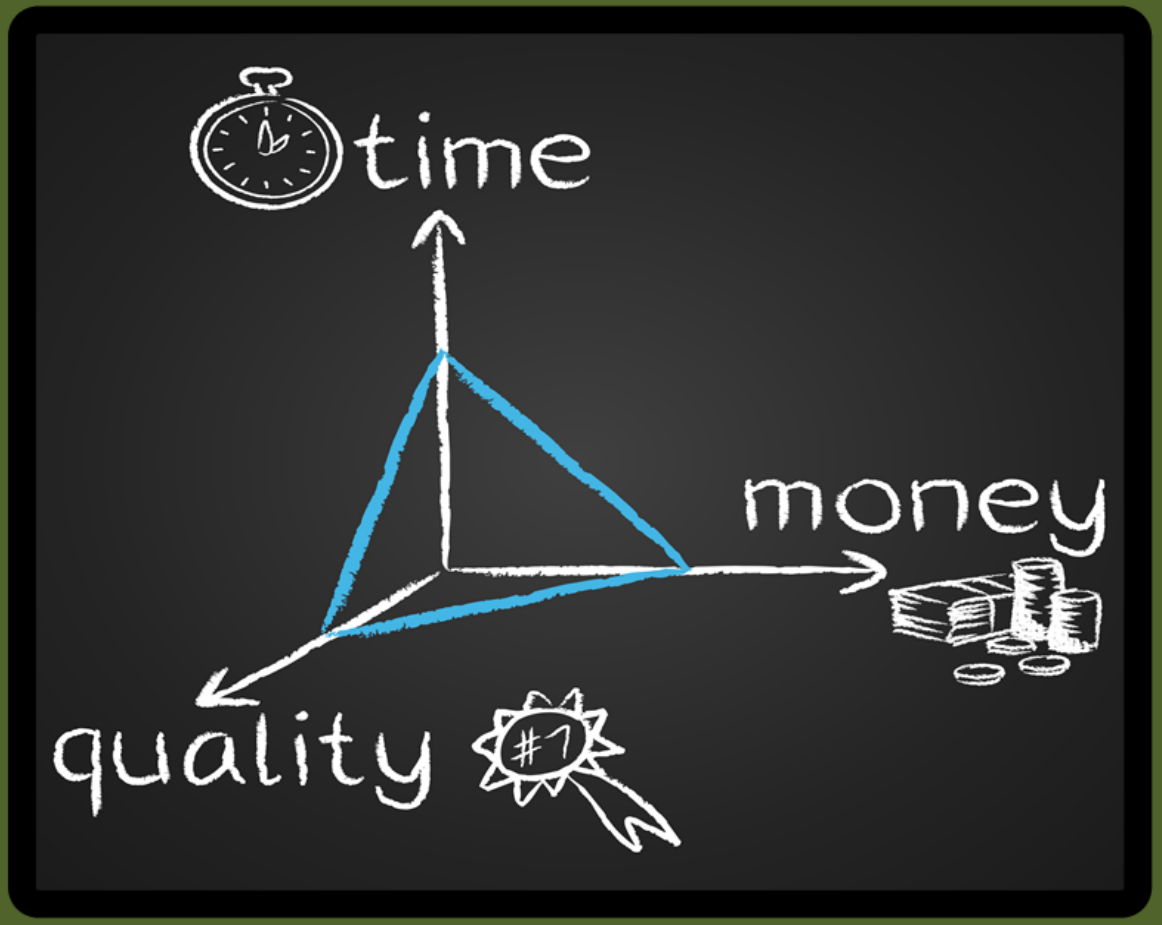
Cyber Skills




# Cyber Skills and Training

Prof Bill Buchanan

## Understanding Risk


What is … a threat … a risk … a vulnerability … the motivation?

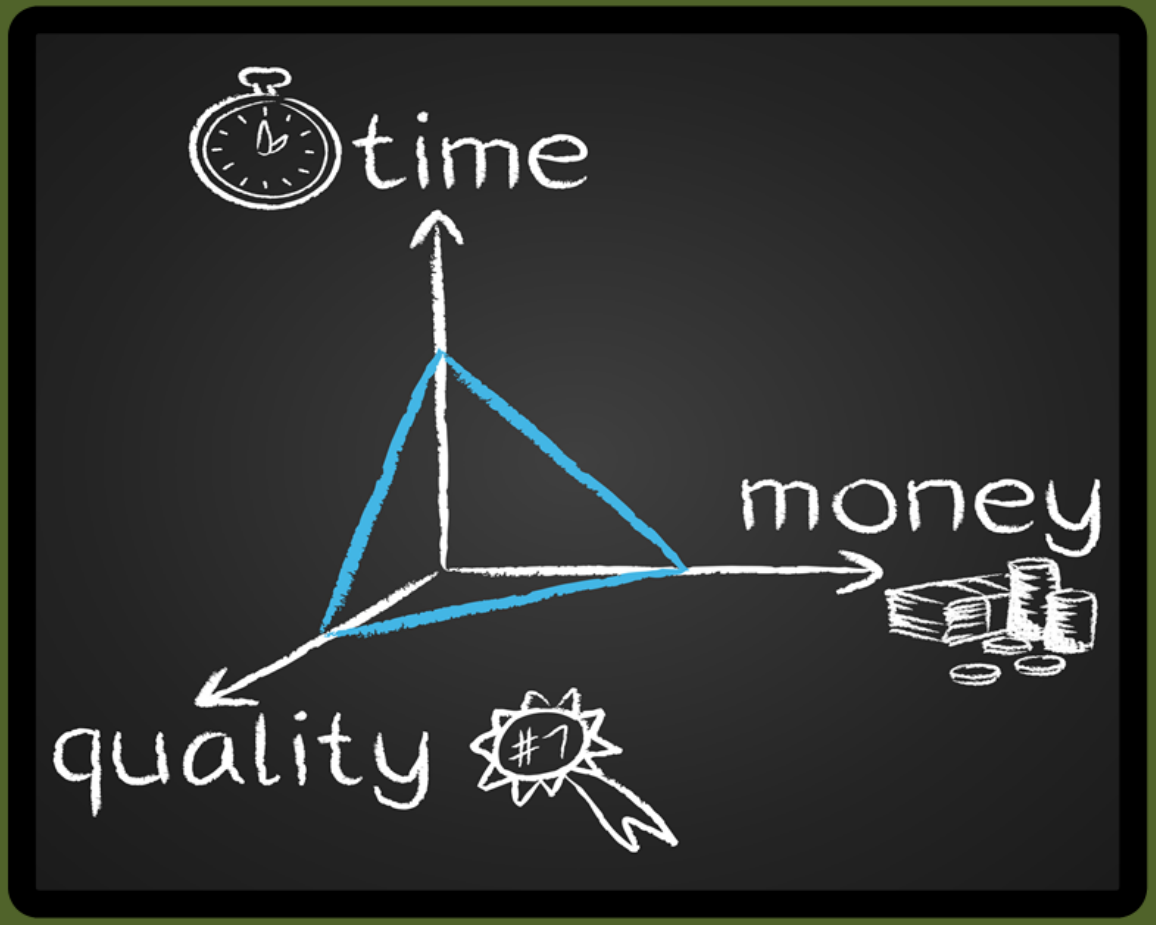
- Wide range of threats to organisations.
- Organisations now highly dependent on their information infrastructure.
- Real-time threat analysis needed to cope with threats.


Risks

New Threats?

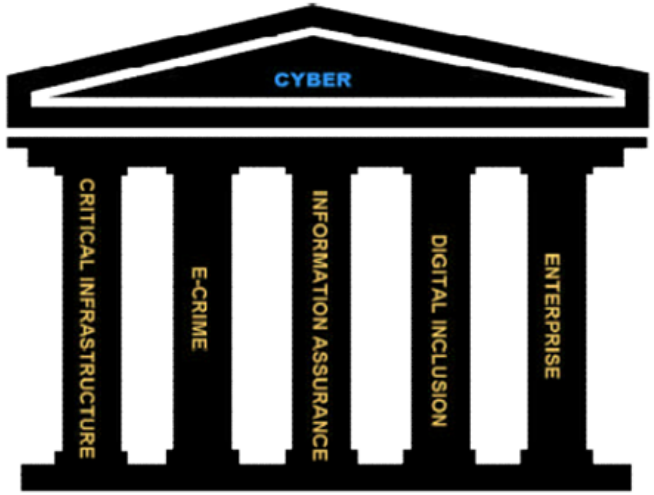
Risks … threats … vulnerabilities

Cyber Skills




# Background

Prof Bill Buchanan




Ministerial Submission.pdf - Adobe Reader

File Edit View Window Help

5 / 6 76.1% Tools Sign Comment

monies to be spent in Scotland.

- Use BIS and CPNI criteria for key businesses and apply these to the Scottish economy, to then ensure that necessary processes and procedures are in place to enhance cyber security.

