



Information Assurance Advisory Council

IAAC

Information Assurance Advisory Council

IAAC

www.iaac.org.uk



Information Assurance Advisory Council

IAAC

Consumerisation Workshop

13 October 2011

BCS Chartered Institute for IT, London

www.iaac.org.uk



Speakers

- Andrea Simmons
 - Managing Director, SPS
 - PhD Student (part-time) at University of Wolverhampton
- Amanda Goodger
 - PhD Researcher (part-time), Cambridge University – information lodestone research programme
 - IA Consultant, CESG, working on 'consumerisation of IT' policy advice & guidance for government
- John Austin
 - Royal Holloway University



Research Programme Intentions

- IAAC will be investigating consumerisation with a view to assessing the risks and impacts of people using their own technology to access corporate information.

“Consumerisation can be fixed, for all of us it is about delivering technology” , James Lyne, Sophos
Quelle Surprise!!!



Workshop Aims

To put together an initial assessment of the:

- Impact on IA of consumerisation;
- Extent to which consumerisation requires a re-evaluation of IA culture, policies and procedures;
- Challenges from consumerisation to established approaches to information ownership, governance, sharing, resilience, confidentiality, identity assurance and other accepted norms;

And ultimately:

- refine the following workshop themes and identify further workshop topics.



Definitions

-the introduction of consumer-oriented technology and behaviours into the realm of Enterprise IT.
-the growing trend where business users are making the ultimate choice in what devices, applications, and services they use to get their work done.
- Consumerisation is a stable neologism that describes the trend for new information technology to emerge first in the consumer market and then spread into business organizations, resulting in the convergence of the IT and consumer electronics industries, and a shift in IT innovation from large businesses to the home
- The increasing influence that our technology experiences as consumers - both hardware and applications - have on the technology that we expect to use at work.
-part and parcel of all these offerings and enabled by the cloud and virtualisation.



Bring your own device

- More mobile phones than people on the planet next year
- 6.8 billion by the end of 2012
- 62.5 million mobile phones in Britain
- China & India more than 1 billion subscriptions
- “Unlike toothbrushes, mobile phones and devices are inclusive” [Metro, Friday 7 October 2011]....?!!
What are the media on about?! And as one contributor pointed out, having more mobile phones than toothbrushes as a planet is not necessarily something to be proud of....!
- Few of the under 30s wear a watch to tell the time – they use their phone instead





The reductive view

- IT is the world's worst industry for repackaging ideas
- Consumerisation is just about another technology purchasing decision to be made/handled (Jo Stanford, Group IT Director, DeVere Group)
- Users have been using private devices professionally for years, ever since laptops started to replace corporate desktops
- BYOD etc is a maturation of 'deperimeterisation' – from 2004 to now – evolution, not revolution



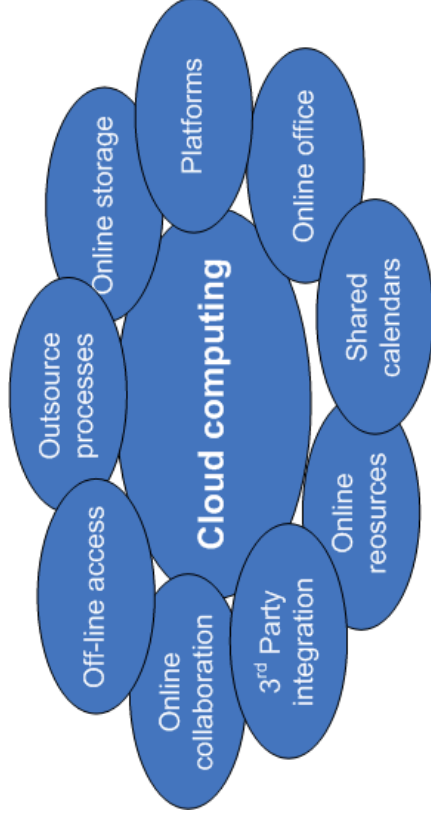
Historically speaking

- IT has been left to “support” users when it has been difficult to get corporate applications to operate on their home machines
- IT used to have to deal with one OS that changed every 3 to 5 years; now IT has to deal with a new platform every 6 months over many OS
- Now moving from focussing on the device to focussing on the platform



Cloud Computing

- **Cloud Computing** is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST)





Information Overload

- We now produce the same amount of information in a single week as we did in the whole of 2002 – 23 billion gigabytes
- We have moved from **information scarcity** to **information glut**
 - Ceaseless bombardment of emails
 - Voicemails and texts
 - Numerous social networking and ‘friend’ requests
 - News alerts
 - Management reports and industry updates
 - Apps
- This has led to **information anxiety**



So what does consumerisation look like?

