacks as a security breach is paramount. Digital and related forensic evidence is a complex issue, spanning networks, organisations and international jurisdictions. The ability to effectively identify a security breach, investigate causation and mitigate risk is a must. Furthermore, to effectively detect and deter any cyber attack, you need to understand the nature, motive and ways of perceived cyber terrorists. In doing so and utilising appropriate countermeasures, best practice and management techniques will mitigate the risk of cyber attack and abuse and enhance protection to your assets.

Workshop Objectives

During the two day workshop, delegates will:

- Discover the difference between computer crime and cyber attacks
- Learn how to effectively identify a security breach as a cyber crime
- Review tools and methodologies for reviewing cyber terrorism
- Appreciate different classes of cyber crime
- Understand the nature motive ways of a cyber criminal and terrorist
- Gain familiarity with key legislation and international provisions for cyber terrorism
- Appreciate the effects of cyber terrorism on different organizations/users
- Appreciate Information Security risk assessment and Information Security Management Frameworks
- Realize the importance of inter agency co-operation at a local, national and international level

P. O. Box. 74693, Dubai, U.A.E.
Tel: +971 4 4571 800
Fax: +971 4 4571 801
E-mail: info@euromatech.com
Web: www.euromatech.com

Training Methodology

Participants will gain detailed knowledge by active participation during the workshop, group discussions and real life case studies. Delivery will be by presentation, group syndicate investigations, training DVD and interactive workshops.

WORKSHOP SUMMARY

The workshop will provide delegates with an understanding of the range of cyber attacks that are undertaken today, and their likely evolution. Using real life case studies, delegates will become aware of the nature, motives and ways of a cyber terrorist, and the methods of digital and management prevention strategies and techniques. It will also provide delegates with an overview of key regulations, statutory provisions and the commercial challenges which this brings.

Organisations will be better educated in relation to technology, legal risks and associated obligations in regards to identification of a cyber attack, security breach and appropriate defences that can be considered as a preventative solution. Appreciation and implementation of Information Security Management Framework, can seek to ensure adequate safeguards are implemented to mitigate identified risks of cyber attack or similar.

This in turn will allow organisations to place good reliance on controls which safeguard and utilise data for relevant business processes. Being able to adapt current best practice will ensure that corporations can understand and mitigate legal risks and challenges which are encountered, both nationally and internationally whilst benefitting from leading and effective solutions. Moreover, effective investigation may likely lead to a reduction in investigative lead time and apprehension of a cyber terrorist.

P. O. Box. 74693, Dubai, U.A.E.
Tel: +971 4 4571 800
Fax: +971 4 4571 801
E-mail: info@euromatech.com
Web: www.euromatech.com

Programme outline

Day 1 - Cybercrime Elements

- Overview of Computer Crime and Cyber Crime and Cyber Attack
- Key Elements of Cyber Crime
- Technology, Policing, and Investigation of Electronic Crime
- Ethical Hacking and Cyber Crime
- Civil and Criminal Considerations
- Case Study
-

Day 2 - Criminal Exploits and Vulnerabilities

- Current Trends in Cyber Crime
  - Identity Fraud & Identity Theft
  - Financial Fraud
  - Offences Against the Person
  - Computer Misuse
  - Sexual Offences
  - Intellectual Property
- Responding to Cyber Attack and Vulnerability
- Commercial and Legal considerations.