

Cloud Environments



The Future of Cloud

Prof Bill Buchanan

Cloud Environments



- Introduction to the Cloud.
- Cloud and Health.
- Cloud and Teaching.
- New Risks ... new Opportunities.

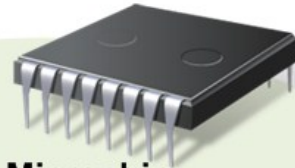
Cloud Environments



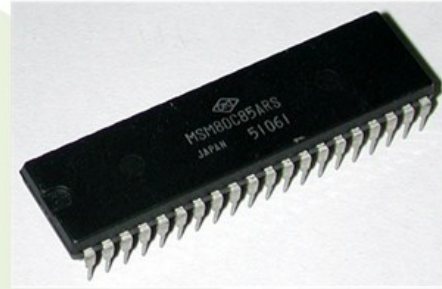
- Introduction to the Cloud.
- Cloud and Health.
- Cloud and Teaching.
- New Risks ... new Opportunities.



Transistor



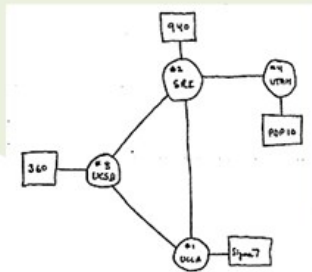
Microchip



Microprocessor



The Cloud



THE ARPA NETWORK

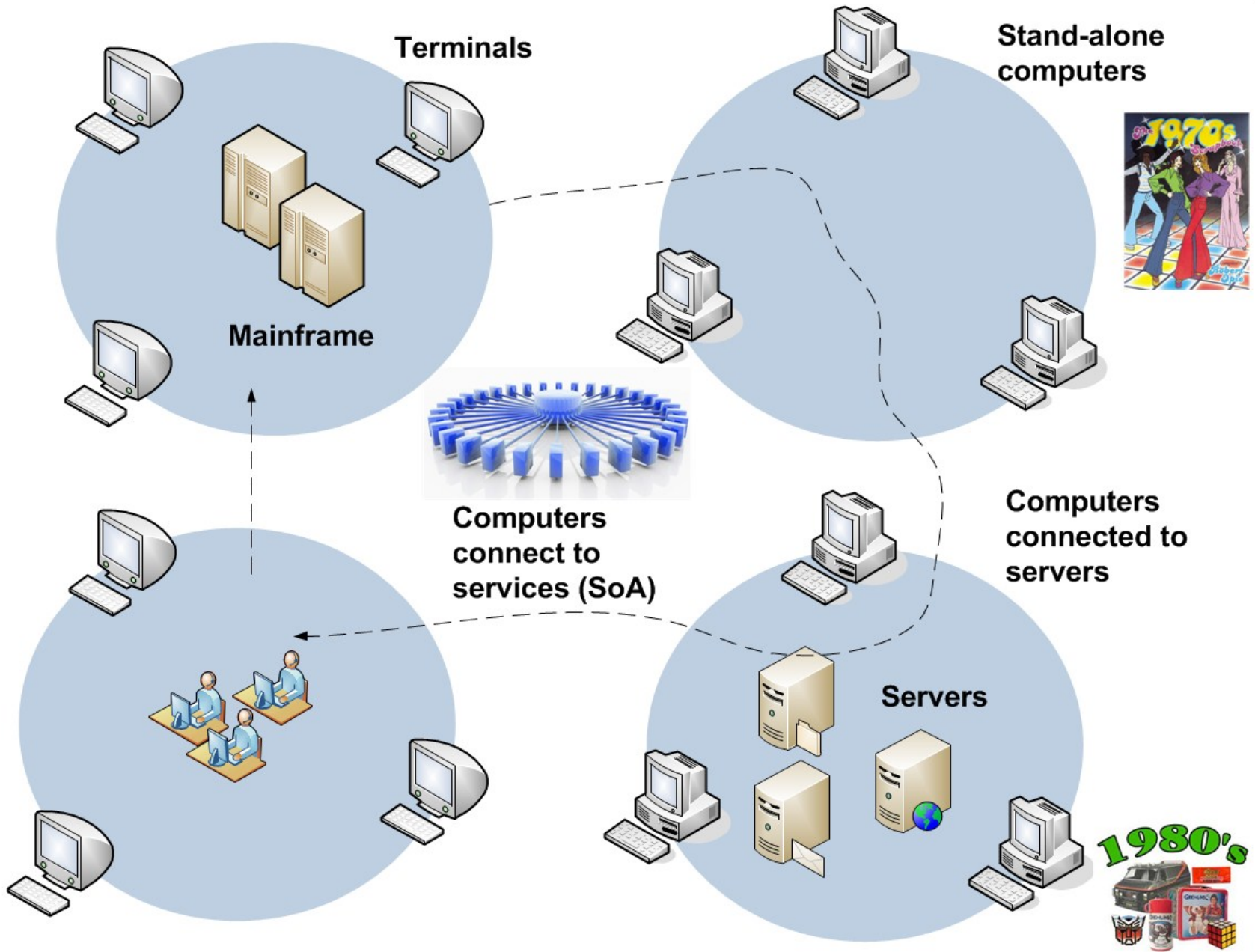
DEC 1969

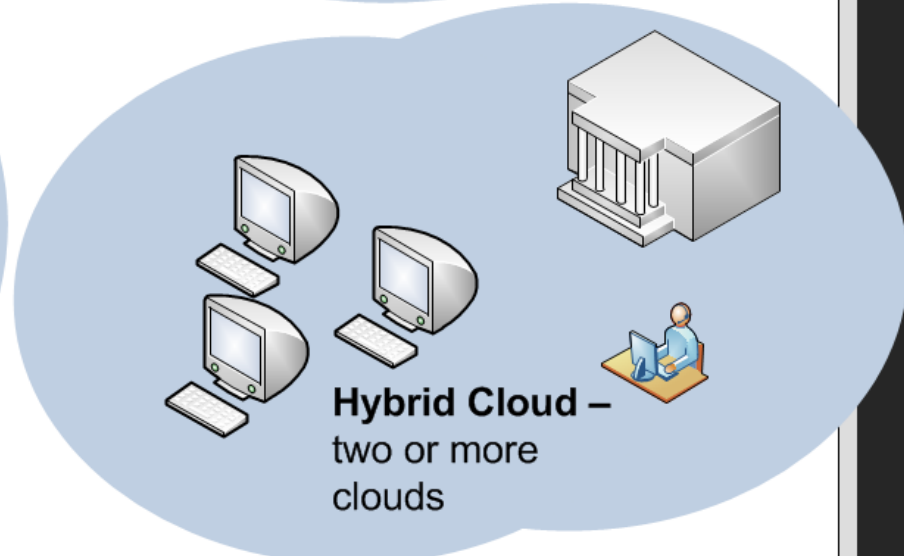
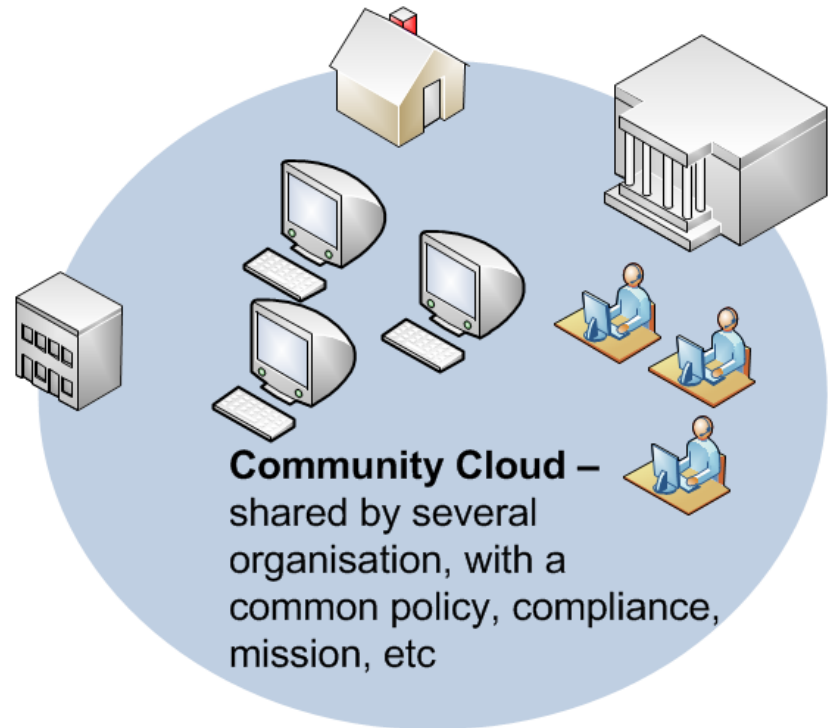
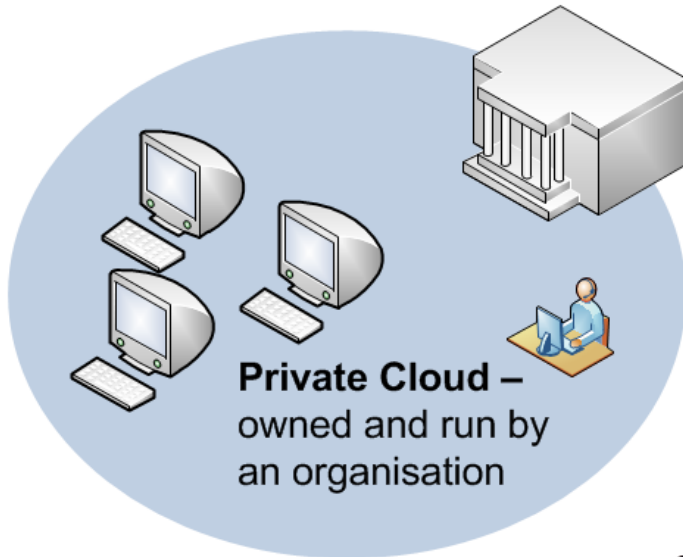
4 nodes

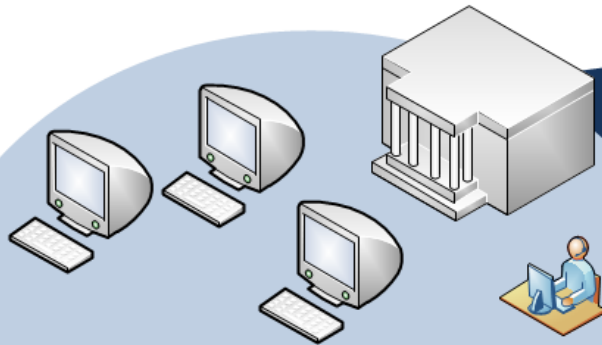
The Internet



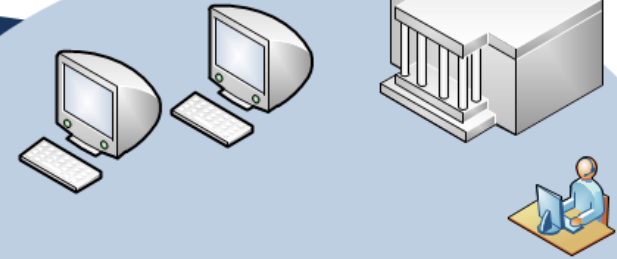
The Personal Computer





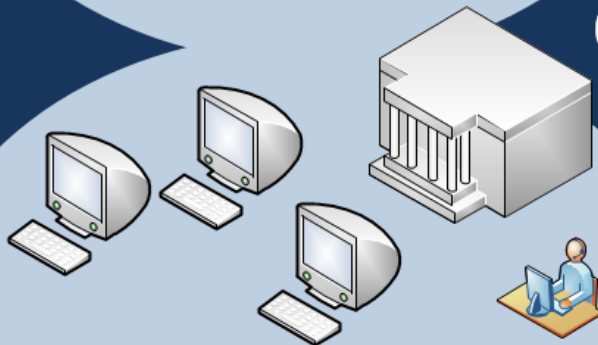


On-demand self-service. Consumers get server CPU, memory, bandwidth and storage resources whenever required.