- Using your iPhone to access your e-mail
- Using Facebook to communicate with colleagues
- Sending that file using your Gmail account that was too big to be sent from your Outlook mail
- Using a tablet PC you purchased because its lighter, more flexible and you “like it better”
- Doctors are using tablets to show patients their x-rays





Benefits

- Employees are more productive using devices with which they are comfortable
- Staff morale improves because they can use their gadget of choice
- Procurement generally spends less resources to constantly re-equip employees with the latest technology because they are upgrading themselves

Consumerisation = happier staff +
increased productivity + high revenues
Consumerisation = a security headache



Risks

- Consumer gadgets used as storage devices could bring malware into the network - ultimately this is the same risk as has existed since everyone started using floppy disks
- Users have a low tolerance to security controls – the more there are, the less likely users are to want to use the device and the more likely they are to work around the controls
- Companies need to understand the risk they are taking on, the liability and the accountability of their employees behaviour through their networks whilst using their own equipment





Risks

- Risks of data leakage and data loss will increase and the likely reputation exposure as a result of a rogue email escaping the organisation will certainly be higher
- Risk of £500,000 fine from the ICO as a result of a serious data breach
- Bottom line - if you are using a personal device with company data, **you are responsible for it and hold the risk** – what was and what can be accessed.
- Workers using social media – you need to be able to audit activity to protect your brand and reputation



What has gone wrong?

- A CEO of a well-known Irish bank was sacked for exceeding the limit of acceptable personal use of his bank-funded Internet facilities. Whilst on a business trip, sitting in his hotel and using his bank-provided laptop, he browsed some escort-related web sites... He lost his job.
- A mayor of a large US city landed in a controversy when more than **14,000** text messages exchanged with one of his colleagues, with whom he had had an illicit affair, became public (*act of moral turpitude*)
- Employee quit a law firm, her previous boss wrote an email to his colleague stating that she could be replaced with a 'busty blonde'. The person who left got hold of the email and the company had to pay £ks in damages.
- Gmail email loss story - <http://bit.ly/r8lupQ>



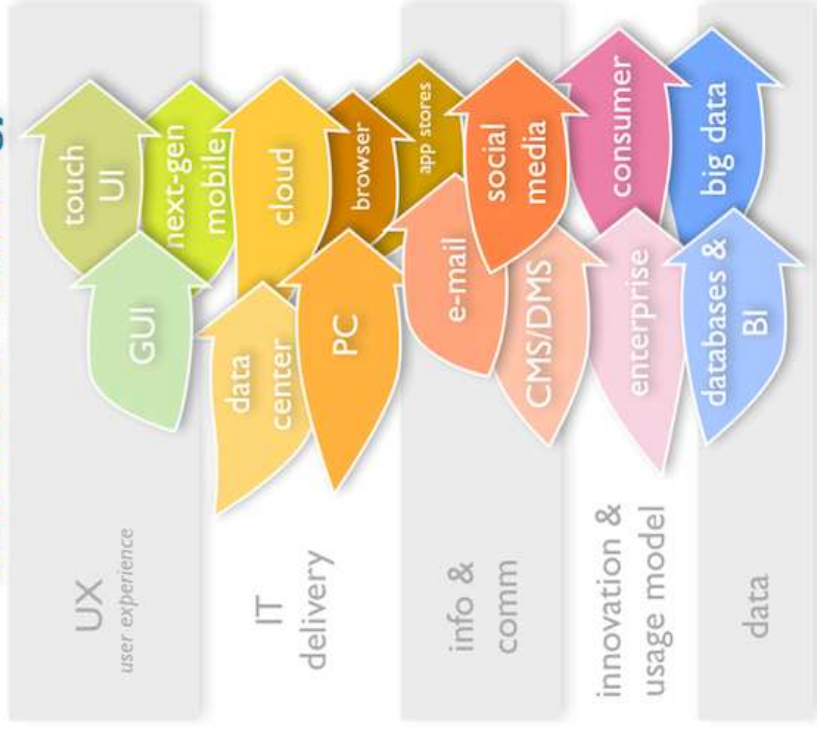
Buy your own device

- Consider this – employee loses their device; the device had 100s of their own photos on it; sensibly employer deploys “remote wiping” service to the lost device.... Employee considers suing employer for loss of photos.... 😞
- Need to manage expectations
- Address legal issues
- Thus, need a policy
- Policy must cover support and maintenance
- Citrix programme....
- Tax breaks – a company can buy an asset to use at home and rent the device to the user, much like the cycle to work scheme – but at least IT can operate programmes that are to the benefit of the user, including anti-virus, doing the patching, blocking infected websites and not compromising the experience whilst still protecting the data



The shifting sands of time

The Major Shifts in 21st Century Information Technology



Iphone and Android devices will be the next big target for malware and man in the middle attacks.....