Additional recommendations, contingent on clarification of UK government funding:

- The Directorate for Employability, Skills and Learning, the Directorate for Business, and Scottish Enterprise to build links with BIS and M15 to capitalise on opportunities for Scotland-based/owned businesses and research facilities to deliver cyber security products and services.
- The Directorate for Employability, Skills and Learning, the Directorate for Business, and Scottish Enterprise to explore opportunities for Scotland based/owned businesses and research facilities in the mainstreaming of cyber security throughout the Ministry of Defence.
- The Directorate for Employability, Skills and Learning should consider SCDEA's DCI Wilson's and the universities' work on developing a centre of excellence in national cyber security skills, and also contact Bill Buchanan of Edinburgh Napier University, as a Scottish component of improving national cyber security skills.
- The Directorate for Learning should seek to ensure appropriate amends to Get Safe Online, to add more Scotland-specific links in the teachers, pupils and curriculum area.
- The Directorate for Employability, Skills and Learning should encourage Scottish universities to seek involvement in the Cyber Security Challenge.
- The Directorate for Employability, Skills and Learning, the Directorate for Business, the Directorate for the Office of the Chief Scientific Adviser, and Scottish Enterprise should ensure that Scotland is at the forefront for gaining UK Government research sponsorship into cyber security challenges.

cyber_green_paper.pdf - Adobe Reader

File Edit View Window Help

1 / 21 65.1% Tools Sign Comment

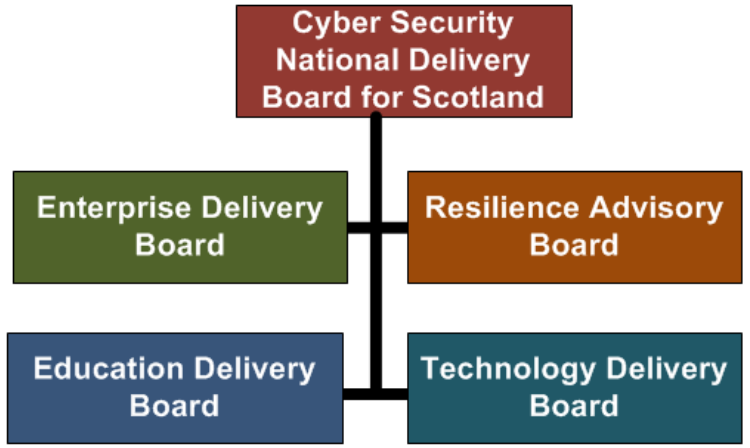
The file you have opened complies with the PDF/A standard and has been opened read-only to prevent modification.

**A Strategic Proposition**

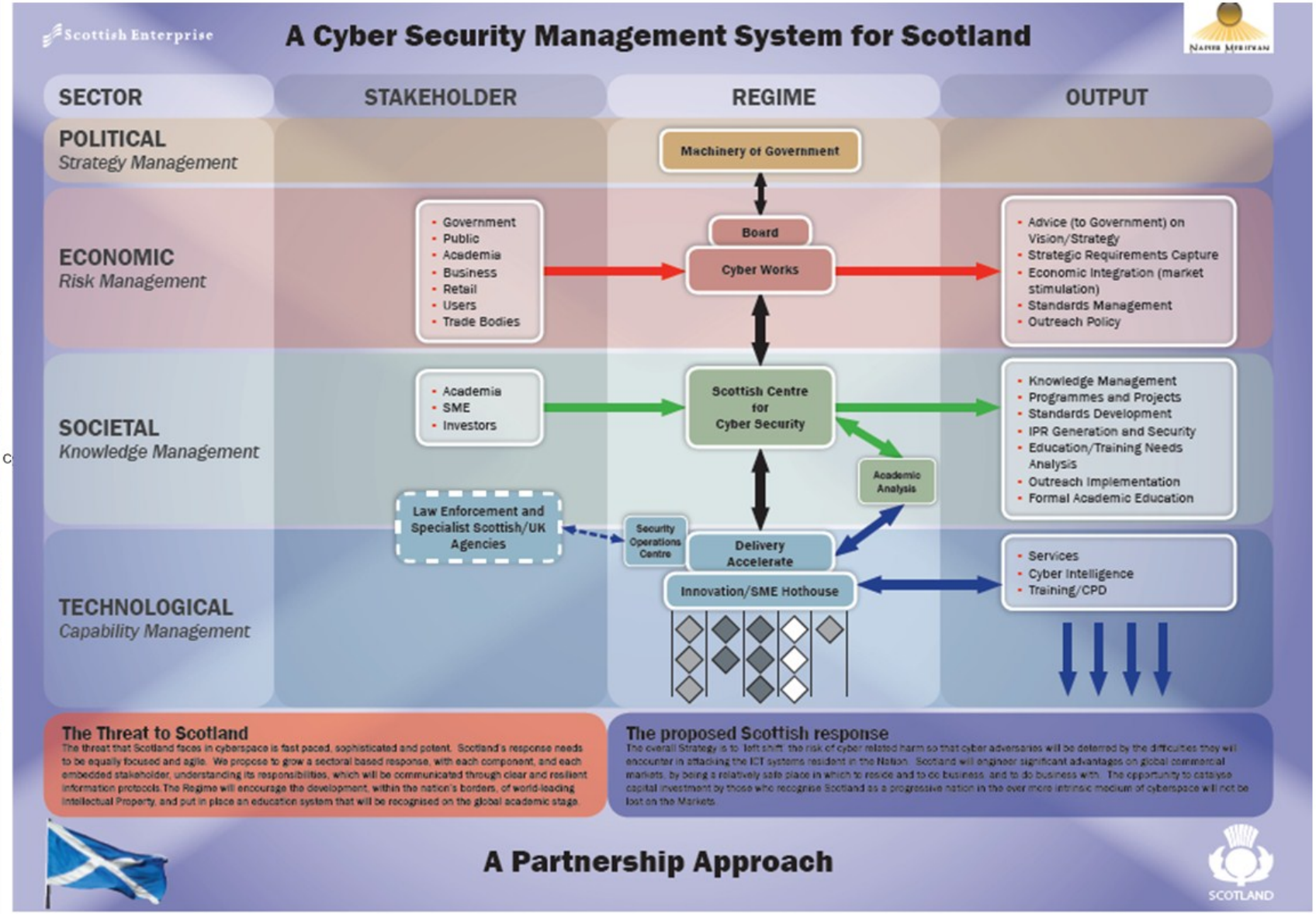
for

**Cyber Security in Scotland**

*April 2012*




Cyber


Scottish Enterprise
A Cyber Security Management System for Scotland
SECTOR
STAKEHOLDER
REGIME
OUTPUT
POLITICAL
Strategy Management
ECONOMIC
Risk Management
SOCIETAL
Knowledge Management
TECHNOLOGICAL
Capability Management
Machinery of Government
Board
Cyber Works
Government
Public
Academia
Business
Retail
Users
Trade Bodies
Advice (to Government) on Vision/Strategy
Strategic Requirements Capture
Economic Integration (market stimulation)
Standards Management
Outreach Policy
Academia
SME
Investors
Scottish Centre for Cyber Security
Knowledge Management
Programmes and Projects
Standards Development
IPR Generation and Security
Education/Training Needs Analysis
Outreach Implementation
Formal Academic Education
Academic Analysis
Law Enforcement and Specialist Scottish/UK Agencies
Security Operations Centre
Delivery Accelerate
Innovation/SME Hothouse
Services
Cyber Intelligence
Training/CPD
The Threat to Scotland
The threat that Scotland faces in cyberspace is fast paced, sophisticated and potent. Scotland's response needs to be equally focused and agile. We propose to grow a sectoral based response, with each component, and each embedded stakeholder, understanding its responsibilities, which will be communicated through clear and resilient information protocols. The Regime will encourage the development, within the nation's borders, of world-leading Intellectual Property, and put in place an education system that will be recognised on the global academic stage.
The proposed Scottish response
The overall Strategy is to 'left shift' the risk of cyber related harm so that cyber adversaries will be deterred by the difficulties they will encounter in attacking the ICT systems resident in the Nation. Scotland will engineer significant advantages on global commercial markets, by being a relatively safe place in which to reside and to do business, and to do business with. The opportunity to catalyse capital investment by those who recognise Scotland as a progressive nation in the ever more intrinsic medium of cyberspace will not be lost on the Markets.
A Partnership Approach
SCOTLAND

Cyber Security in Scotland

Cyber

Ministerial Lead

**Fergus Ewing**
Minister for Energy Enterprise and Tourism as the ministerial lead for Cyber Security in Scotland.

**Cyber Security National Delivery Board for Scotland**
**Chair:** Scottish Govt Director-General
**Membership**
Scottish Govt Cyber Lead
Scottish Govt CNI rep
Scottish Govt Enterprise rep
Scottish Govt Education rep
Scottish Govt Digital Inclusion rep
Enterprise Delivery Champion
Education Delivery Champion
Technology Delivery Champion
Crime Enforcement Rep
Information Assurance Rep
Senior Industry Rep
Senior Academic Rep