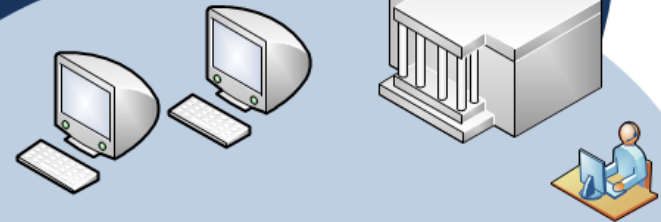


Location independent resource pooling. Multiple customers use shared resources within the provider, without actually knowing where the exact location of these are.

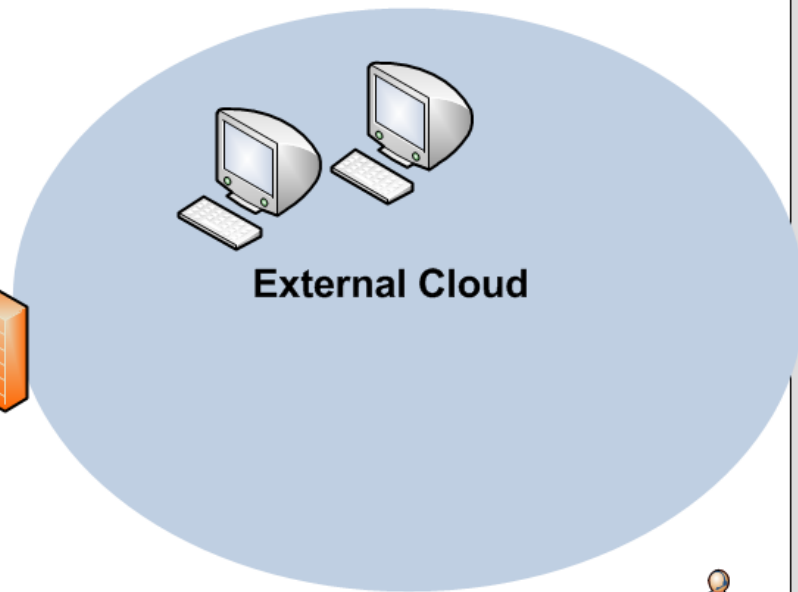
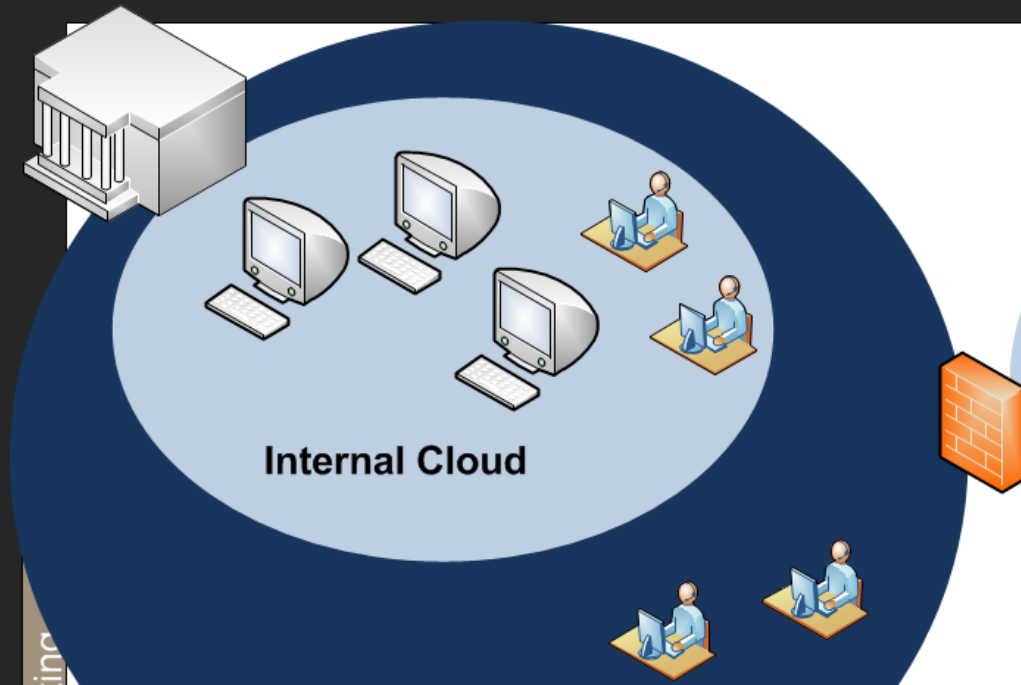
CLOUD



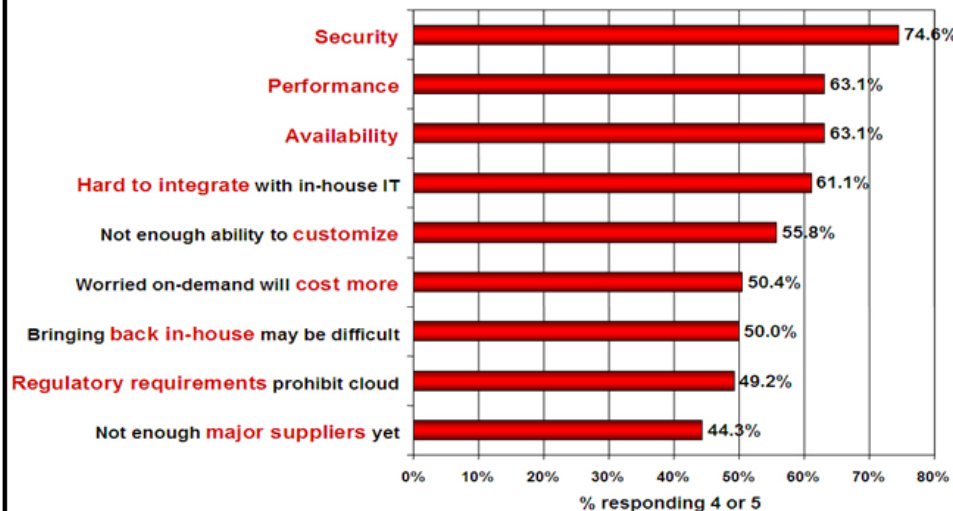
Rapid elasticity. Consumers can easily scale-up and scale-down, whenever required.



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.



Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
 (1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

Audit/compliance

Can I be compliant with statutory and regulatory requirements?

- Where is my data stored?
- Who handles breach notifications?
- How long is my data stored for?
- How is eDiscovery handled?

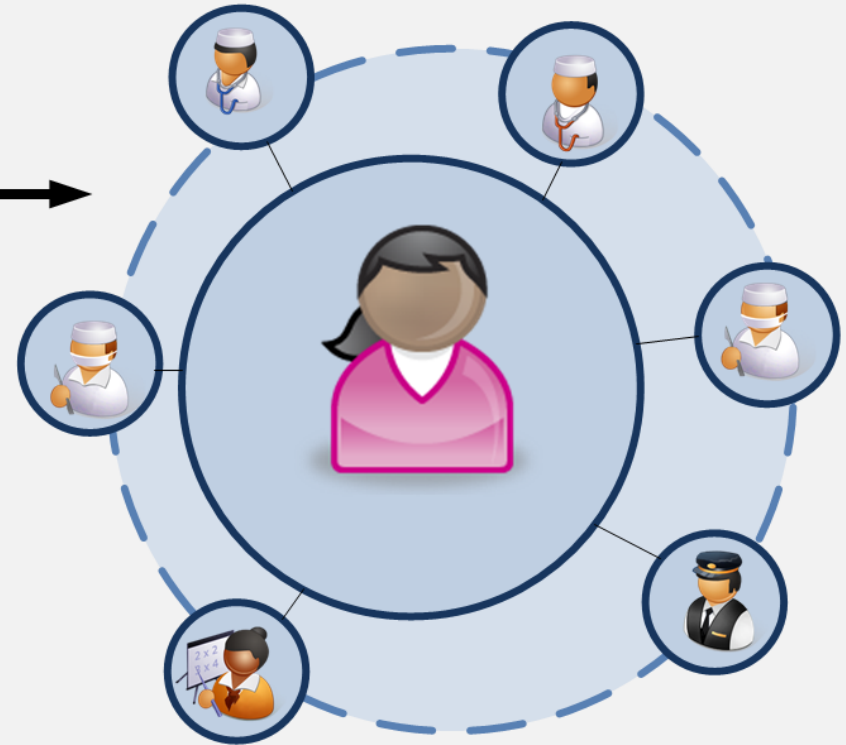
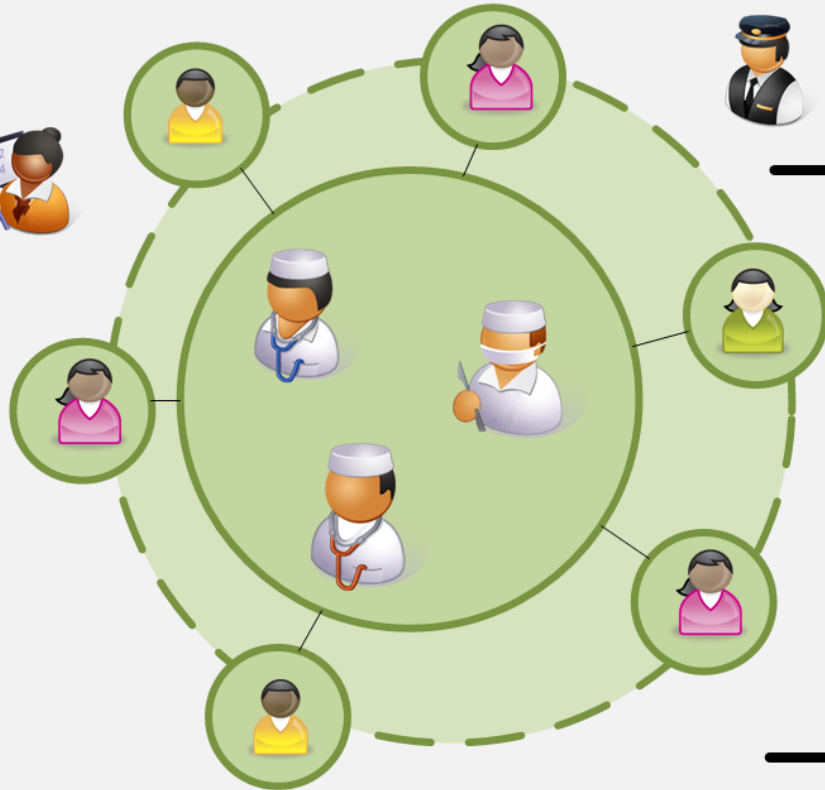
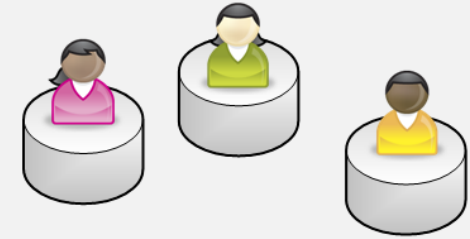
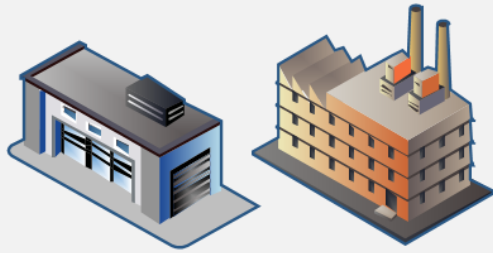
Cloud Environments



- Introduction to the Cloud.
- Cloud and Health.
- Cloud and Teaching.
- New Risks ... new Opportunities.

