



**THE KENYA INSTITUTE OF MANAGEMENT**

P.O. Box 43706-00100 Nairobi, Kenya

Tel: +254 - 20-2445600

Mobile: +254 - 722-956289

email: [mkaburu@kim.ac.ke](mailto:mkaburu@kim.ac.ke)

website: [www.kim.ac.ke](http://www.kim.ac.ke)

## **Information Security: Protecting the Global Enterprise (Workshop)**

Date: February 23-24, 2010

Venue: Sarova PanAfric Hotel, Nairobi

### **Introduction**

Information is one of organisation's most important assets. Protection of information assets is necessary to establish and maintain trust between the organisation and its customers, maintain compliance with the law, and protect the reputation of the organisation. Timely and reliable information is necessary to process transactions and support organisation and customer decisions. An organisation's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed. Its value can be optimally achieved by managing risk investments.

### **Definition**

Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintains information vital to its operations. On a broad scale, an organisation has a primary role in protecting information services infrastructure. The security of the organization's systems and information is essential to its safety and soundness and to the privacy of customer information. The security program must have strong board and senior management level support, integration of security activities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities.

### **Objectives**

The objectives of this workshop will be to:

- Identify the importance of information to organisation and society in general.
- Describe and apply concepts, principles and techniques relating to the security of information.
- Describe and apply classification systems for information.
- Outline the ethical and legal issues associated with information security and analyse their implications.
- Demonstrate an understanding of the advantages, disadvantages, threats and vulnerabilities associated with various IT environments.
- Describe the role of risk analysis and contingency planning in information security.
- To protect the organisation's business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability.

Luther Plaza, 2<sup>nd</sup> Floor  
Uhuru Highway/ Nyerere Road Junction

- To establish safeguards to protect the organisation's information resources from theft, abuse, misuse and any form of damage.
- To establish responsibility and accountability for Information Security in the organisation.
- To encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Security incidents.
- To ensure that the organisation is able to continue its commercial activities in the event of significant Information Security incidents.
- To enable the participants to do their organisations' information security self assessment.

### **Course Contents**

1. Information security objectives
2. Information security concepts, principles and techniques.
3. Information assets and threats
4. Information risk analysis
5. Data protection, privacy, and copyright acts and laws
6. Information management
7. Use of Internet as an information resource
8. Document security
9. Monitoring security and information flow
10. Logical protection of systems
11. Incident handling and best practices
12. New business information security self assessing and mitigating techniques.

### **Target Group**

1. CEO's
2. ICT Managers
3. Finance Managers
4. Bank Managers
5. Human Resource Managers
6. Auditors
7. Information Officers
8. Information Systems Managers
9. Information Systems Auditors
10. Records Officers
11. Company Secretaries
12. Information Security Officers

## **Workshop Schedule**

### **Day 1**

8:30-10:00 a.m. Global Threats to Information & Telecommunication Systems

10:00-10:15 a.m. **Break**

10:15-12:00 p.m. Wireless Internet Security

12:00-1:00 p.m. **Lunch Break**

1:00-2:30 p.m. Online Fraud and Risk Management

2:30-2:45 p.m. **Break**

2:45-4:30 p.m. Incident Handling, Business Continuity & Disaster Recovery Plan

4:30-5:00 p.m. **Questions & Answers**

### **Day 2**

8:30-10:00 a.m. Assessing Risk: Conducting Vulnerability Assessment

10:00-10:15 a.m. **Break**

10:15-12:00 p.m. Developing a High Impact Security Management Strategy

12:00-1:00 p.m. **Lunch Break**

1:00-2:30 p.m. Best Practices for Implementing a Business Centric Security Management Strategy