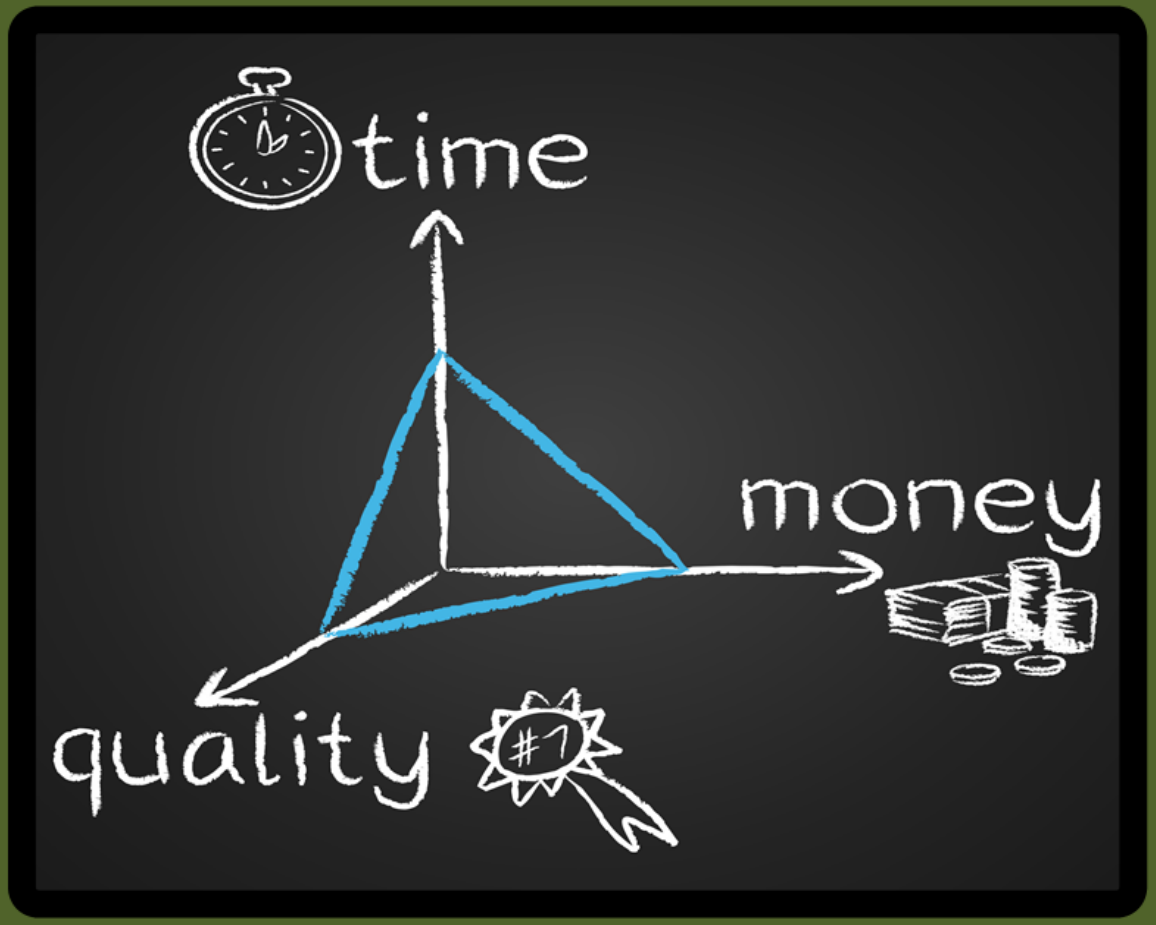
**Resilience Advisory Board For Scotland (Cyber)**
**Chair:** *Senior Govt Figure*
**Membership**
*As per current Scottish Govt Cyber Group*
*Scottish Govt Cyber Lead*

**Enterprise Delivery Board**
**Chair:** CEO Scottish Enterprise
**Membership**
Scottish Enterprise Lead
Scottish Govt Enterprise Rep
Scottish Gov CNI Rep
Financial Services Rep x 2
Finmeccanica Rep
Rep from Tech Delivery Board
Security segment Rep
Retail segment Rep
Energy sector Rep
Manufacturing Rep
Crime Enforcement Rep
Information Assurance Rep

**Education Delivery Board**
Chair: Senior Academic Figure
Membership
Scottish Govt Education Rep
Rep from Enterprise Del Board
Crime Enforcement Rep
Napier University Rep
Glasgow Caledonian Univ Rep
St Andrew's Rep
Security specialist Rep
Financial services Rep
Information Assurance Rep
Knowledge Mgmt Specialist
Outreach Rep

**Technology Delivery Board**
Chair: Senior Entrepreneurial Figure
Membership
Scottish Govt Technology Rep
Scottish Enterprise Rep
Crime Enforcement Rep
Rep from Enterprise Del Board
Academic Rep
Scottish Procurement Rep
Specialist Security Software Reps SME Reps

Cyber Skills




# Cloud-based Training

Prof Bill Buchanan

Terminals

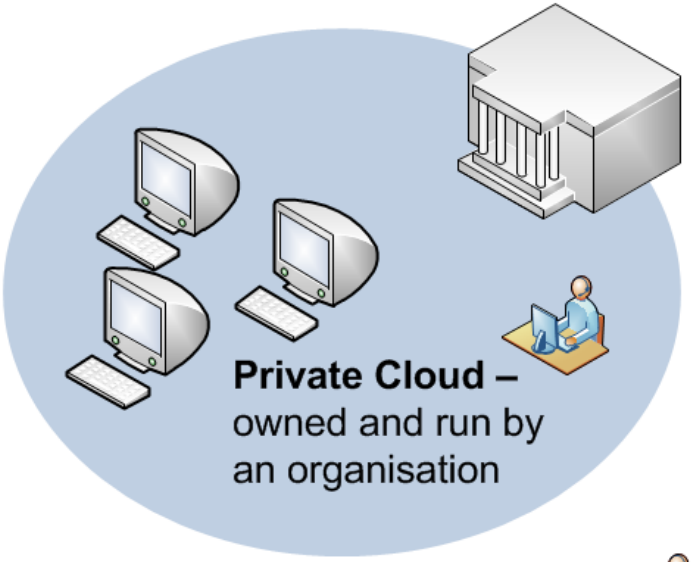
Mainframe

Stand-alone computers

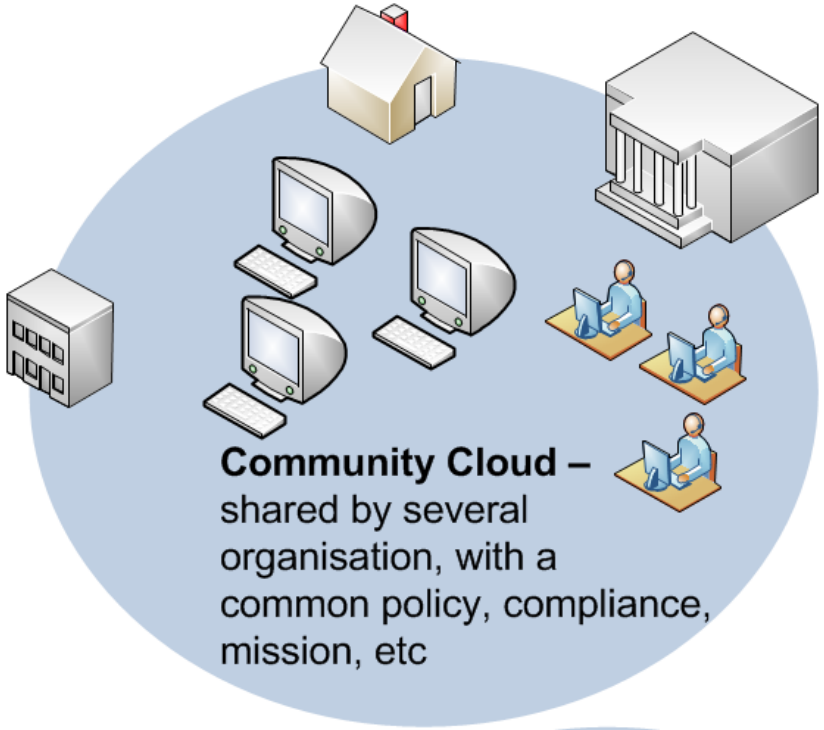

Computers connect to services (SoA)