Industry Age

Information Age



**Centralised, Non-integrated,
Ad-hoc, Clinician Focused, Reactive,
Clinician Control of Records**

**Distributed Patient Care, Holistic,
Patient Focused, Pre-emptive,
More Patient Control of Health**



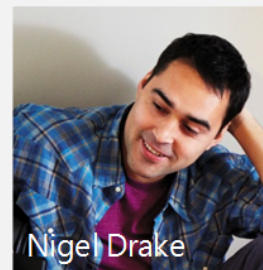
Nurse Kate

- Healthcare Professional.
- Invited user



Deirdre Drake

- Care Subject
- 82 years old
- House bound
- COPD (Chronic Obstructive Pulmonary Disease)



Nigel Drake

- Invited user

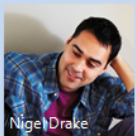


- GP.
- Invited user

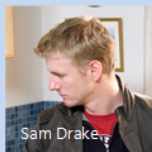


Sam Drake

- Site Creator
- Primary Carer



Nigel Drake



Sam Drake



Nurse Kate

Assisted Living
(Informal and
Trust based)

Primary Health Care (Formal
and role-oriented) - GP

Secondary Health Care
(Formal and role-oriented)
- Hospitals/A&E

Social Care/Health/etc



Nurse Kate

Societal

Technical

Lack of integration between assisted living, primary and secondary care

Patient records are often static

Aging population

Different systems/formatting used for data

Lack of information sharing across the public sector

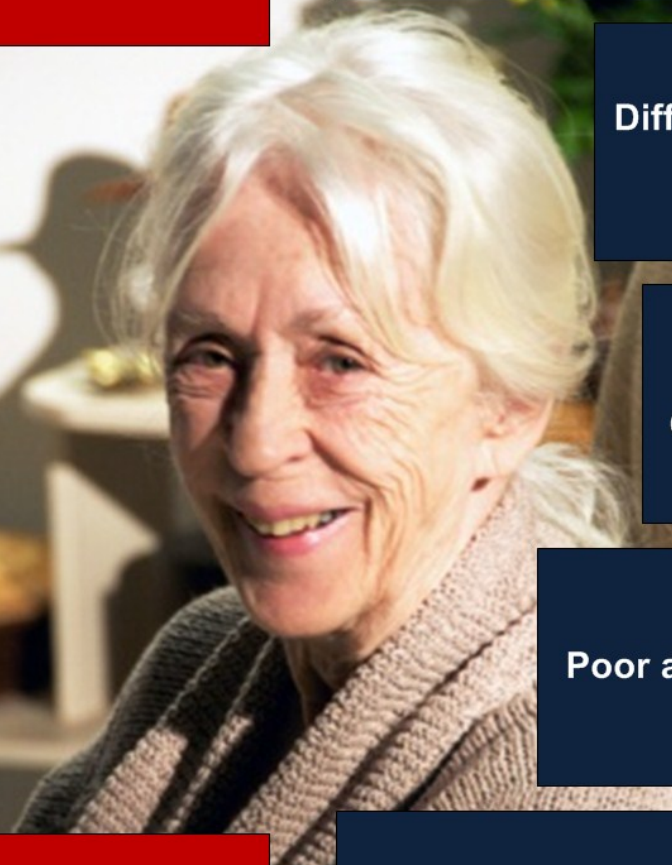
Limited/difficult access methods ... typically Government infrastructures ... lack of trust

Strong demand to consume health care data

Poor access control to data

Lack of integration with careers and trusted people

Data often aggregated and context is often lost



**Digital
Trust**

Rights

**Clinical
Services**

**Human
Trust**

Identity



Strong

Infinite

Governance

possibilities

Translation of rights
Translation of identities



**Strong Governance
Policy**

**Assisted Living
(Informal and Trust
based)**

**Primary Health Care (Formal
and role-oriented)**

**Secondary Health Care
(Formal and role-oriented)**

Manager might ask: What's difference in length-of-stay between different age categories for June?

Consultant might ask: How does the Early Warning Score affect the length-of-stay?

Family friend might ask: In which ward is Deirdre?

PatientID



Static Patient Record

- Often localised
- Different systems/formats
- Poor access control
- Poor identity verification
- Cannot be aggregated
- Etc.



Domain A

ConsumerID (RoleID)

Data Storage (within the Cloud in buckets)

PatientID Bucket

Dynamic Patient Records

Security Policy (including interdomain rights)

CaptureTime

EventID

LocationID

CapturerID (RoleID)

PatientID

ClinicalMeasureID (ClinicalUnitsID)

DeviceID

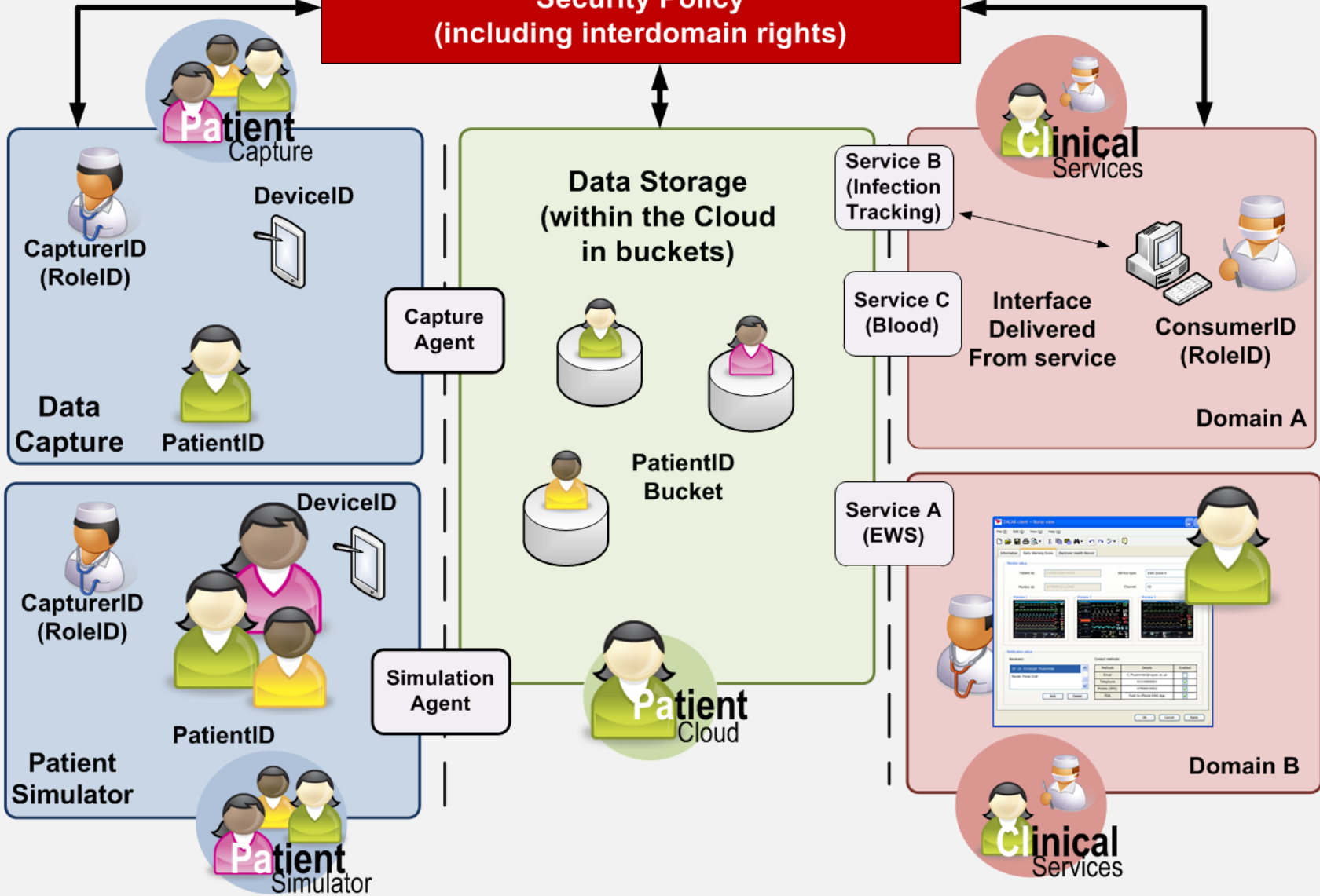
AreaID

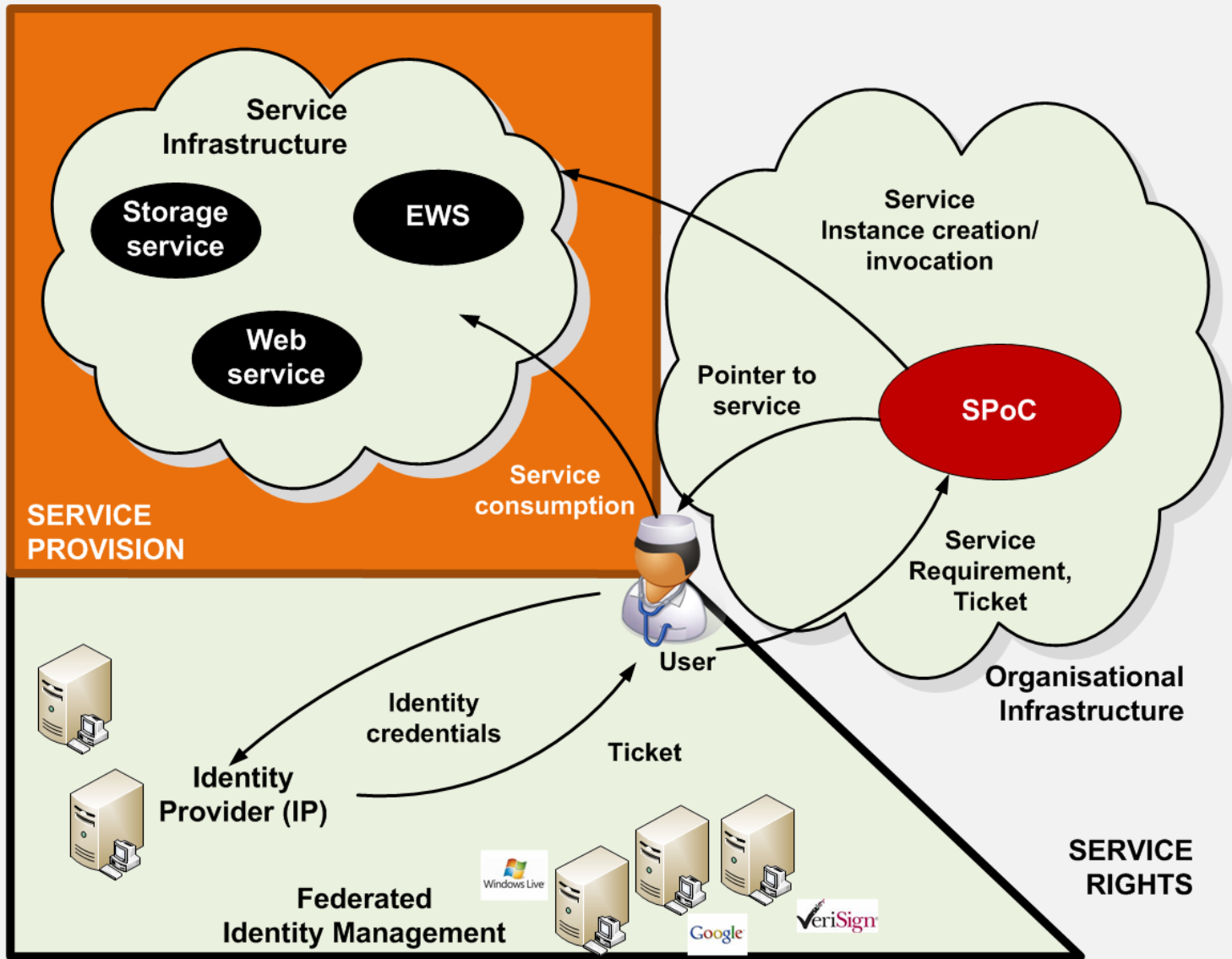


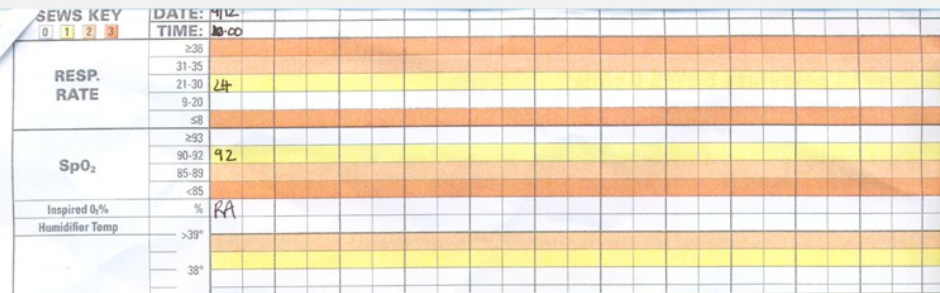
Security Policy Translation Bridge

Data Translation

Security Policy (including interdomain rights)







Observation Chart

NHS
Lothian

Consultant: _____

Date chart commenced: _____

This is chart number _____ this admission

Actual or estimated patient weight _____ kgs

ASU: _____

Attach a patient Addressograph here or

Name: _____

DOB: _____

Unit No: _____

An Early Warning Score (SEWS) must be calculated every time patient observations are recorded. If SEWS score 4 or more then call the appropriate doctor and nurse in charge using the guidelines below. Increased frequency of observations (minimum hourly) should be commenced and a detailed report of the patient's medical notes should be completed.

