Combating Cyber Crimes

29th June – 3rd July 2015

TRAINING WORKSHOP OUTLINE

Title:	Combating Cyber Crimes: Technical, Legal and Regulatory Measures
Proposed Dates:	29th June – 3rd July 2015
Duration:	5 days
Venue:	Mutare, Zimbabwe
Fees:	US$1,200 AFRALTI Member States US$1,440 Non-AFRALTI Member States

Course Overview:
Today, the Internet has become an integral part of modern societies with over 2.4 billion users connected in the world. This has in turn created a new realm for malicious users to perpetrate fraud, theft and forgery and transmit illegitimate content just as it happens in the traditional offline setup.

Government agencies, business organisations and individuals are nowadays depending on the Internet to fulfil their obligations and business objectives. With the sophistication cyber attacks, availability of user-friendly attack tools, loopholes in legal frameworks, organised online crimes, vulnerabilities in hardware and software systems, cyber security continues to be the greatest concern.

This intensive 5-day course discusses the safeguards that should be taken to ensure that government agencies, business organisations and end users benefit from the full advantages of Internet. The course also prepares participants for security related certifications like CISA, CISM, CISSP among others.

Target Audience:
This course will significantly benefit ICT professionals who design, build and manage enterprise information security, and anyone who is concerned about the integrity of the cyber world.

Pre-requisite/s:
- Participants should possess at least one year of IT or related experience with additional understanding of critical areas of business operations
- Experienced professionals with 3 years or more experience from the security, risk management, facility, IT security, business operations who have direct or indirect responsibilities are encouraged to attend.

Pain Points:
Information Security management is poised with numerous challenges that deter it from achieving the core objectives namely:
- Authenticity which allows trustful operations by guaranteeing that the handler of information is whoever s/he claims to be.

- Confidentiality which is understood in the sense that only authorized users can access the information, thus avoiding this information being spread among users who do not have the proper rights.
- Availability which refers to being able to access information whenever necessary, thus guaranteeing that the services offered can be used when needed.
- Integrity is the quality which shows that the information has not been modified by third parties, and ensures its correctness and completeness.

Value Proposition:
A new study reveals that boardroom executives are still unaware of cyber threats, much to the chagrin of those working in information security. Information security requires a clear understanding of relevant technological issues and of the social/organisational issues, as well as the relationships between them. This workshop covers these concerns by:

- Offering modules that cover security technologies, incident response and digital investigations, network security implementations as well as information security from a management perspective.
- Providing a curriculum that is relevant to the changing needs of the Information Security industries and professions.
- Adopting the philosophy that security has to be baked in to the business – and not just at a cyber level. Security is a business issue, and has to include how people operate; how information is used (including via telephone, paper and any other way).

Methodology:
Majorly, PowerPoint presentations and case studies are used to partake this instructor-led training. It is made interactive, with lecturer-participants questions to provide as much relevant case studies and practical examples as possible to the domains of practice to the participants.

Workshop Objectives:
The objective of this workshop is to familiarize the participants on the importance of safe and secure online computer and mobile device practices as well as internal policies, to ensure the security of the organization's network infrastructure and information. In addition, the workshop will provide information regarding current and growing threats posed by the proliferation of internal and external individuals, nation states and competitors to the organization's infrastructure.

Expected Outcomes:
Upon completion of this course, participants will be able to:

- Demonstrate how Information systems are penetrated
- Learn security mechanisms used to defend systems against attacks.
- Explain the legal and regulatory and compliance measure to counter Internet crimes

Workshop Contents/Topics:

Module 1: Cyber crimes and threats

- Computer crimes or cybercrimes
- Common cyber crimes
- What is the reach of cybercrimes
- Internet crime reports
- Peer-to-Peer networks
- Smishing and Vishing
- Social networking sites

Module 2: The Need for Cyber Security

- Describe the goals of cyber security.
- Describe the evolution of cyber security.
- Describe the drivers for cyber security.
- Describe cyber attacks types (reconnaissance attacks; access attacks; DOS, DDOS).
- Discuss how cyber crimes are threat to government, public sector; private sector and citizens.
- Describe cyber attacks mitigation.

Module 3: Understanding Cyber Technology

- Describe the cyber world
- Understanding the TCP/IP
- Describing the internet architecture and design
- Describe communication channels
- Describe internetworking components
- Describe cyber applications

Module 4: Information Security Governance and Risk Management

- Identification of an organization's information assets
- development, documentation and implementation of policies, standards, procedures and guidelines
- Information classification/ownership
- Risk management concepts: Asset Identification, Exposures and Countermeasures
- Personnel security
- Security education, training and awareness

Module 5: Mitigating cyber crimes using Applied Cryptography

- Explain how cryptology consists of cryptography (encoding messages) and cryptanalysis (decoding messages) and how these concepts apply to modern day cryptography.
- Explain how securing communications by various cryptographic methods, including encryption, hashing and digital signatures, ensures confidentiality, integrity, authentication and non-repudiation.
- Describe the use and purpose of hashes and digital signatures in providing authentication and integrity.
- Explain how authentication is ensured.
- Explain how integrity is ensured.
- Explain how data confidentiality is ensured using symmetric encryption algorithms and pre-shared keys.
- Explain how data confidentiality is ensured using asymmetric algorithms in a public key infrastructure (PKI) to provide and guarantee digital certificates.

Module 6: Cyber Security Architecture and Design

- Fundamental concepts of security models
- Capabilities of information systems (e.g. memory protection, virtualization)
- Countermeasure principles - design, implement, monitor, and secure, operating systems, equipment, networks and applications
- Vulnerabilities and threats

Module 7: Securing organisation's resources

- Resource protection - the controls over hardware, media and the operators with access privileges to any of these resources.
- Incident response and handling
- Attack prevention and response
- Patch and vulnerability management
- Securing Administrative Access with Authentication, Authorization, Accounting (AAA)
- Multifactor authentication

Module 8: Securing Network Communications

- Describe firewalls
- virtual private network
- Intrusion detection systems and intrusion prevention systems

Module 9: Vulnerability assessment and Audit

- System scanning
- Vulnerability assessments tools vulnerability assessments
- Executing penetration tests
- Review log files and working with syslog servers

Module 10: Business Continuity and Disaster Recovery Planning

- Business impact analysis
- Recovery strategy
- Disaster recovery process
- Provide training

Module 11: Legal, Regulations, Investigations, and Compliance

- Fighting crime using CERTs and Coordination cybersecurity efforts
- National and international coordination
- Issues and Challenges with Cyber Security and Internet Governance
- National Cybersecurity Policy: Balancing Risk and Innovation
- Network Disaster Recovery
- Cyber crimes laws and regulations
- Cyber crimes investigations – gathering evidence to determine whether a crime has been committed.
- Computer forensic procedures
- Admissible evidence - compliance requirements/procedures

POTRAZ

Ms. Norah Zaranyika,
Public Affairs Officer,
Email: zaranyika@potraz.gov.zw
Tel: +263 712 871 341

AFRALTI

Mr. Jonathan P. Mwakijele,
Head of Training, Consultancy and Research Unit
Email: training@afralti.org
Tel: +254 20 265 5011,
+254 710 207 061