Computers connected to servers

Servers

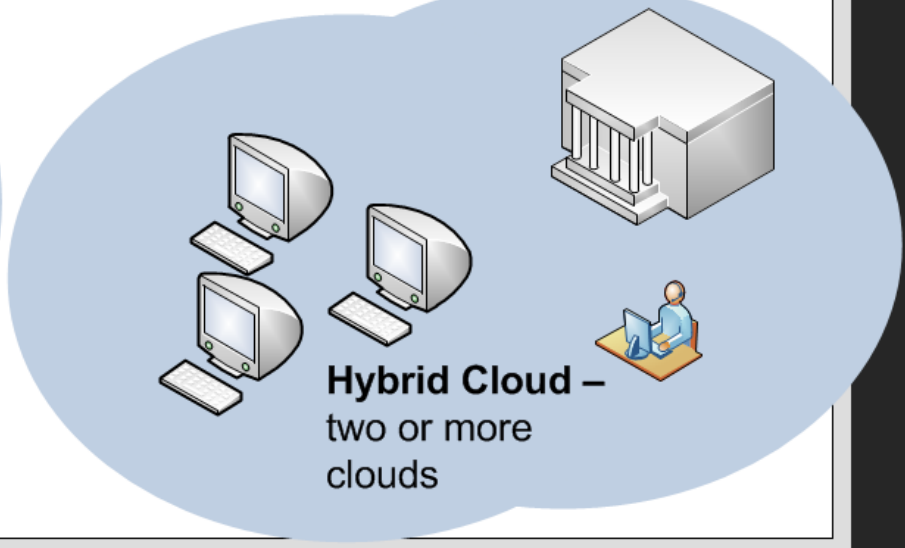


**Private Cloud –** owned and run by an organisation

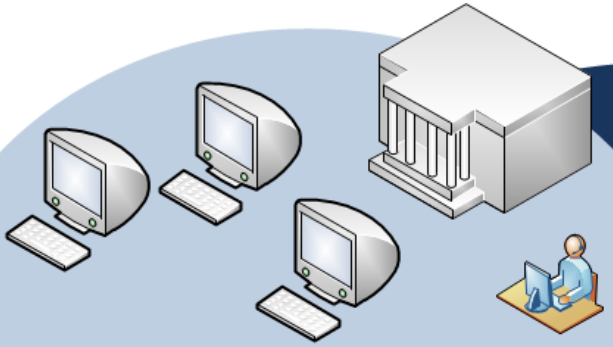


**Community Cloud –** shared by several organisation, with a common policy, compliance, mission, etc

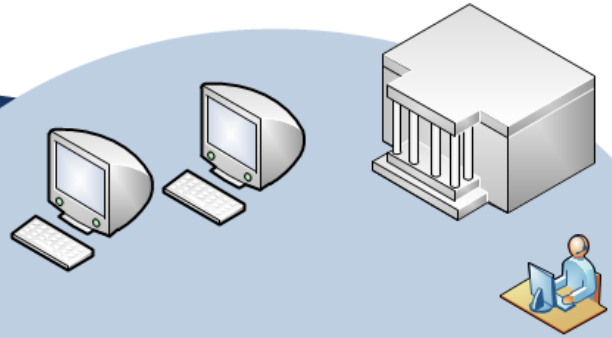

**Public Cloud –** owned by an organisation selling a cloud infrastructure



**Hybrid Cloud –** two or more clouds

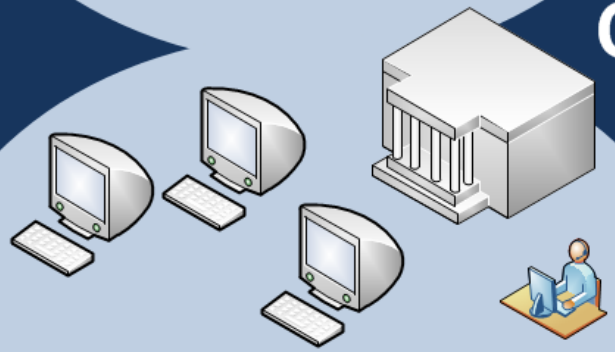


**On-demand self-service.** Consumers get server CPU, memory, bandwidth and storage resources whenever required.

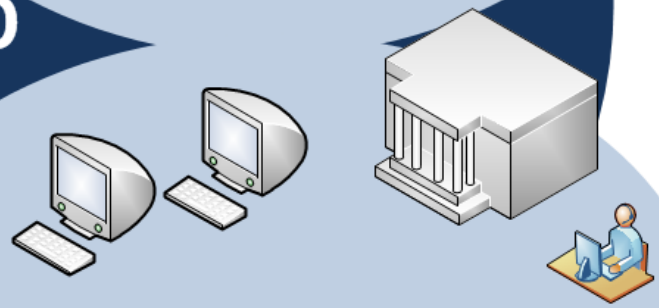


**Location independent resource pooling.** Multiple customers use shared resources within the provider, without actually knowing where the exact location of these are.

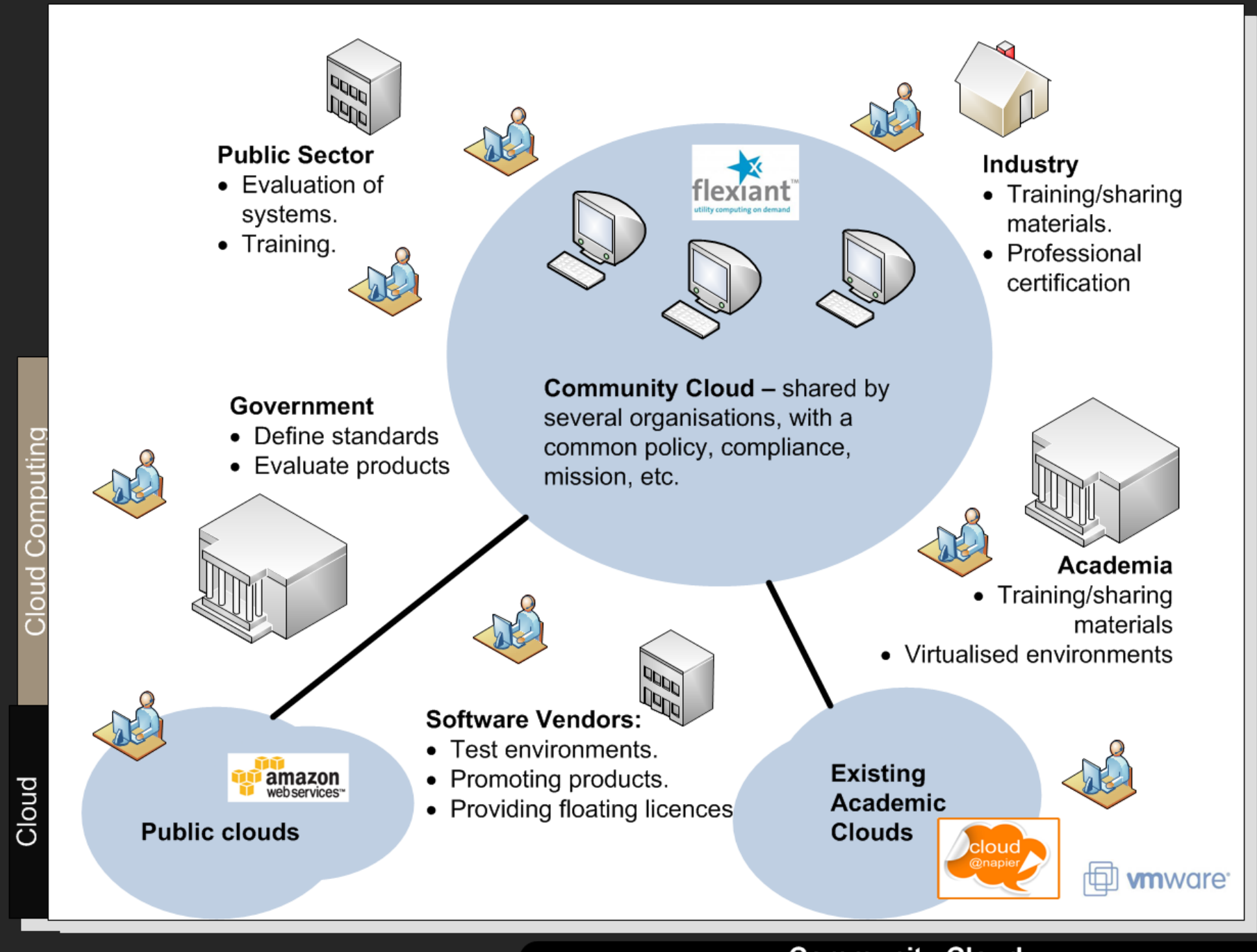
# CLOUD



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



**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.


Cloud Computing
Cloud
Public Sector
• Evaluation of systems.
• Training.
Industry
• Training/sharing materials.
• Professional certification
flexiant
utility computing on demand
Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc.
Government
• Define standards
• Evaluate products
Academia
• Training/sharing materials
• Virtualised environments
Software Vendors:
• Test environments.
• Promoting products.
• Providing floating licences
amazon web services
Public clouds
Existing Academic Clouds
cloud @napier
vmware
Community Cloud