Early Warning Score 4 or more
or concern with a patient's condition.

Call Junior Doctor & Senior Nurse/Nurse Practitioner
If Dr cannot attend within 20 mins, they should arrange a Deputy.

Practitioner/Dr unable to attend within 20 mins or SEWS increased by 2 or patient deteriorating.

Call appropriate SHO/Registrar & Senior Nurse/Nurse Practitioner

Dr unable to attend within 10 mins or SEWS increased by 2 or patient deteriorating.

Call appropriate Registrar/Consultant
Consider ICU referral/review of treatment plan

Early Warning Score 6 or more
or rapidly deteriorating patient.

Persistent Pain – 6 or above and unresponsive to guidelines

Call Medical Staff/Senior Nurse/Nurse Practitioner

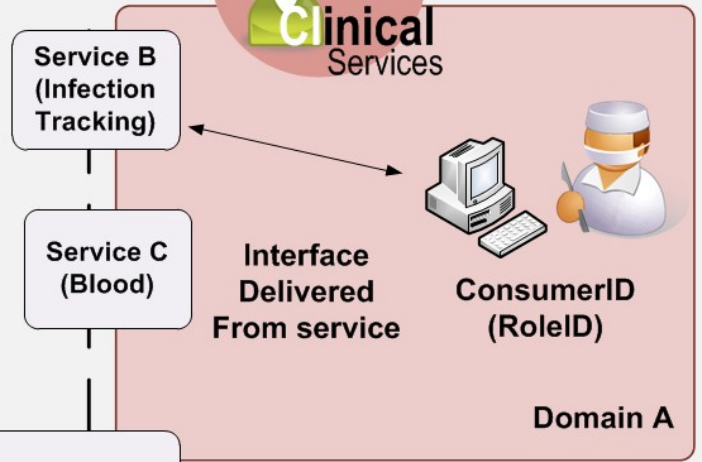
For further advice contact:

ACUTE
Mon- Fri: Bleep Acute Pain Team
Out of hours: On-call anaesthetist

CANCER-RELATED
Mon- Fri: Bleep Palliative Care Team
Out of hours: via switchboard

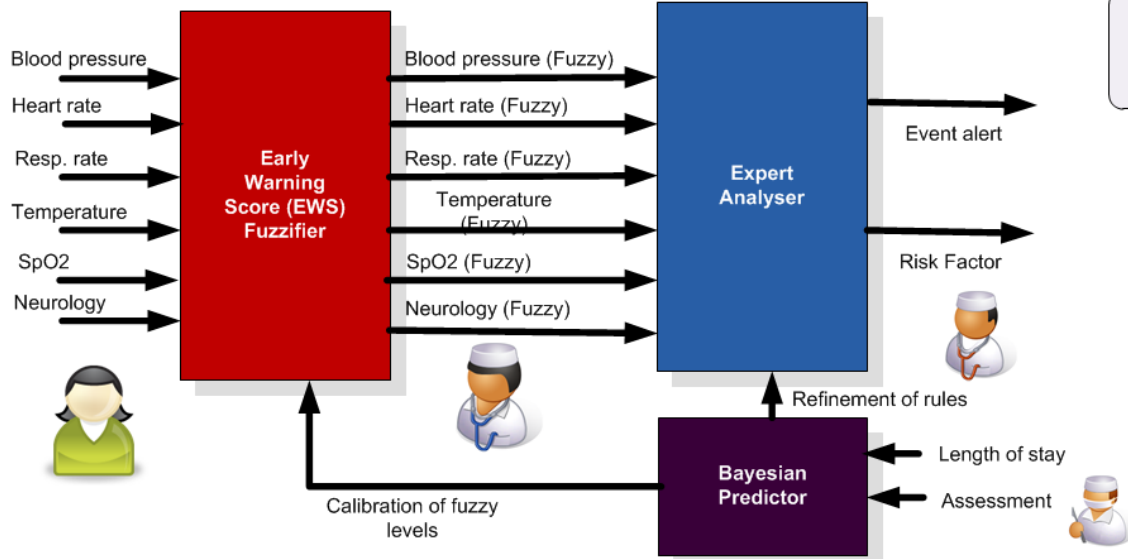
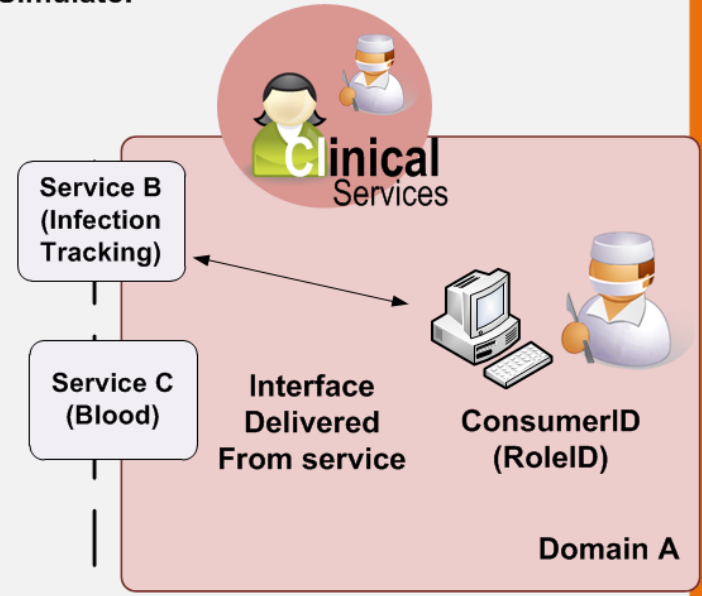
Reorder Ref: WLT1016-Rev: 05/07

Service A (EWS)

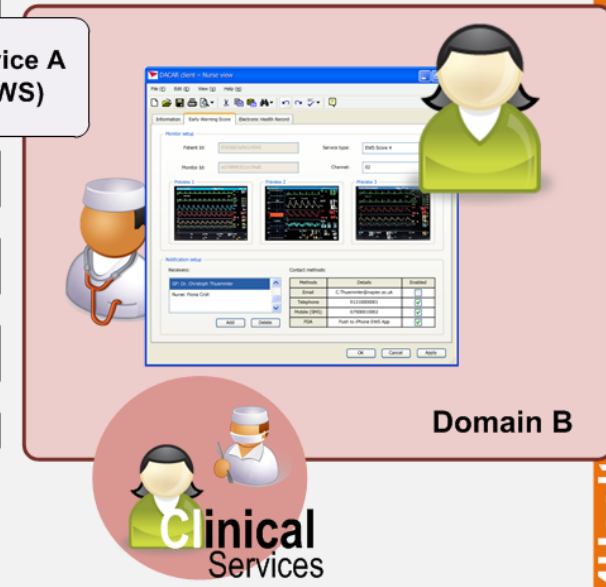




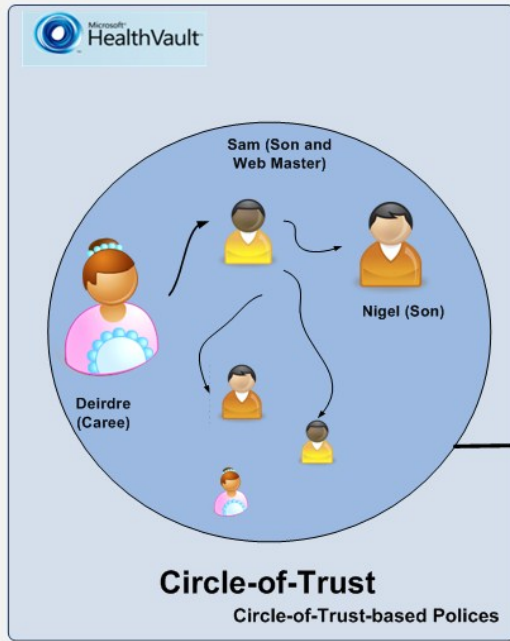
Patient Simulator



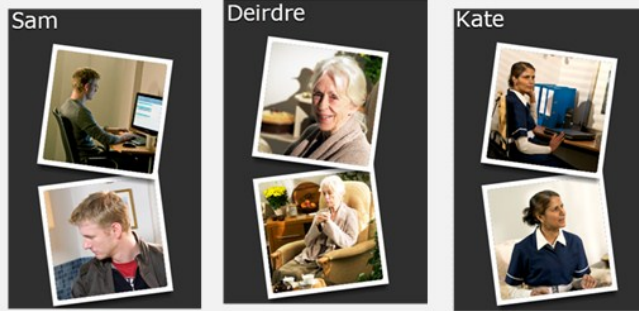
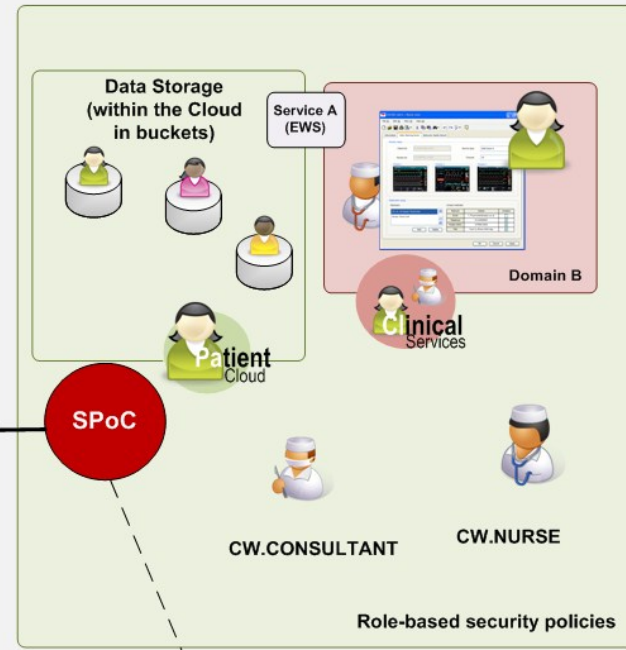
Service A (EWS)



