Certificate in

Cyber Security

Offered as a partnership between Cape Peninsula University of Technology (CPUT), French South African Institute of Technology (F'SATI) and CS Interactive Training

"Ex-Israeli agents' threatened cyber attack on South Africa"

"Spy Cables expose South Africa's alarming security failings"

These are just some of the headings around the globe today as spy documents are released on sites such as www.aljazeera.com and www.theguardian.com/uk

The documents highlight (amongst others) the current lack of adequate cyber security policies and effective security governance frameworks as well as the failure to implement suitable technologies and controls, especially within the government sectors. Of more concern is the mentioned shortage of skilled cyber security people in key positions as well as a shortage of adequate training programs. Security awareness amongst general employees is problematic and basic to advanced cyber security training programs are not efficient.

Cyber security is not just a buzz word, but rather encapsulates proper understanding of security threats and vulnerabilities, design and implementation of effective controls, cyber-criminology and warfare, detailed risk management and effective security governance across all spheres of the business.

The Certificate in Cyber Security developed and offered as a partnership between academia and industry, is a step to build capacity in cyber security and to address the shortages in focused training opportunities for corporate staff.

Target Market

Security personnel working within the spheres of information and computer security as well as prospective students that want to embark on a career within the cyber security domain.

Entrance qualification

Matric certificate or equivalent qualification with a minimum of 50% for Mathematics.

Experience within the information security industry will be beneficial. Attendees must have Internet access and suitable computing hardware and software in order to participate on the e-learning forums and complete practical assignments.

Structure of the course

The course consists of four modules. Each of the modules is presented by way of two days contact (face-to-face) sessions followed by a 2-3 week e-learning period. A student has to pass all four modules with a minimum mark of 70% in order to successfully complete the course and receive the certificate in Cyber Security.

Next Offering (2015)

Pretoria/Centurion region:

Module 1: 9 & 10 April (9h00-15h30) followed by a three week e-learning period.

Module 2: 7 & 8 May (9h00-15h00) followed by a three week e-learning period.

Module 3: 4 & 5 June (9h00-15h30) followed by a three week e-learning period.

Module 4: 2 & 3 July (9h00-15h30) followed by a three week e-learning period.

Cape Town (Bellville):

Module 1: 13, 14 & 15 April (8h30-13h30) followed by a three week e-learning period.

Module 2: 18, 19 & 20 May (8h30-13h30) followed by a three week e-learning period.

Module 3: 17, 18 & 19 June (8h30-13h30) followed by a three week e-learning period.

Module 4: 13 & 14 July (9h00-15h30) followed by a three week e-learning period.

Core Syllabus

MODULE 1: COMPUTER SYSTEMS AND THE SECURITY ENVIRONMENT

Introduction to Information Security

- Codes, ciphers & secrets
- Security principles & environment
- Cyber criminology
- Cyber warfare

Threat environment

- Security awareness
- Information warfare
- Social engineering
- Malicious code (i.e. botnets, malware)
- Introduction to the attack process
- Introduction to attack vectors
- Social networks (i.e. attacks via facebook, twitter, etc.)

Computer Systems Essentials

- Introduction to operating systems
- Networking & communication essentials
- Internet & Web essentials
- File management & database systems
- Application software
- Secure software design & testing

MODULE 2: ANALYSIS, TECHNICAL WRITING & CRYPTOGRAPHY

Elementary Encryption

- Encryption & Decryption
- Substitution ciphers
- Transpositions
- Symmetric & asymmetric encryption
- Stream & block ciphers
- Confusion & diffusion
- Data Encryption Standard (DES)
- AES Encryption Standard
- Public Key encryption: RSA
- Hash functions
- Practical applications of encryption (i.e. Bitcoins)
- Digital signatures
- Digital certificates

Cryptanalysis & Control

- Breaking encryption schemes
- Tools & controls

Analysis & Technical Writing

- Security information analysis & synthesis
- Technical report writing

MODULE 3: TECHNICAL SECURITY

Program Security

- Flaws & fixing faults
- Program errors
- Targeted malicious code
- Controls against program threats

Operating System Security

- Operating system flaws
- Memory and address protection
- Control access
- File protection
- User authentication
- Open source systems

Network & Internet Security (6 hours)

- Network threats
- Controls
- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Email security
- Web security

MODULE 4: SECURITY GOVERNANCE

Laws, Rules & Regulations

- Local and International
- Rights of employees and employers
- Computer crime
- Privacy
- Ethical issues & case studies

Security Policies, Plans & Procedures

- Military & commercial policies
- Policies in action
- Security models
- Security plans & procedures
- Security evaluation

Security Design & Management

- Planning for security
- Planning for contingencies
- Developing the security program
- Security management models and practices
- Risk analysis & management
- Identifying & assessing risks
- Accessing & controlling risks
- Protection mechanisms

NQF Level

NQF Level 5

Open Badges

A digital badge is an online representation of a skill earned. Open Badges is a new online standard to recognize and verify learning.
Badges as per industry certification will be issued after successful completion of the certificate.

Presenters

Prof. Elmarie Biermann will be the main facilitator. She holds a PhD in Computer Security from the University of South Africa and boasts experience in security consulting, training, research as well as the development of security content in both industry and academia. She published a large number of academic and industry papers and is currently involved in the management of several security companies.

Partners

Cape Peninsula University of Technology (CPUT) is a leading University of Technology that provides a wide range of qualifications within the Western Cape. CPUT is a public higher education institution, established in terms of its own statute and the Higher Education Act and an accredited training provider within the ETDP-SETA.

The French South African Institute of Technology (F'SATI) offers international Master of Science and Doctorate programmes in Electronic Engineering in collaboration with ESIEE-Paris, a graduate school in electronic engineering in France.

CS Interactive Training provides training and support to teams of business and ICT professionals that are responsible for systems and business change management initiatives within organisations. Their goal is to enable organisations to build core competencies that enable the managing of change more effectively and reduce complexity within core processes and systems.

Course fee

R 19 400

Apply Today

For more information and application forms, please contact:

Prof. Elmarie Biermann
elmarie@infobahn.co / elmarie@acm.org