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

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

**Enhancing skills**
- Supports a wide range of pre-built enviroments 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


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

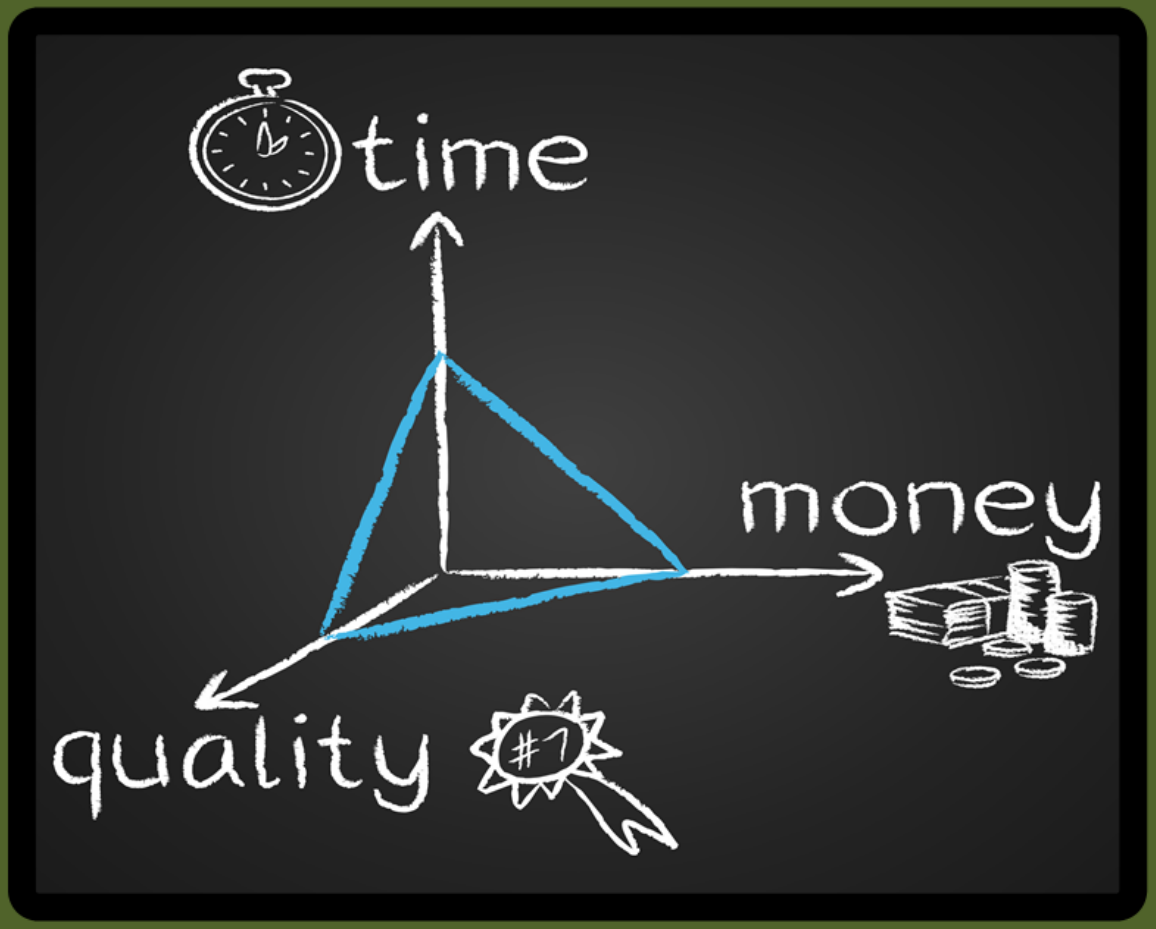
**Continuation of work**
- Students can carry their infrastructures throughout modules/ years.

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

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

**Snap-shots of work**
- Student can create snap-shots, and move back and forward amoungst them.

Cyber Skills




# Example in Teaching

Prof Bill Buchanan

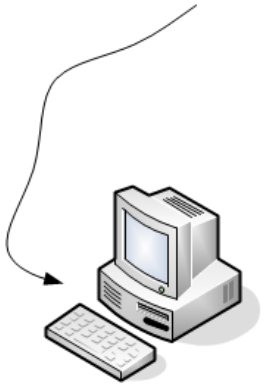
White Hat

Good...

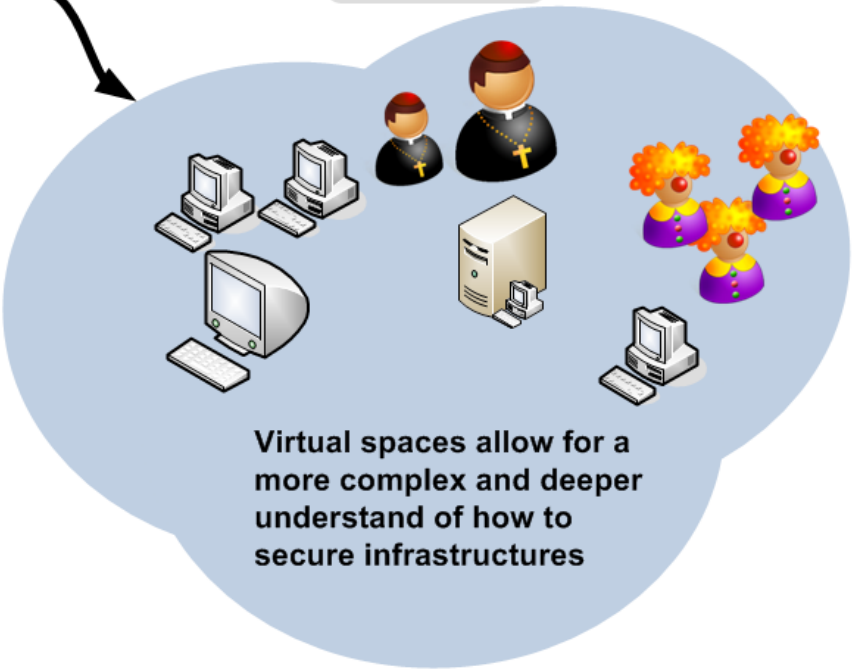
... Bad

Black Hat

Grey Hat



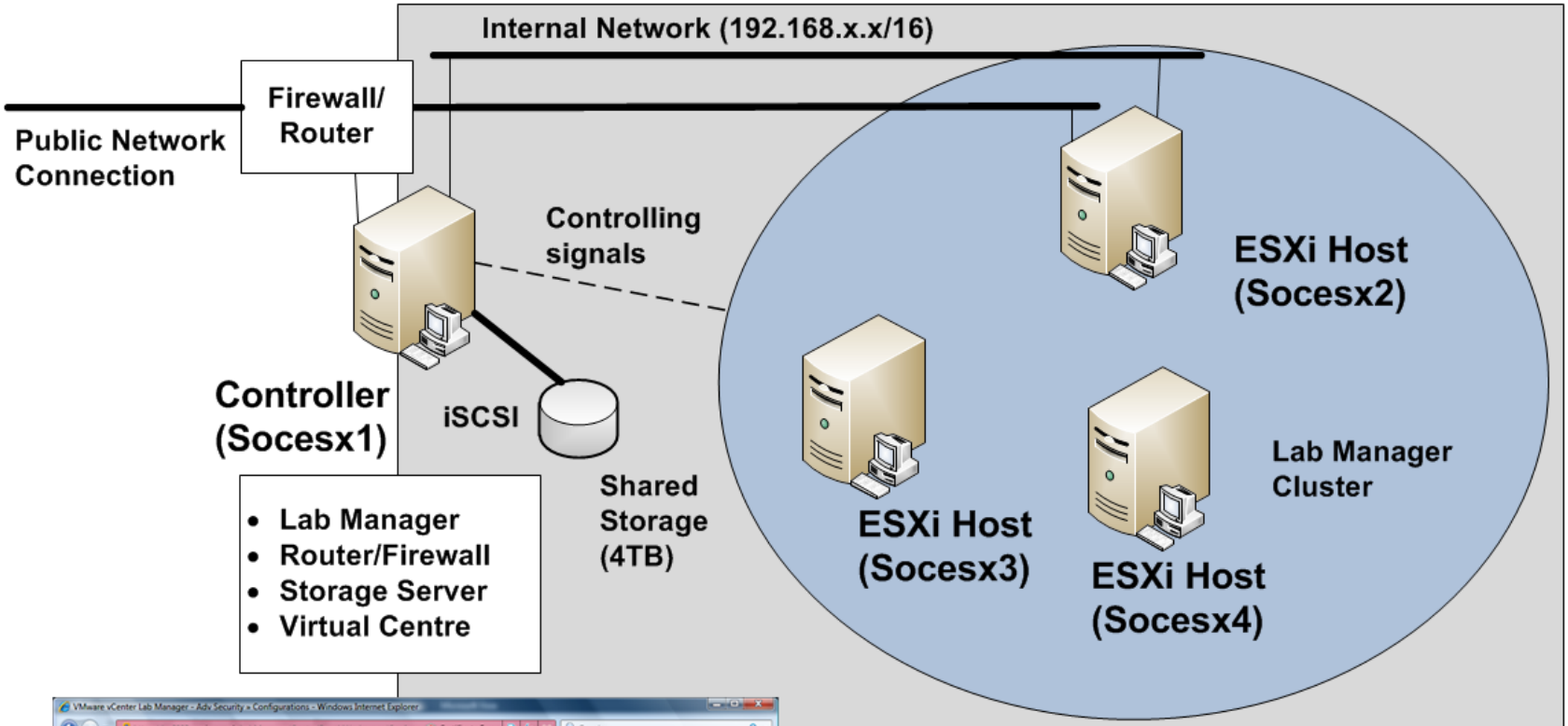
Difficult to use many of the techniques within a real-life space

