Cyber skills

Defining the Skills-base for the Future

Professor Bill Buchanan
CSI (Computer Security Institute) found:
- 70% of organisations had breaches
- 60% of all breaches came from inside their own systems

Corporate access

Data stealing

External hack

DoS (Denial-of-service)

Personal abuse

Worms/viruses

Terrorism/extortion

Fraud

Network/Organisational perimeter

Fundamentals

Introduction

Intrusion Detection

Users

Systems

Data

Assets

Firewall/Gateway
(cannot deal with internal threats)

Outside and inside threats

Author: Prof Bill Buchanan
Aging population.  
Climate Change.  
Transport and mobility issues.  
Failure to Innovate.  
Old methods of governance.  

Better Society

Excellent science

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.

Cyber infrastructure

Funding will be focussed on the following challenges:

- Health, demographic change and wellbeing;
- Food security, sustainable agriculture, marine and maritime research, and the bio-economy;
- Secure, clean and efficient energy;
- Smart, green and integrated transport;
- Inclusive, innovative and secure societies;
- Climate action, resource efficiency and raw materials

Competitive Industries

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.
Cyber skills

Defining the Skills-base for the Future

Focusing on Risks, Threats and Vulnerabilities ...
“Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each puts risk into a different context ... different vocabularies, definitions, metrics, processes and standards ... “ Woloch (2006)
Cyber skills

Defining the Skills-base for the Future

The Skills Road Map
- Intrusion Detection.
- Access Control.
- System Development and Maintenance.
- Security Policy Implementation.

- Access Control.
- Data Leakage.
- Auditing.
- Asset Classification and Control.
- Data Infrastructure.

- Risk Management.
- Business Continuity.
- Physical and Environment Security
- Human Resource Security
- Incident Management.
- Security Policy Definition.

- Ethical responsibility.
- Legal infrastructure.
- Compliance.
# Insiders

## Digital Investigator
- Disk Forensics.
- Phone forensics.
- Network forensics.
- Criminal Analysis.
- Social Networks.

## Real-time Defence/Critical Response
- Response Units

## Proactive Defence
- Firewalls
- Intrusion Detection.
- Server/Network infrastructure

## Homeland Defence
- Terrorism.
- Society threats

## Security Maintenance

## Security Evaluation

## Business Crime Investigator
- Accounting Forensics.
- Fraud analysis.

## Audit/Compliance
- ISO 27001.
- PCI.
- HIPPA.

## Risk Analysis/Brand Awareness/Data Leakage

---

**Governance/Judicial Infrastructure**
Cyber skills

Defining the Skills-base for the Future

Engaging Students
Part-time/Full-time mode

Distance/Blended Learners

MPhil/PhD

MSc level Security/Digital Forensics Dissertation (1x60 credits)

CISSP

EnCase

CEH

Cisco

Microsoft

Four Year Undergraduate Degree

Work-based Learning

60 credits

Defining standards:
- Academia.
- Scottish Police.
- SMEs.
- Large industry.
- Professional Bodies.
- Public sector.
- Etc.
Private Cloud – owned and run by an organisation

Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc

Public Cloud – owned by an organisation selling a cloud infrastructure

Hybrid Cloud – two or more clouds
On-demand self-service. Consumers get server CPU, memory, bandwidth and storage resources whenever required.

Rapid elasticity. Consumers can easily scale-up and scale-down, whenever required.

Location independent resource pooling. Multiple customers use shared resources within the provider, without actually knowing where the exact location of these are.

Pay per use. All access to resources is monitored, and paid for either by advertising or usage. Payment methods: per users created, per hour usage (service), etc.
Public Sector
- Evaluation of systems.
- Training.

Industry
- Training/sharing materials.
- Professional certification

Government
- Define standards
- Evaluate products

Academia
- Training/sharing materials
- Virtualised environments

Software Vendors:
- Test environments.
- Promoting products.
- Providing floating licences

Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc.

Existing Academic Clouds

Public clouds
Distance learners
- Exact environments as face-to-face students.
- Blended learners have greater choice and flexibility.

Enhancing skills
- Supports a wide range of pre-built environments within a sandboxed infrastructure.

Working across institutions
- Cloud environments allow for working across traditional boundaries.

Project work
- Students can start from existing well-tested environments.

Engaging students
- State-of-the-art infrastructures

Group working
- Students can integrate their systems in an isolated environment.

Robust infrastructures
- No more 9-5pm, Mon-Friday environments.

Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc

Industry
- Adding evaluation infrastructures.
- Post project work/interesting areas of work.
- Ability to review materials presented to students.
- Ability to study within the workplace.

Continuation of work
- Students can carry their infrastructures throughout modules/years.

Snap-shots of work
- Student can create snapshot, and move back and forward amongst them.
Difficult to use many of the techniques within a real-life space

Virtual spaces allow for a more complex and deeper understand of how to secure infrastructures

Demands on professional certification

Employers now require in-depth knowledge and a range of skills
Tool validation:
- Supports a wide range of tool validation.
- Ever changing environment for a range of testing.

Skills:
- Allows students to remotely complete labs.
- Students training on state-of-the-art infrastructures.
- Different labs can be created for different situations (DF Tools/OSs/etc).
- Supports remote/distance learning.
- Infrastructure can be ring-fenced.
- Supports group work in an isolated environment.
- In-depth analysis of infrastructures.
- Students can build systems from scratch.
- Students can update their own infrastructure/tools, as required.
- Seems to engage the students, and show them a wide potential.
- Encourages students to continue work after the lab/tutorial.
- Time windows of labs/tutorials can be carefully controlled.
- Extensive and complex infrastructures assessed within a sandboxed environments.

Drawbacks:
- Requires an investment in time in creating and maintaining the virtual image.
- Students can avoid the lab situation.
- Possibly requires a backup strategy for labs (if using network-based virtualisation – but has advantages that a standalone version does not need a network connection).
- Goes against the stand-alone machine philosophy.

Other advantages:
- Easy for teaching team to update.
- Helps with franchised colleges.
- Easy setup for classroom demonstrations.
- Infrastructure can be ring-fenced.
- Produces repeatable labs.
- Not dependent on Napier/network infrastructure.
- Time windows of labs/tutorials can be carefully controlled.
Cyber infrastructure

Better Society

- Aging population.
- Climate Change.
- Transport and mobility issues.
- Failure to Innovate.
- Old methods of governance.

Excellent science

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.

Competitive Industries

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.

Funding will be focussed on the following challenges:

- Health, demographic change and wellbeing;
- Food security, sustainable agriculture, marine and maritime research, and the bio-economy;
- Secure, clean and efficient energy;
- Smart, green and integrated transport;
- Inclusive, innovative and secure societies;
- Climate action, resource efficiency and raw materials
Cyber skills

Defining the Skills-base for the Future

Professor Bill Buchanan