Assisted Living



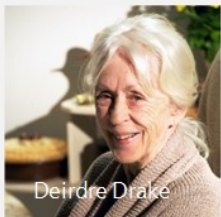
Primary/Secondary Care



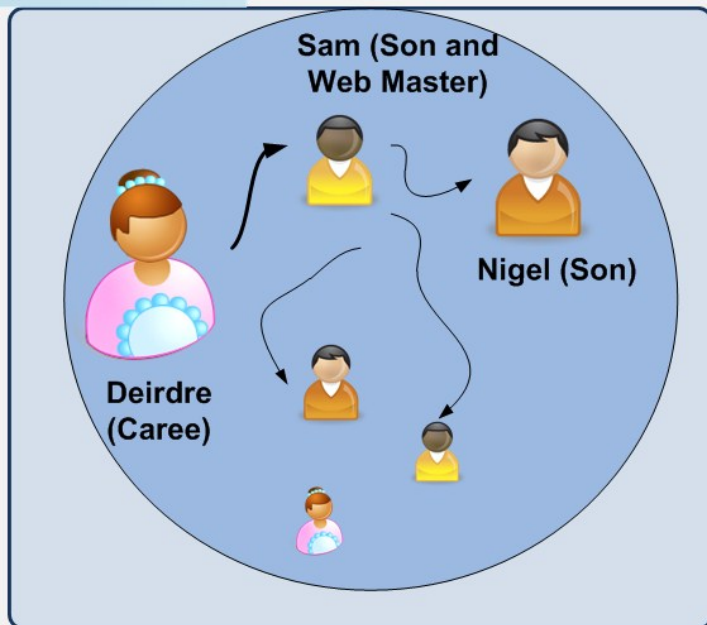
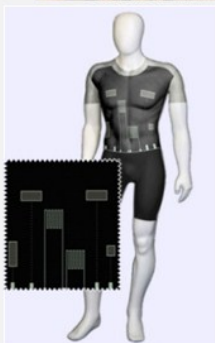
```
[permit] [C&w.NURSE] [C | R] [Temp | SpO2 | HR | BP | RR | Pain] of [Patient26078] with [EWS] from [Chelsea & Westminster Hospital] for [*] records in [P2010-12-30T00:00:00] using [Data Protection Act]
```

```
[permit | deny] [Requester] [C | R | U | D] [Attribute] of [Object] with [Context] from [Owner] for [N] records in [Time window] using [Compliance]
```

Governance Policy



Deirdre Drake

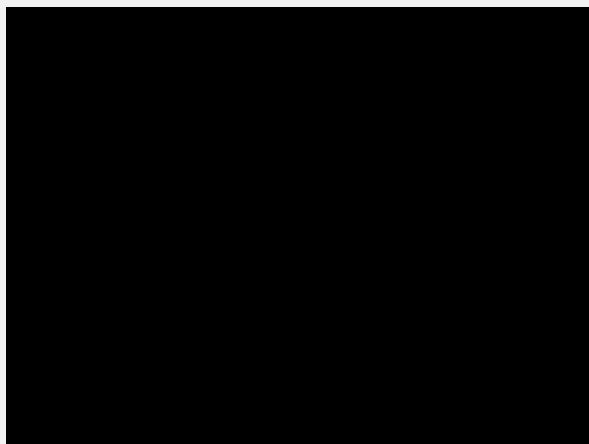


Circle-of-Trust

Clinical vest monitors:

- Blood pressure.
- Temperature.
- Heart Rate.
- SPO2.
- Location (GPS).

Data uploaded into the Cloud

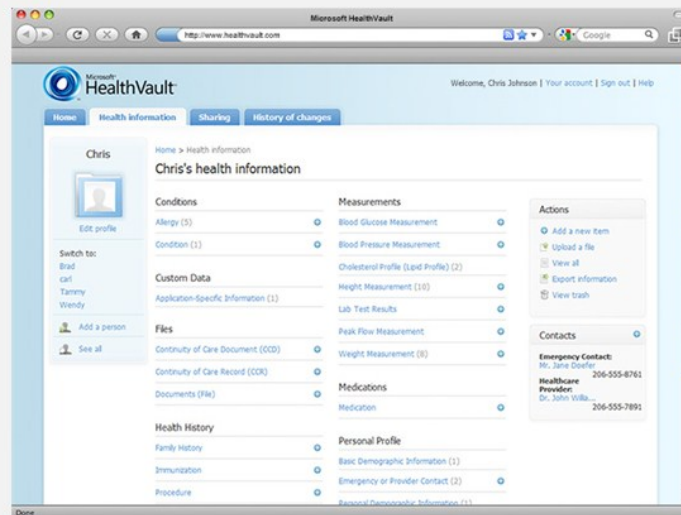


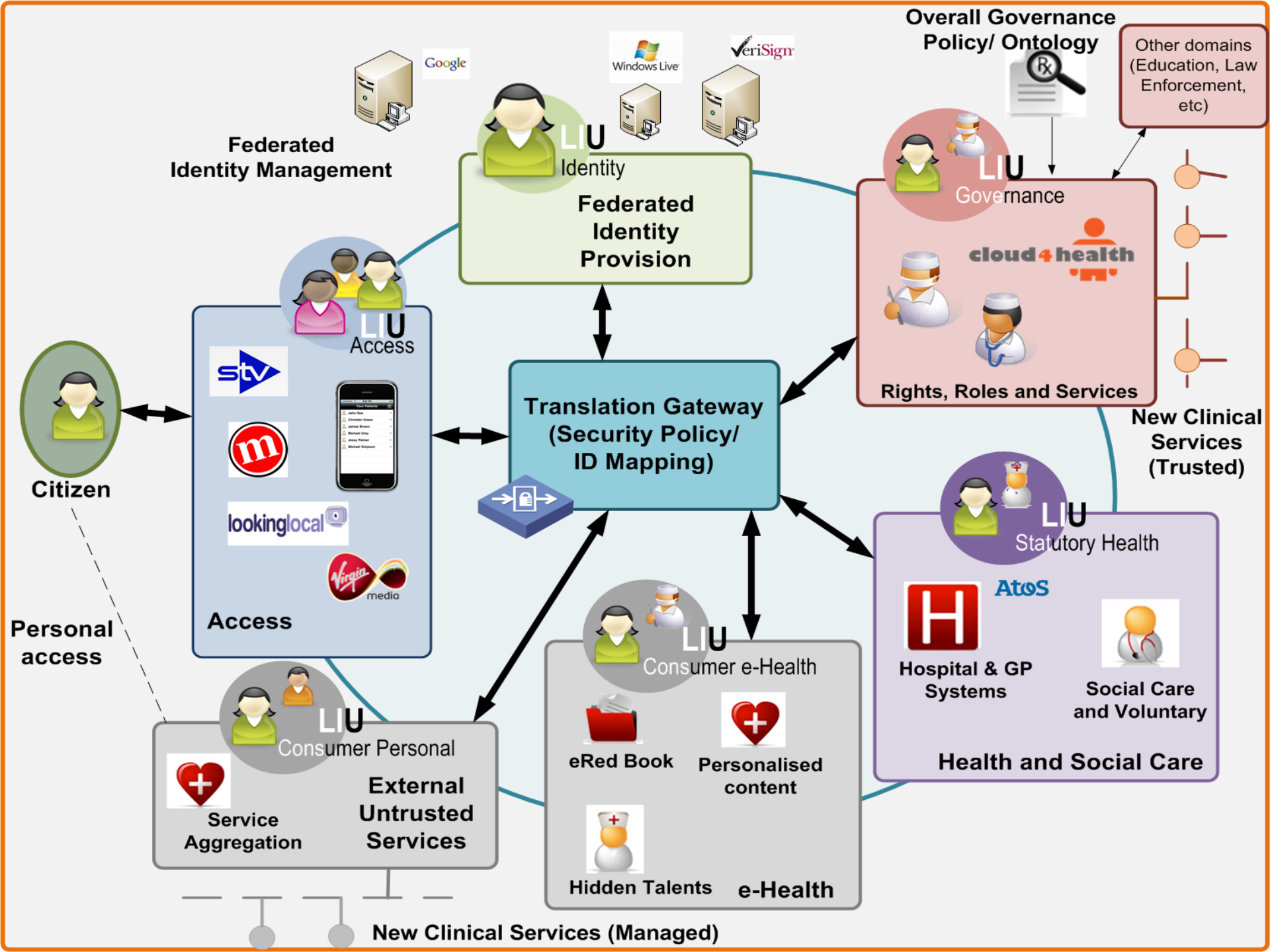
My GP-in-the-Cloud



Data buckets analysed for:

- Clinical alerts.
- Security alerts.
- Malfunction alerts.



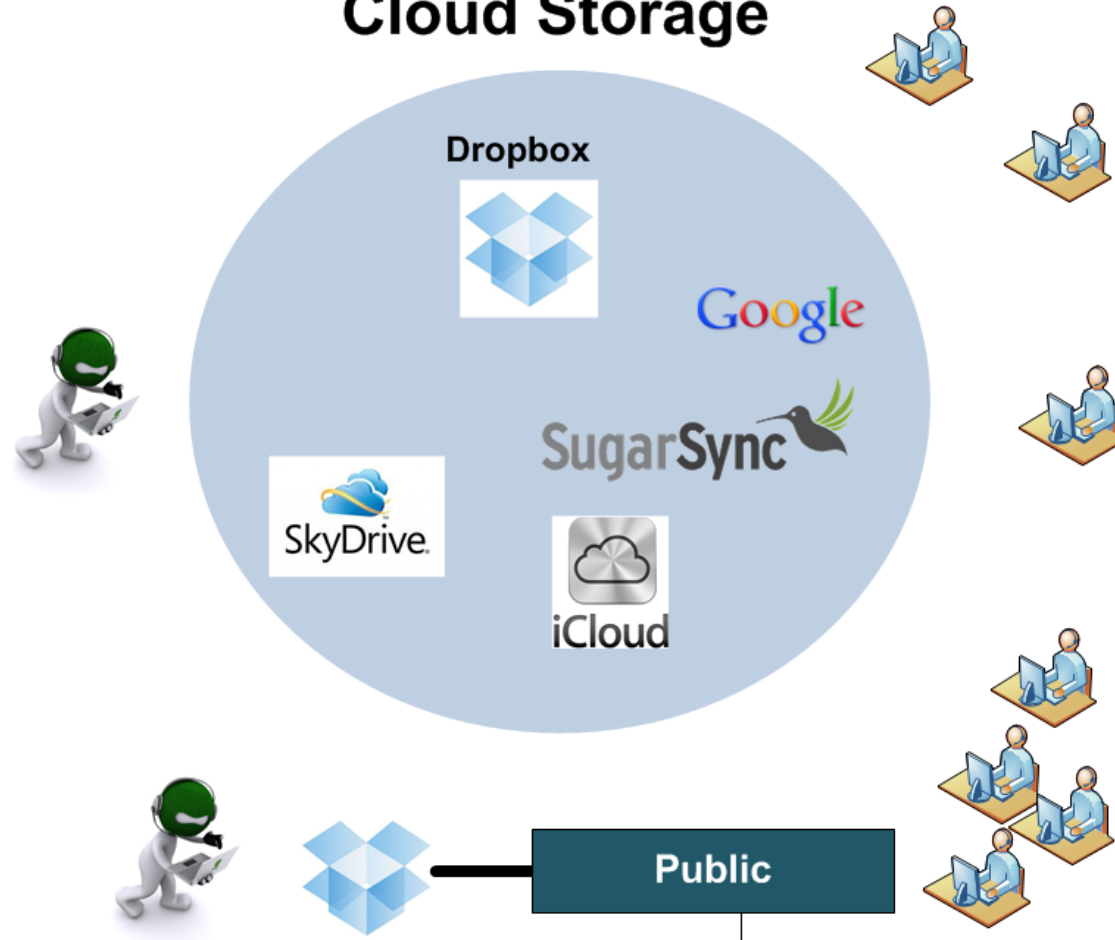


Cloud Environments



- Introduction to the Cloud.
- Cloud and Health.
- Cloud and Teaching.
- New Risks ... new Opportunities.