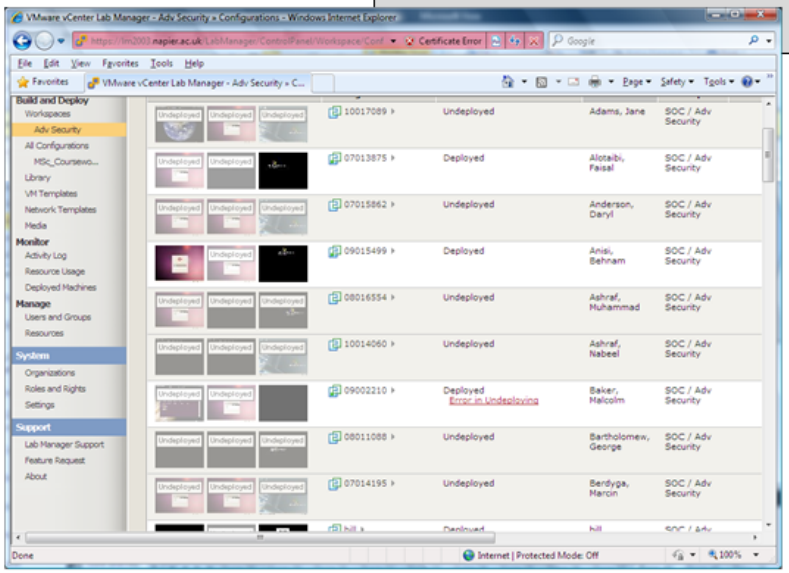


Virtual spaces allow for a more complex and deeper understand of how to secure infrastructures

Demands on professional certification

Employers now require in-depth knowledge and a range of skills



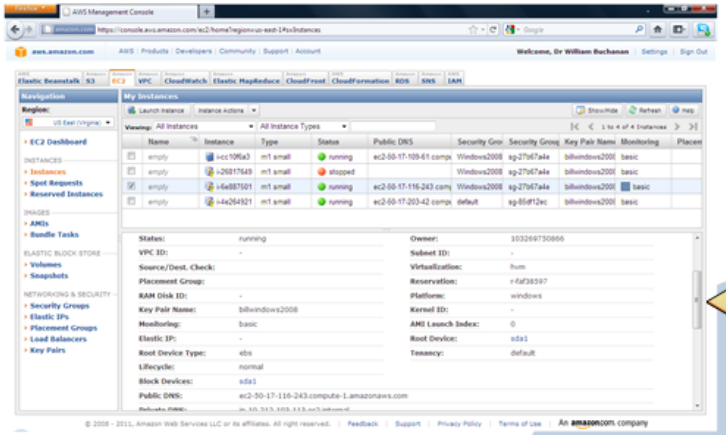
vCenter

Cloud

vmware

cloud
@napier

Napier vCenter infrastructure



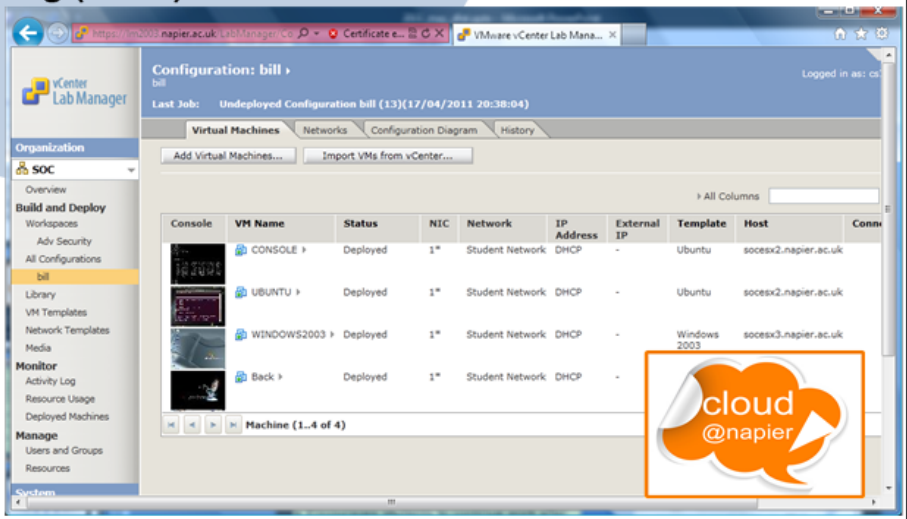
**Virtualised and Cloud-based labs (AWS):**

- Range of state-of-the-art operating systems and tools.
- Evaluation of Public Cloud resources.

**Teaching of four modules in computer security, digital forensics and database systems for 2010-2012 (inc. Host-based Forensics, Security and Forensic Computing and Adv Security and Digital Forensics at BEng/BEng (Hons)/MSc level**

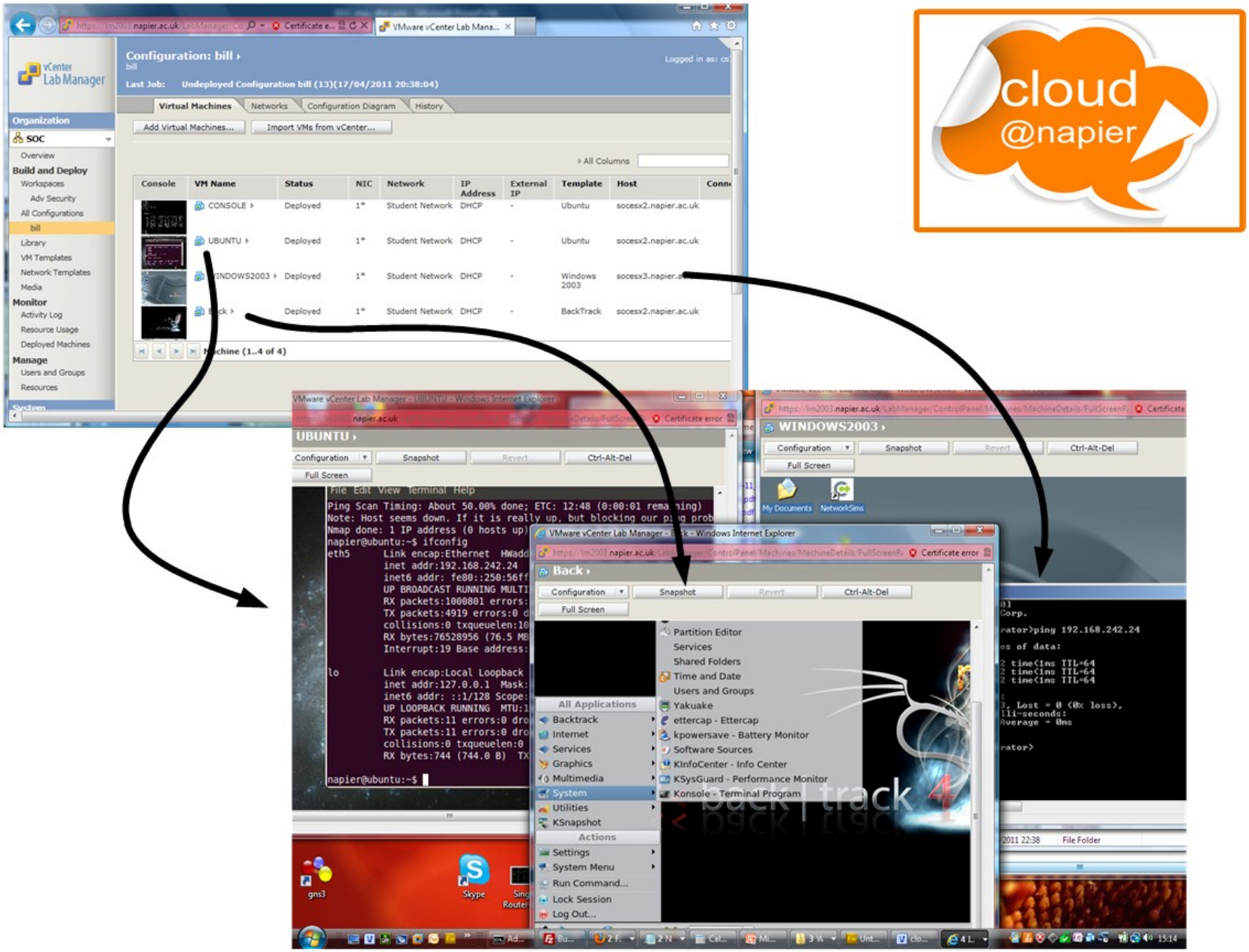
**Virtualised and Cloud-based labs:**

- Complex infrastructures for evaluation for students.
- Deep analysis of security and digital forensics in an isolated environment.
- Industry standard tools and methods.