2:30-2:45 p.m. **Break**

2:45-4:30 p.m. Information Security Policies, Standards & Procedures

4:30-5:00 p.m. **Plenary Session & Issuing of Certificates**

## Agenda Summary:

- ❖ Global Threats to Information & Telecommunication Systems
  - ✓ Online Identity Theft
  - ✓ Spyware, Malware and Key loggers
  - ✓ Botnets
  - ✓ Click Fraud
  - ✓ Cyber terrorism
  - ✓ Web 2.0 Applications -Social Networks
  - ✓ Mobile devices – iphones, blackberries e.t.c.
  - ✓ Blended wireless devices – wi-fi, 3G & 4G
  - ✓ Virtualisation
  - ✓ Cloud Computing
- ❖ Best Practices for Implementing a Business Centric Security Management Strategy
  - ✓ Protecting Critical Servers
  - ✓ Protecting Mobile Devices and Communication
  - ✓ Network Defenses
  - ✓ Security Awareness
- ❖ Information Security Policies, Standards & Procedures
- ❖ Wireless Internet Security
  - ✓ Rogue wireless access points
  - ✓ Distributed Denial of Service (DDOS)
  - ✓ Arp Poisoning
  - ✓ Man in the Middle (MITM)
- ❖ Online Fraud and Risk Management
- ❖ Incident Handling, Business Continuity & Disaster Recovery Plan
  - ✓ What is an incident?
  - ✓ How to handle an Incident
  - ✓ BCP Process
  - ✓ Business Impact Analysis (BIA)
  - ✓ Recovery Strategy
- ❖ Assessing Risk: Conducting Vulnerability Assessment
- ❖ Developing a High Impact Security Management Strategy
  - ✓ Data encryption
  - ✓ Firewalls
  - ✓ Hardening OS
  - ✓ Patching
  - ✓ Access Control

**Cost:** Ksh. 25,000 inclusive of V.A.T.

### Registration Information:

Call Mercy: 020-244600,020-2445555,0722-956289

### Presented By:



**THE KENYA INSTITUTE OF MANAGEMENT**



Luther Plaza, 2<sup>nd</sup> Floor  
Uhuru Highway/ Nyerere Road Junction

## **Workshop Presenters Profile**

### **Evans Kahuthu, Bsc, MBA, MCP, MCTS**

Mr. Kahuthu is a Web and Database application developer and Information Security Specialist with over 10 years experience in the IT industry.

From 2001 until June 2009, he worked as the Web and Application Development coordinator at the California State University, San Bernardino where he was in charge of over 150 websites and database applications.

Security and accessibility of these applications was his core job function.

In addition, he was a member of the IT team that was tasked with Security Awareness and Training. This team was the author of the Web Security Policies for the California State University.

Between September 2006 and December 2008, he was a part time Lecturer at the California State University, San Bernardino College of Business and Public Administration where he taught database management, security, administration and e-commerce.

Currently, Mr. Kahuthu is a research associate with the Inland Commerce and Security Institute at California State University, San Bernardino. He is also the Chief Technologist at Teqlink Solutions LTD which is a full service internet/web design/Information Technology security consulting company with offices in California, USA and Nairobi, Kenya.

Mr. Kahuthu is a member of Information Systems Audit and Control Association (ISACA) serving IT governance professionals, the Open Web Application Security Project (OWASP) a consortium of international web application security developers. He is also a contributor at the Hacked Africa Zone website which reports hacked websites in Africa.

### **Gichuki John Ndirangu, CEH, CPTP, OSCP**

Mr. Gichuki is an IT Security and Forensic analyst whose expertise includes network penetration testing, computer vulnerabilities, attack scripts and exploits among others.

Mr. Gichuki has consulted with both the private and government sector including but not limited to the Kenya police, CID and the Department of Defense.

He is a Security and exploit Researcher for Milw0rm Security a non -Profitable organization. He has over 6 years experience in IT Security environments. He has undertaken projects cutting across a number of sectors including Financial, Manufacturing, Hospitality, Government and agriculture.

He has attained several certifications and enough experience in the security field. The following are the IT Security Certifications. CEH- Certified Ethical Hacker, CPTP- Certified Penetration Testing Profession, Security +, SANS Web application Security Pentester. Recently did and passed, Offensive Security Certification Profession. OSCP.

Luther Plaza, 2<sup>nd</sup> Floor  
Uhuru Highway/ Nyerere Road Junction

Mr. Gichuki has worked with Kenya Police, on Cyber investigations under Inspector Kisavi now in Special Operations, Vigilante House. Also worked under Inspector Mboya on several other cases that involved CCU.

He has also worked with the Kenya Anti-Corruption Commission (KACC) where his duties included but not limited to, breaking into targeted emails, Information Gathering of targets, phone bugging and tracking Systems, email tracing, Forensics Presentations in Court as a special witness. Forensics Gathering and backing up of the Forensics database and Equipments

In addition he also worked with the Department of Defence, Kenya-DOD where he was in charge of training users on how to use Linux and UNIX operating Systems and help them to migrate from Microsoft Windows to the world of Open-Source and also training users on CEH certification.