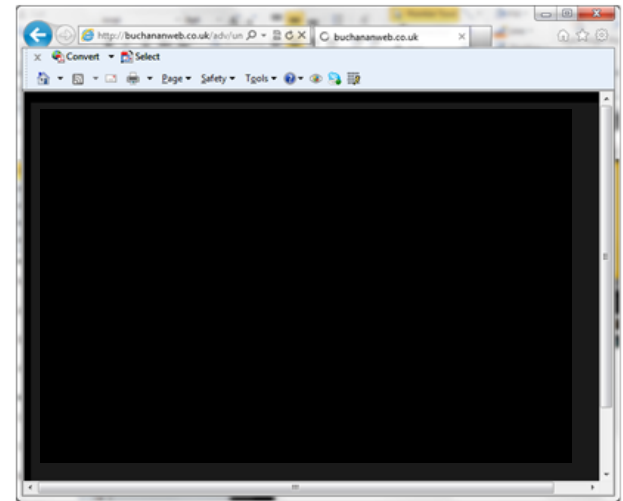
Cloud Storage



https://dl.dropbox.com/u/40355863/2012_june_napier_staff_conference_cloud.pptx



Lecture Capture



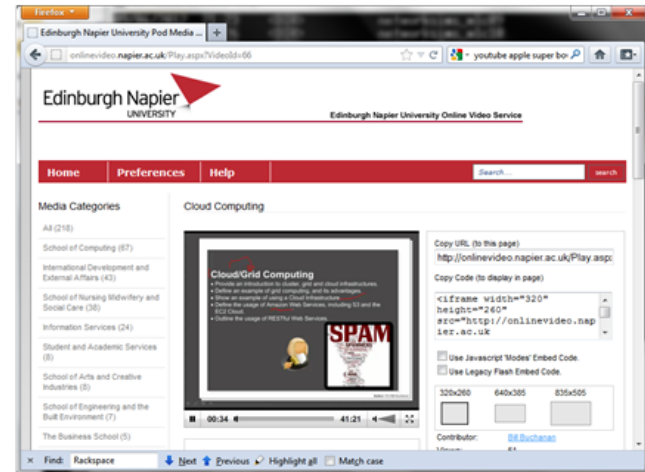
First generation: Export to Flash



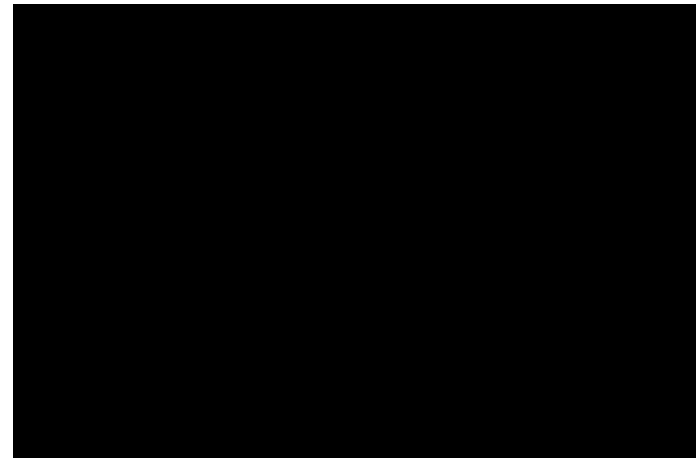
Forth Generation: Mobile



Third generation: Cloud Delivery



Second generation: MP4



Demographics

Top geographies

- United States
- India
- United Kingdom
- Brazil
- Canada

Gender

- Male 83.7%
- Female 16.3%



Discovery

Top playback locations

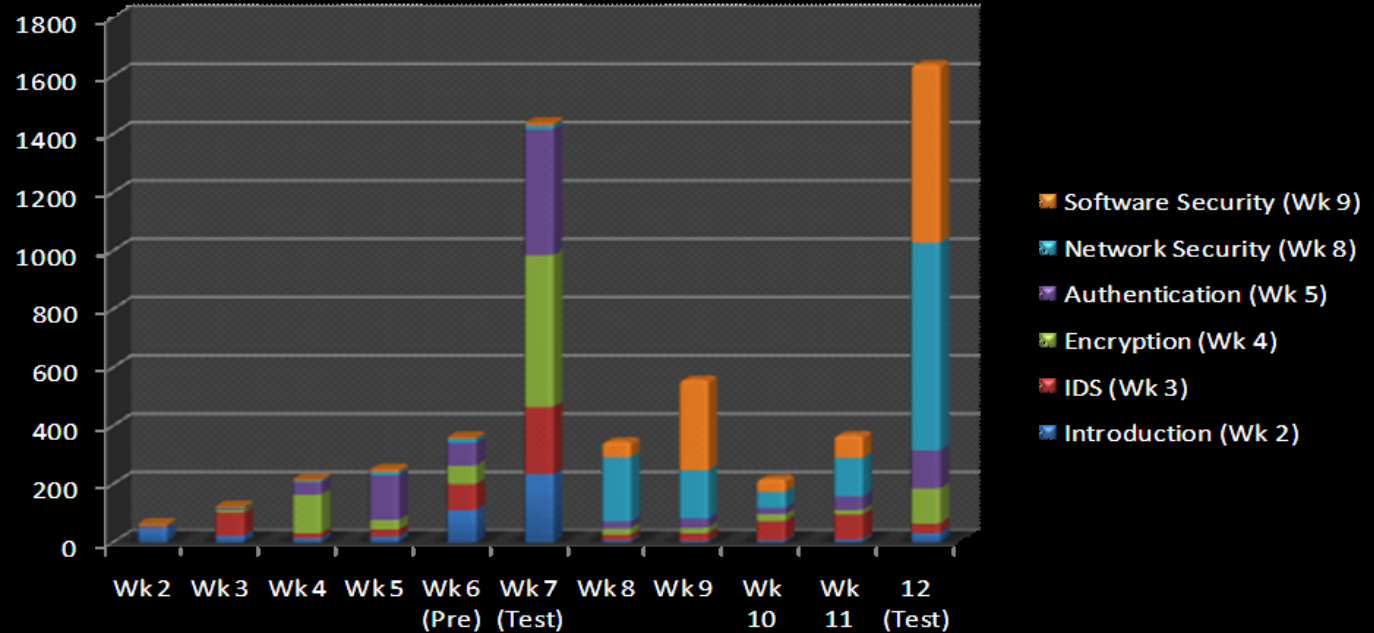
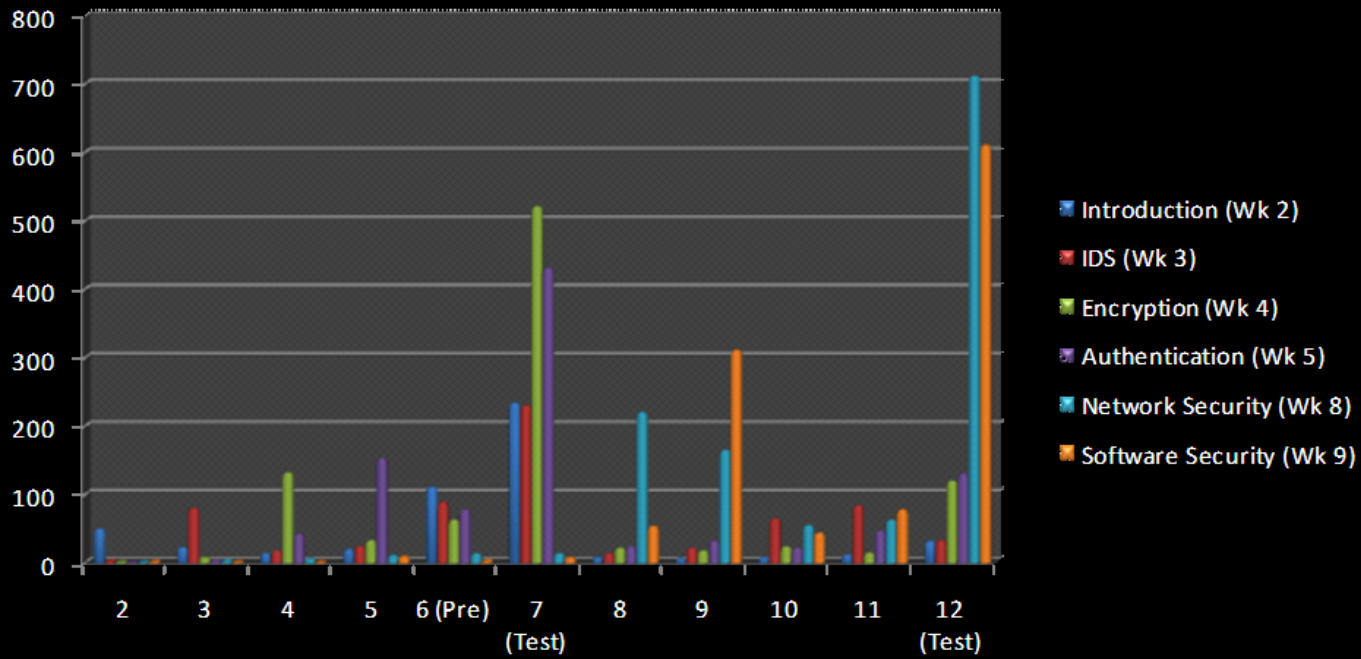
- YouTube watch-page 83.2%
- Mobile devices 16.2%
- Embedded player on other websites 0.6%
- Other 0.0%



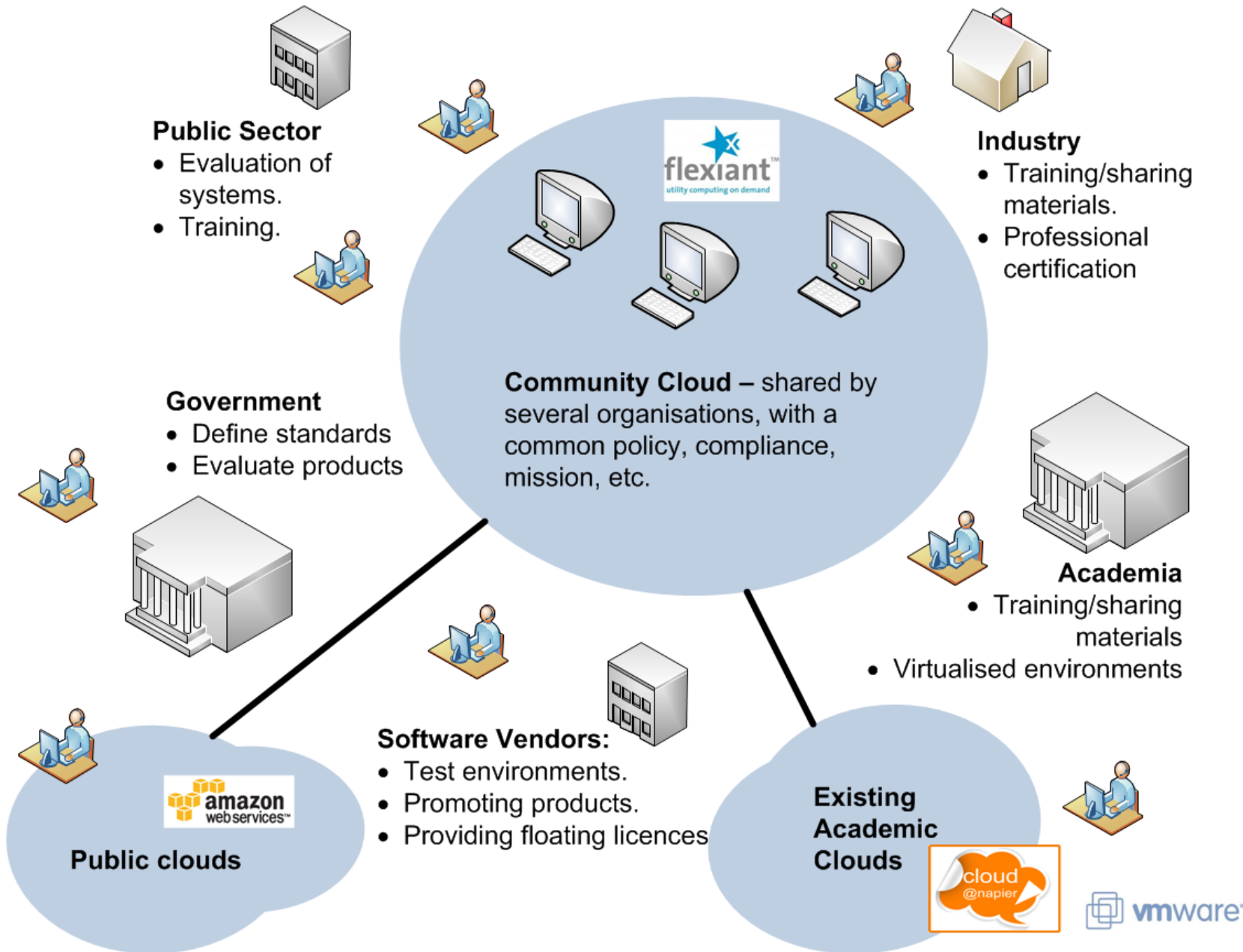
Top traffic sources

- View referrals from YouTube 63.6%
- Mobile apps and direct traffic 32.9%
- View referrals from outside YouTube 3.5%
- Other 0.0%





Online lecture usage





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 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.