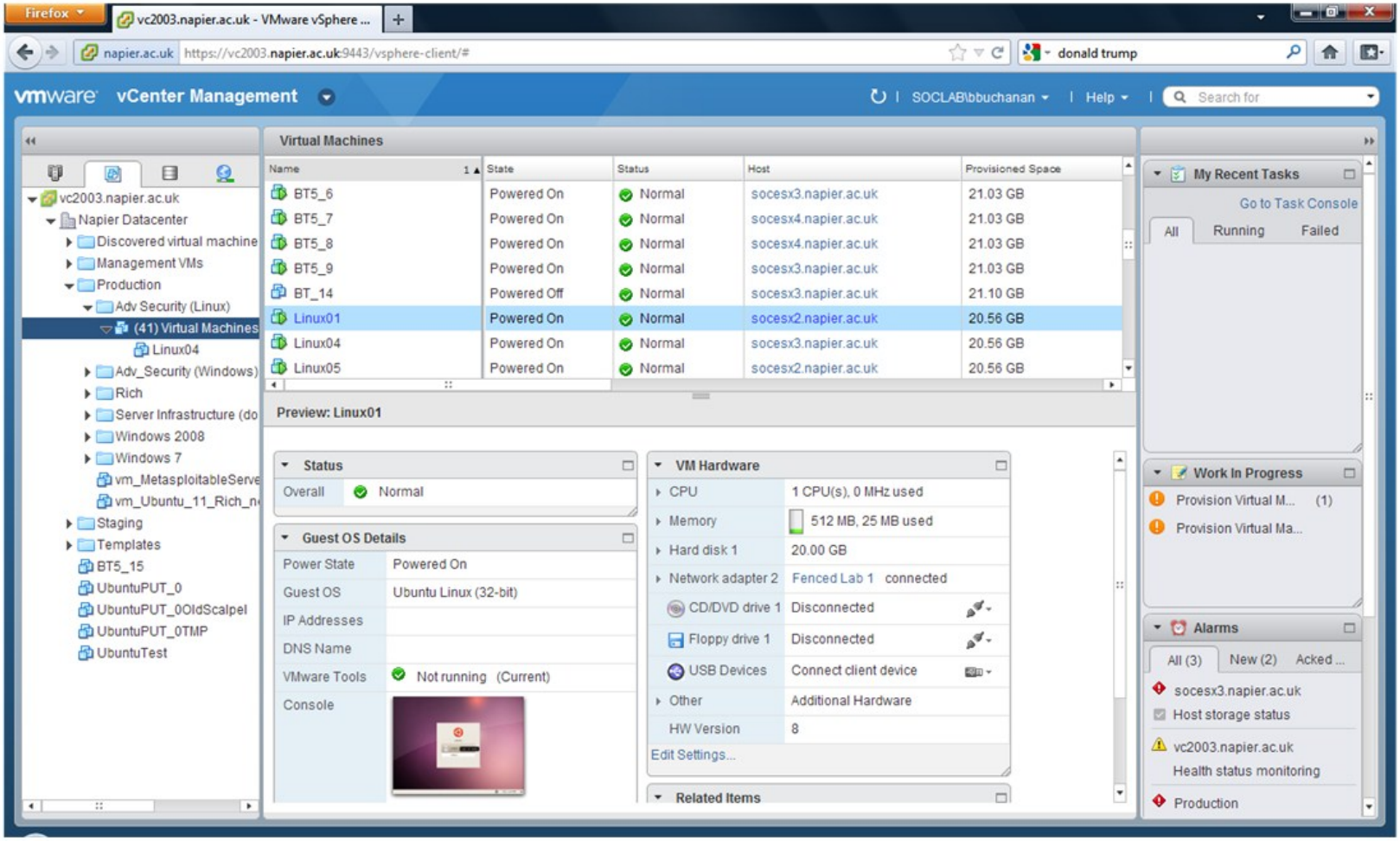

Cloud Computing

Cloud




Cloud Computing

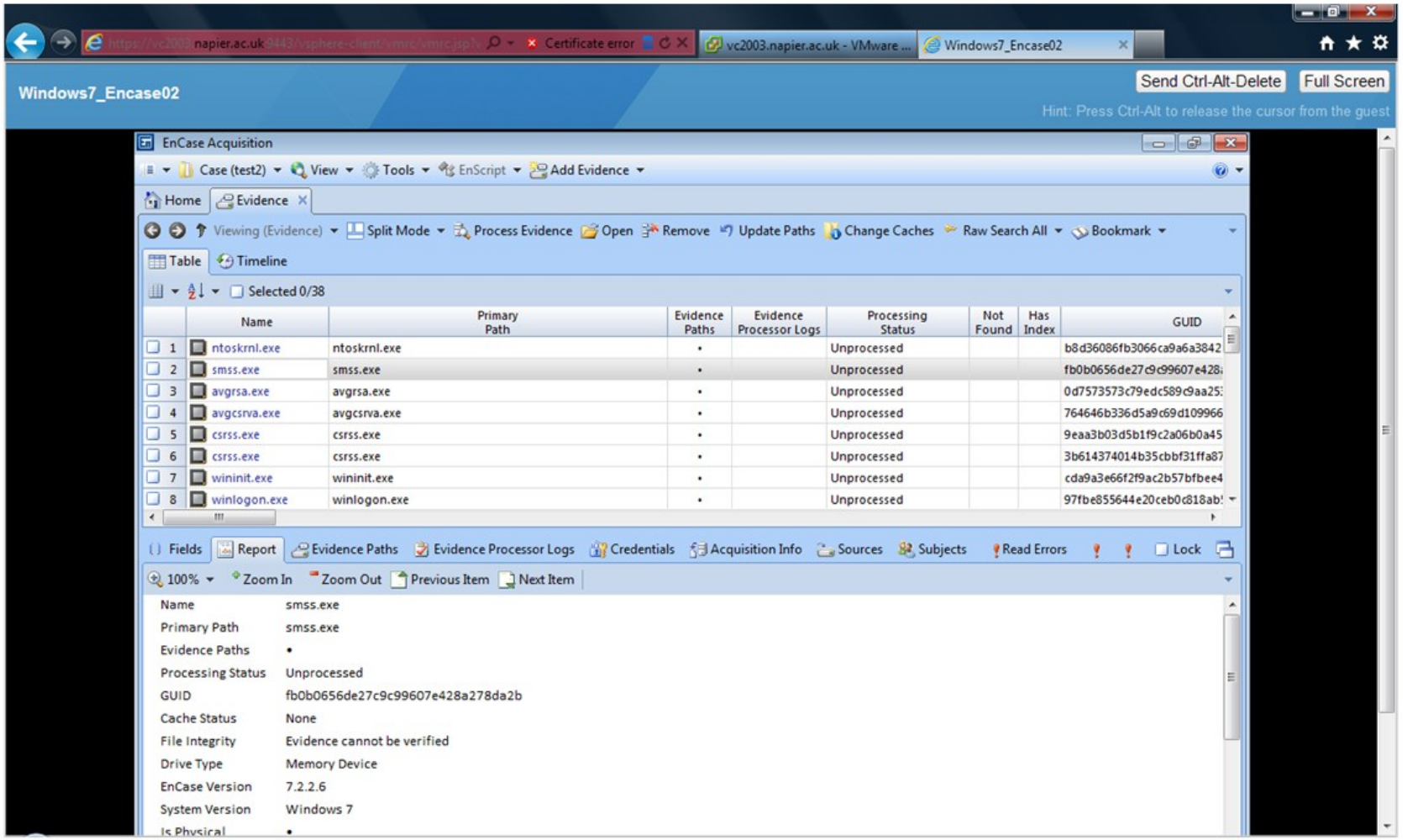
Cloud




Virtual Training

Cloud

Virtual Infrastructure

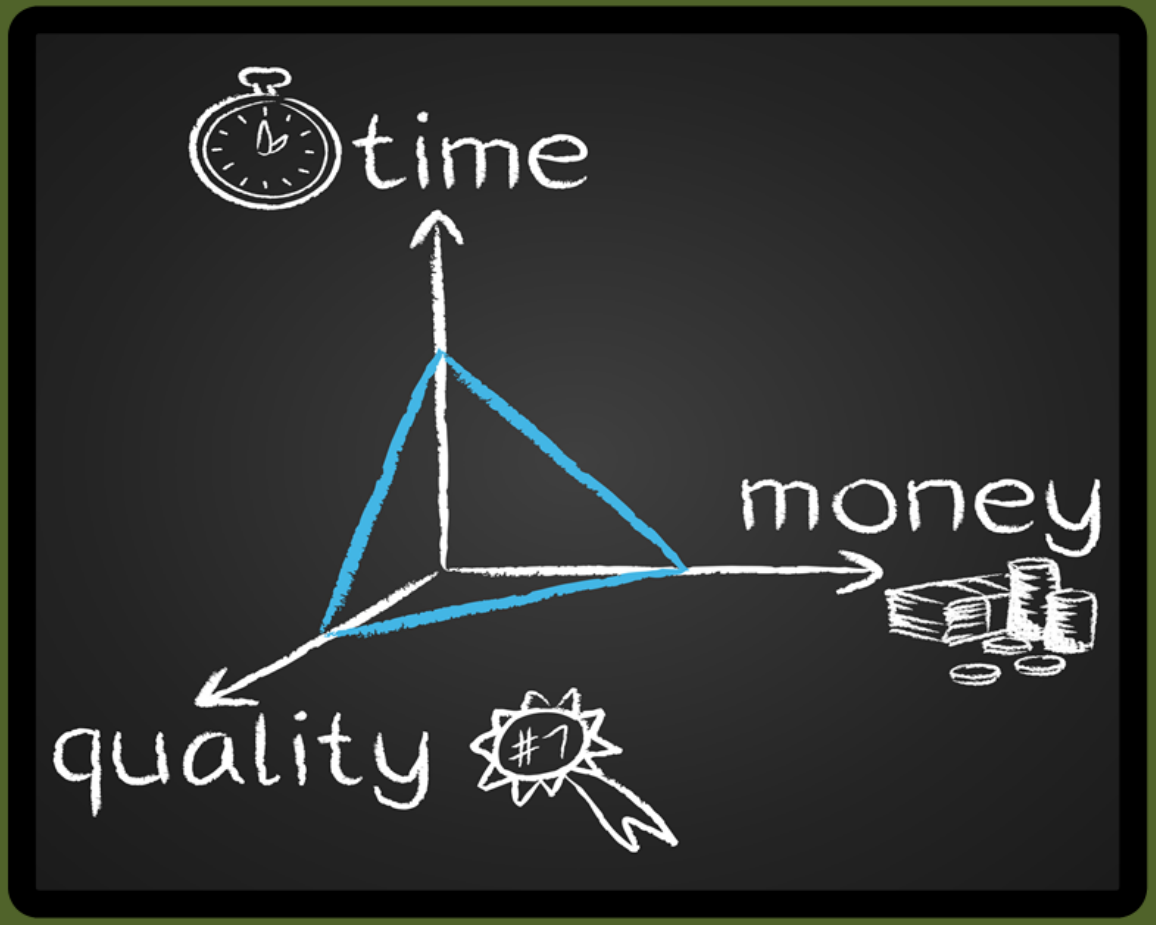



Virtual Training

Cloud

Virtual Infrastructure

Cyber Skills




# Training Infrastructures

Prof Bill Buchanan

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

Intruders

**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**

Roles

Cyber

Roles

**Training Issues:**

- Students not exposed to a wide range of tools and environments.
- Lack on training on real-life environments.
- Physical location can restrict training opportunities.
- Lack of standardized images of training.
- Lack of engagement from industry/law enforcement (not in Scotland!)
- Environments are often fairly static and not changing.
- Focus on knowledge-based professional certification.

**Academia:**

- Cannot produce graduates fast enough, and with the right range of skills.
- Lack of flexibility in programmes.
- Disconnect between recruitment from industry and universities.
- Large variation in standards of educational provision.
- Lack of accreditation of professional practice at post graduate level.
- Lack of industry doctorate support.
- Lack of access to standard tools using in security and digital investigations.