Mr. Gichuki has been working with Teqlink Solutions in training, assessing, analyzing and mitigating risks for organizations and employees. He is also a contributor at the Hacked Africa Zone website which reports hacked websites in Africa.

### **Resource Profile**

The following people will provide course content, material support to be used during the workshop.

#### **Javier Torner, Ph. D.**

Dr. Javier Torner is the University Information Security Officer at California State University San Bernardino. Dr. Torner is the Director of the Information Security Office which coordinates and oversees the implementation of enterprise information security initiatives and measures for the university's telecommunications network and computer and information systems.

Under his direction the Information Security Office provides, among others, guidance in conducting risk and vulnerability assessments for information systems, manages the intrusion detection and incident response capabilities of the campus, and conducts computer forensics investigation.

Dr. Torner periodically conduct workshops and presentations on information security topics to different groups inside and outside the university, including upper management, IT directors, and technical staff groups .

Dr. Torner is currently the President for the Information System Security Association Inland Empire Chapter. Dr. Torner is a Professor of Physics with over twenty years of teaching and working experience with data communication networks and computer systems.

#### **C. E. Tapie Rohm Jr., Ph.D., F.I.I.M.A.**

Dr. C. E. Tapie Rohm Jr. is a very unusual person. He is a nationally and internationally recognized scholar, educator, consultant, author, entrepreneur and businessman. He has consulted for such large firms as IBM, Westinghouse, Mead, Gannett to numerous medium and small/entrepreneurial

Luther Plaza, 2<sup>nd</sup> Floor  
Uhuru Highway/ Nyerere Road Junction

businesses. He has been a consultant to governmental agencies like the State of California-Department of Justice, the Federal Highways Department, the US Department of Defense, the Islamic Nation of Pakistan, the People's Republic of China, the Republic of Tanzania (East Africa), Kuwait. He has lectured in the countries of Egypt, Turkey, England, Ireland, Scotland, Sweden, Ecuador, and Republic of China (Taiwan). He has sat on various advisory boards for such corporations as WordPerfect, Expertillegents, Hearthstone Institute and the like. He has been a CIO, CFO and CEO for various businesses.

Dr. Rohm has taught for the past two decades at various educational institutions. He is currently a professor of Information and Decision Sciences at California State University San Bernardino. He is an Honorary Professor at the Hebei Academy for Social Sciences in the PRC. He is a former Fulbright Scholar to Tanzania, East Africa. He is one of the founding Executive co-Directors of the Inland Commerce and Security Institute and former Executive co- Director of the Empire Center for Entrepreneurship (which became ranked fourth nationally for graduate program under his leadership at California State University San Bernardino).

He is an Editor-in-Chief of two journals: ***Journal of International Technology and Information Management*** and ***Communications of the IIMA***. He has been honored as a Fellow in the International Information Management Association. He has authored or co-authored numerous journal articles. He is one of the founders of the International Information Management Association. He has obtained many grants. He is on a number of Editorial Review Boards (ERB).

#### **Conrad Shayo Ph.D.**

Conrad Shayo is a Professor of Information Science at California State University San Bernardino. Over the last 28 years he has worked in various capacities as a university professor, consultant, and manager. He holds a Doctor of Philosophy Degree and a Master of Science Degree in Information Science from the Claremont Graduate University. He also holds an MBA in Management Science from the University of Nairobi, Kenya; and a Bachelor of Commerce Degree in Finance from the University of Dar-Es-Salaam, Tanzania. He has consulted for the World Bank, Swiss Agency for Development Corporation, and the US Government. His research interests are in the areas of IT assimilation, performance measurement, distributed learning, end-user computing, organizational memory, instructional design, organizational learning assessment, reusable learning objects, IT strategy, and "virtual societies." Dr. Shayo has published these and other topics in various books and journals. Currently he is involved in developing reusable learning objects and web based learning game simulations. He is also consulting in the areas of tourism promotion, joint ventures, and poverty eradication in developing countries. He is a Co-Editor (with Dr. Magid Igbaria) of the book: *Strategies for Managing IS/IT Personnel*.