Snap-shots of work

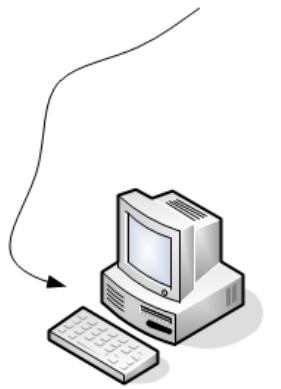
- Student can create snapshots, and move back and forward amongst them.



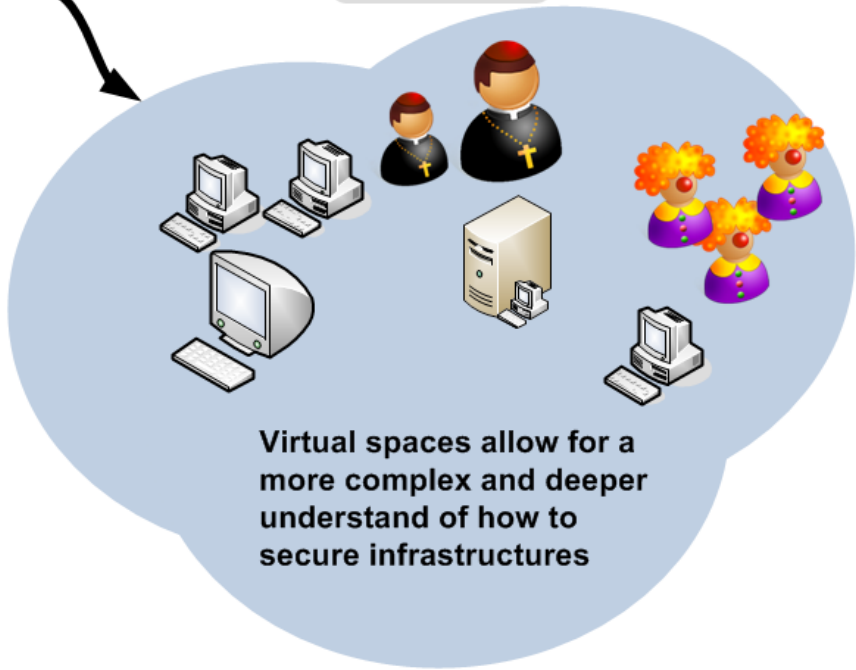


Good...

... Bad



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

Cloud Environments



- Introduction to the Cloud.
- Cloud and Health.
- Cloud and Teaching.
- New Risks ... new Opportunities.

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.



Technological

Social

A cause or a fight?



Who? ... Why? ...
Where? ... When?

- One person's freedom fighter is another's terrorist.
- One person's cause is another person's fight.

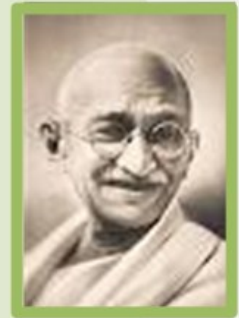
Martin Luther King



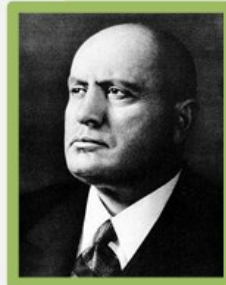
Che Guevara



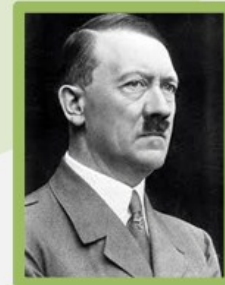
Dalai Lama



Mahatma Gandhi



Benito Mussolini



Adolf Hitler

A cause or a fight?



Who? ... Why? ...
Where? ... When?

- One person's freedom fighter is another's terrorist.
- One person's cause is another person's fight.

Martin Luther King



Che
Guevara

A cause or a fight?



Who? ... Why? ...
Where? ... When?

- One person's freedom fighter is another's terrorist.
- One person's cause is another person's fight.

Martin Luther King



Che
Guevara

Hacktivism



Who? ... Why? ...
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

2012

- Anonymous focus on India on censorship.
- Virgin Broadband over PirateBay block.
- SOCA (Serious and Organised Crime Agency) over arrests, also Norwegian Lottery and Bild.
- Home Office sites over Gary McKinnon case.

2010, Mastercard and Visa

- Why: Decision to stop processing payments to the whistle-blowing site Wikileaks,
- Result: DDoS attacks on Visa, Mastercard, om.nl and politie.nl

2011, Tunisian government websites

- Why: Censorship of the Wikileaks documents
- Result: DDoS attacks against sites. Some Tunisians assisting in these attacks.

2009. Climate Research Unit of East Anglia University

Why: Emails published showed conspiracy to suppress data that contradicted their conclusions on global warming (Russian FTP server)

2011, HBGary

Why: HBGary were going after Anonymous
Reward: Emails published, Web site defaced.

2010, Australian Government.

Why: Australian Government's attempt to filter the Internet.

2012. Department of Justice and the FBI. Denial of service attack

2011. Sony's PlayStation Network.

- Why: Sony were suing Geohotz, who jailbroke the PlayStation 3.
- Result: Afterwards, a group of hackers claimed to have 2.2 million credit card numbers from PSN users for sale



Hacktivism



Who? ... Why? ...
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

2011, Tunisian government websites

- Why: Censorship of the Wikileaks documents
- Result: DDoS attacks against sites. Some Tounisians assisting in these attacks.

2011. Sony's PlayStation Network.

- Why: Sony were suing Geohotz, who jailbroke the PlayStation 3.
- Result: Afterwards, a group of hackers claimed to have 2.2 million credit card numbers from PSN users for sale

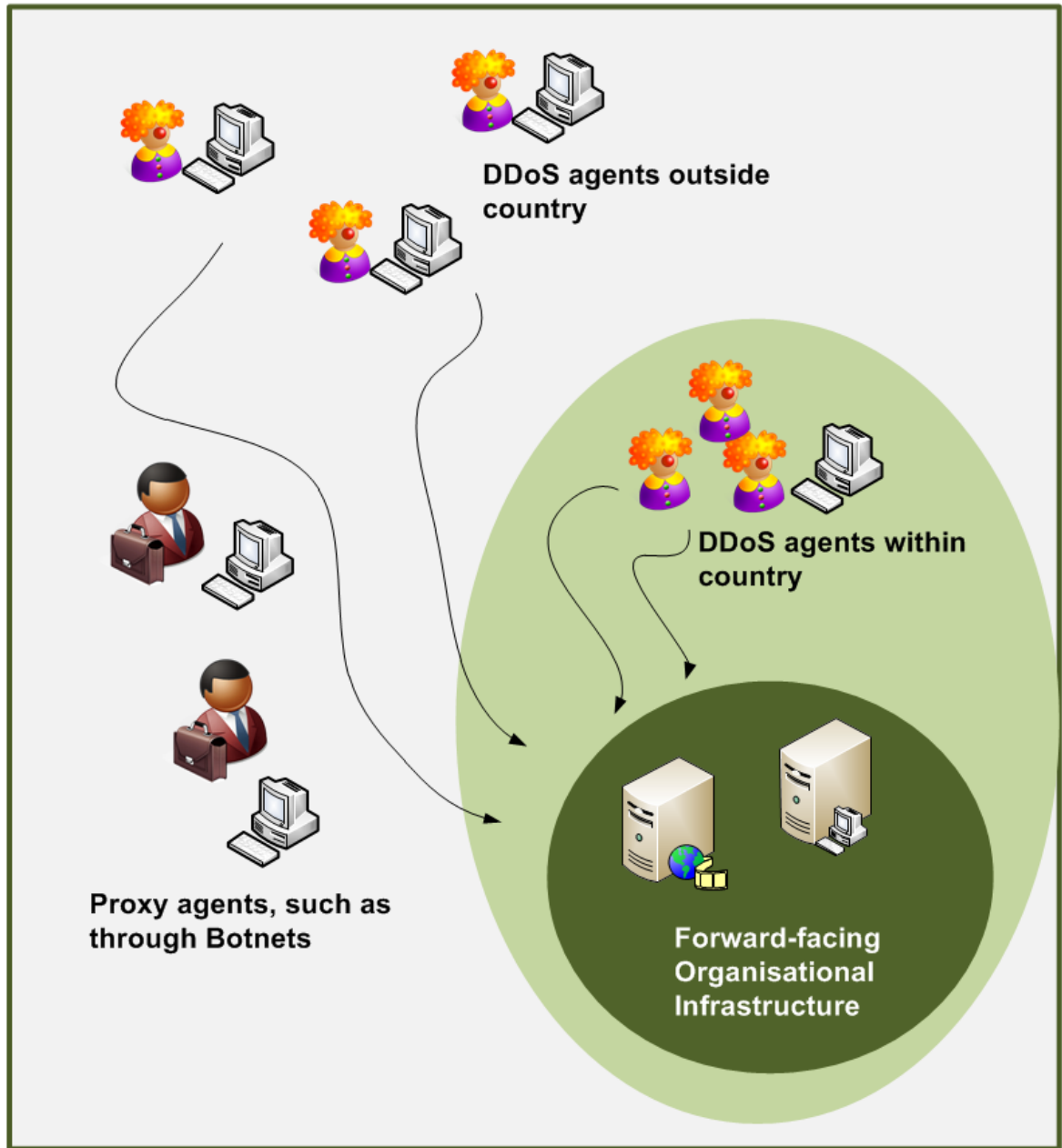


Denial of Service

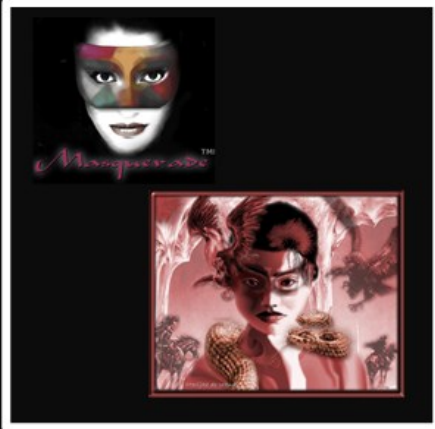


Who? ... Why? ...
Where? ... When?

- DDoS is difficult to defend against.
- Agents often exist outside the country.
- Agents often use proxy agents to perform attack.