- Levels of achievement for undergraduate and postgraduate levels not well defined.



Security Professionals

Digital Investigators

Developers

General Public

Definition of levels of achievement across Scotland

Standardised and Visualised Labs

Sharing of resources across universities

Requirement to train at every level

Seminars by Industry/ Law Enforcement Experts

Integration with European training infrastructures (2Centre)

**Cyber Training Infrastructure**

Accreditation of work based learning

Collaborative Training infrastructures for Key Sectors

Accreditation for professional certification

Fully On-line Material: Lectures, Labs and Tutorials

Need for more public engagement in Scotland

Future?

Cyber

The Future?

MPhil/PhD

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

CISSP

EnCase

CEH

Cisco

Microsoft

MSc level Security/ Digital Forensics (6x20 credits)

Four Year Undergraduate Degree

Work-based Learning

60 credits

Part-time/Full-time mode

Distance/Blended Learners

## Defining standards:

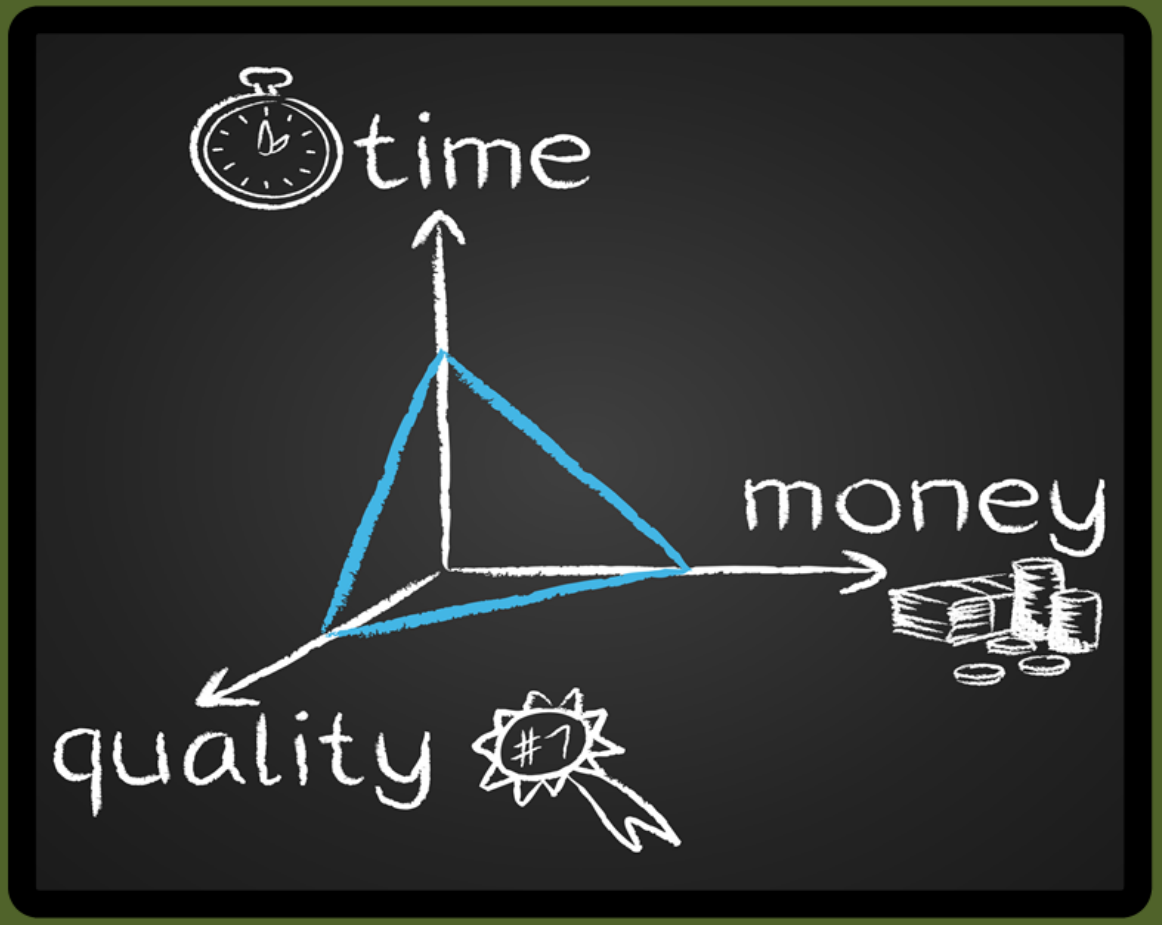
- Academia.
- Scottish Police.
- SMEs.
- Large industry.
- Professional Bodies.
- Public sector.
- Etc.

Roles

Cyber

Roles

Cyber Skills




# Cyber Skills and Training

Prof Bill Buchanan