Botnet



The army of evil

A study of Torpig over 10 days found:

- 180,000 infections and gathered over 70 GB of data.
- More than 1.2 million IP addresses which contacted the command and control server.
- 8,310 accounts at 410 different institutions, included 1,770 PayPal account, with 1,660 unique credit and debit card numbers.

Control by proxy

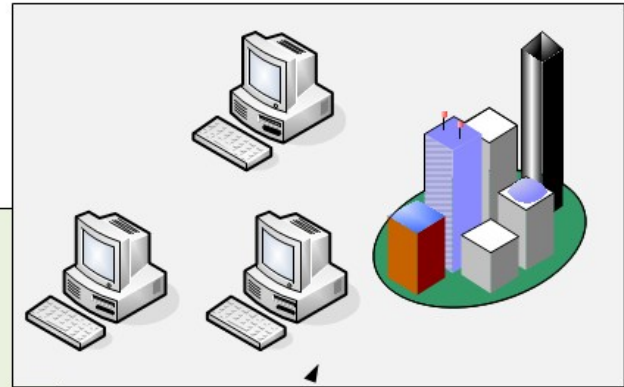
Botnet

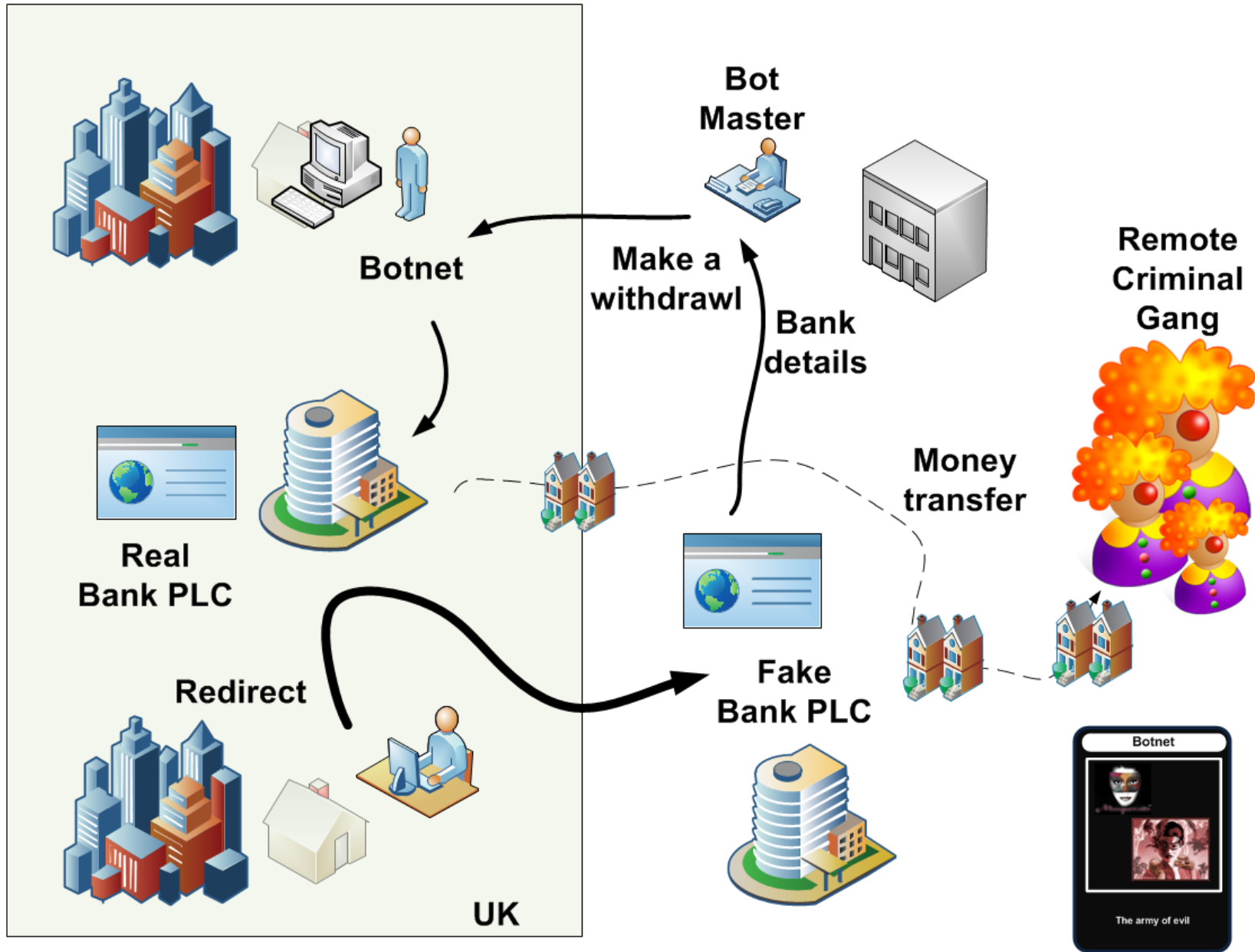


Botnet access

Botnet command

Bot Master





Social Networks



Data Leakage ... and what are people saying about us?

- Open Source Information can often lead to IP Theft.
- Threats against brands and organisations can occur within short time intervals.

Twitter and Facebook

- Company profile.
- IP Leakage.



“XYZ Sucks” Sites

- Bad reputation.
- IP Leakage.

Blogging

- Bad sentiment against brands and organisations.



Organisation Risk?

Poor Affiliate Selling

- Bad reputation.
- Fraud.

Google Hacks

- IP Theft.
- Company Documents.

Rallying Calls

- Fast rallying against brands/organisations.



... increasing **brand awareness** and **improving brand reputation** are often the two main objectives for social media marketing .. So beware of the flip-side ... negative sentiment.



D: e-Perception

- Twitter activity.
- Semantics of external activity.
- Bulletin board activity.
- Blogging activity.
- Geographical presence analysis.

Analysis:

- Twitter Feed rate.
- Semantic Analysis (+2 – foreclosure, loss, attack. fraud ☹; +1 – bad/won't, -1 – good, help, kind -2 - ☺).
- Retweeting activity.
- Geographical Analysis.
- Weighing factors for key domain players (eg BBC).



Huffington Post @HuffingtonPost
Bank of America returns foreclosed home to mother with disabled daughter huff.to/LyHGU1

Expand

6h



Bank of America @BofA_News
#BofA passes 10 mln #mobilebanking customers, marking growth of nearly 3 mln active users in the past year: go.bofa.com/38u5

Expand

23 May




CNBC @CNBC
BayernLB sues Bank of America over losses on hundreds of millions of dollars of countrywide mortgage debt it bought. --Court Filings

Expand

22 May

Respected sources

Black list



The Onion @TheOnion
NEWSWIRE: Man Who Just Received Complimentary Daffy Duck Checks Can't Stay Mad At Bank Of America onion.com/MCDntN

Expand

25 May



ThinkProgress @thinkprogress
Occupy protesters help Los Angeles woman + disabled daughter save their home from Bank Of America thkpr.gs/Jsecvu

Expand Reply Retweet Favorite

25 May



Adryan @Adryan711
Bank Of America is the worst bank ever!

Expand

24 May



Action @BoneKnightmare
Bank Of America Apparently Doesn't Want Credit Card Customers Who Pay Their Cards Off bit.ly/KgYRuu

Expand

19 May

Other sources

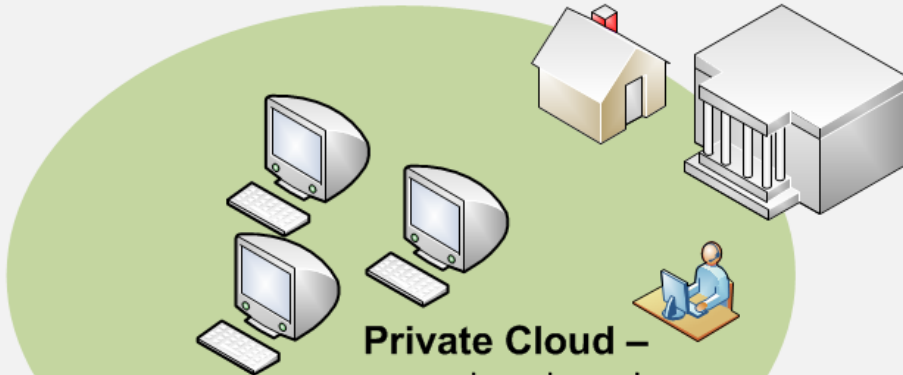
Clouds

RISK

Where is my data?
Where is my servers?
Where are my people?

Can I be compliant with statutory and regulatory requirements?

- Where is my data stored?
- Who handles breach notifications?
- How long is my data stored for?
- How is eDiscovery handled?



Private Cloud – owned and run by an organisation



Public Cloud – owned by an organisation selling a cloud infrastructure



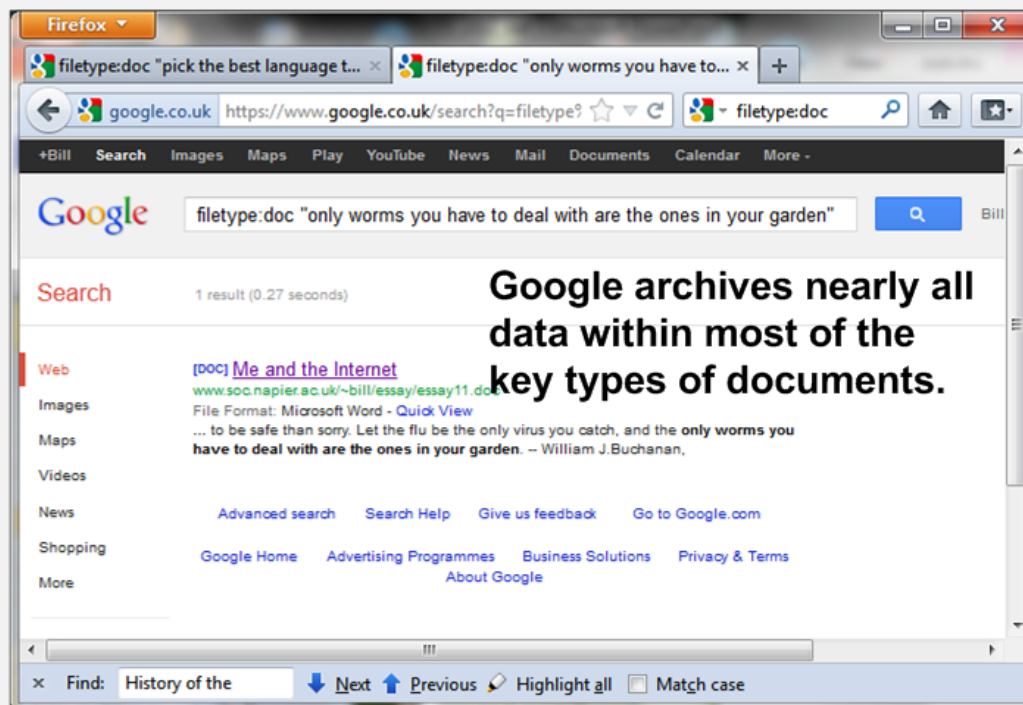
Sharing Applications

Clouds

RISK

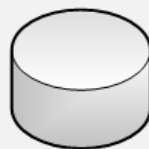
Where is my data?
Where is my servers?
Where are my people?

- Document markings are important.
- Proactive methods required for scanning open source.
- Watermarking required.
- Scanning of on-site documents required to match and documents found.



Google archives nearly all data within most of the key types of documents.

Pre-scan of documents

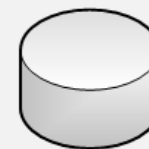


Matching system



Scan for open source documents

Documents found



Open source searches

Cloud Environments



- Introduction to the Cloud.
- Cloud and Health.
- Cloud and Teaching.
- New Risks ... new Opportunities.