From <http://izdnet.com/blog/hinchcliffe-on-20-net>



IAAC definition

- Information Assurance is the certainty that the information within an organisation is *reliable, secure and private*. IA encompasses both the *accuracy* of the information and its *protection*, and includes disciplines such as information security management, risk management and business continuity management.

IAAC Report, February 2003, Engaging the Board – Corporate Governance and Information Assurance

- Information is fundamental to the business of government. Effective IA is core to ensuring that this asset is safeguarded appropriately. The continued growth throughout government in the use of ICT systems, all linked together, carries with it increased vulnerability. In addition these ICT systems are under threat of attack from foreign intelligence services, criminal gangs, and even individuals inside the organisation.



Putting it all together (c. 2006)

- **Information Assurance is the confidence that the information assets within an organisation are reliable, accurate, secure and available when required.**
- Information Assurance:
 - includes information held in every form (information systems, on paper, other records)
 - is underpinned by a management process that takes a co-ordinated approach to information assets across an organisation.
 - embraces information management – including information security management, information and records management, data protection, privacy (close confidentiality links and Organization for Economic Co-operation and Development [OECD] guidance requirements) and physical protection
 - includes aspects of: – corporate governance – risk management – business continuity
 - must be maintained throughout an organisation's lifecycle in the face of changing threats, vulnerabilities and dependencies.



Consumerisation and IA

- Enterprises will need to
 - decide whether to ignore it or embrace it
 - work out what information can be shared by whom and with whom, through what channels
 - control access to sensitive data ensuring that only authorized people gain access to the data
 - verify that the data is only being used for the purpose intended
 - discover and document what data types they have (asset inventory), where it is stored and where it travels to
 - validate that the data is not compromised
 - insure that no one is altering the data
 - comply with auditor requirements
 - provide proof of data protection compliance



Key concerns

- Data has been moved beyond the secure boundaries of a network
- Knowing
 - **what** you've got
 - **where** it is – the main challenge for many folk (especially public sector)
 - a mountain in Montana?
 - **who** has it
 - **when** you need it, where to go to find it
 - **how** long you need to keep it for
 - that it is secure
- Most people are blurring work and play – and this is only going to get more blurred over time
- Dealing with apps that are out of bounds is tricky (Apple and Google will never say no to an app....)



Questions You Can Ask:

- Application interfaces will need to be dynamically rendered and optimized for the resolution and UI of the client device; which will result in requirement for more edge computing capability for presentation layer.
- How can organisations ensure that their users have access to the same applications and data no matter where they are, regardless of device?
- Is your organisation shifting from fat client computing models creating an entirely new set of workloads to manage, new demand to balance, and still deliver on SLAs?
- How do you manage application and infrastructure maintenance when access via mobile devices is around the clock?
- Is your organisation prepared for the proliferation of devices with multiple standards to support?



Questions You Can Ask:

- Is your data centre ready for an increase in transaction load as employees have broader access to core enterprise apps from any device?
- Have you considered how you might leverage the use of next generation mobile devices and social computing and the impact that has on your IT capabilities and critical core business applications?
- How do you engage with your customers today? Have you considered how to use social media and social computing to provide better customer service to your clients?
- Are you taking advantage of the advanced capabilities of mobile devices to provide better customer and employee service?



Questions You Can Ask:

- How often does your organisation monitor for data losses/leaks? What is the game plan once there is a leak – communication, plugging the leak etc.? How do you prioritize.
- How does your organisation ensure that data is not compromised and that unauthorised people are not accessing and altering the data?
- How does your organisation control access to network resources and ultimately authorise access to the data?
- Has your organization developed the necessary training requirements and acceptable use agreements for the use of mobile devices and social applications?
- What security tools does your organisation use for audit compliance?



Questions You Can Ask:

- Does your organisation have the ability to identify and manage all mobile devices, including employee's personal devices used for work?
- Can your organisation provide end users reliable access to information anywhere, anytime without sacrificing performance, business agility and the security of your data?
- How does your organisation provide technical support to employees who use their personal devices?
- How will your organisation get in front of the support needs of all their end users in the campus, branches, home offices and hot spots while consolidating the multitude of vendors they have to manage?



Solutions are available

- User education – the first line of defence! Clued up employees are less likely to make mistakes 😊
- Secure access controls
- Remote wiping capabilities for devices that out-of-policy, non-compliant, active threats, lost or stolen or at a user’s employment termination
- Virtual desktop images (Citrix Thin Client etc) / decent sand boxing – providing a “work” and “play” environment
- Policies – inclusive, non offensive, not draconian
- Products
 - Security Incident and Event management (SIEM) products
 - MobileIron - <http://en.wikipedia.org/wiki/MobileIron>
 - Zenprise - <http://www.zenprise.com/>

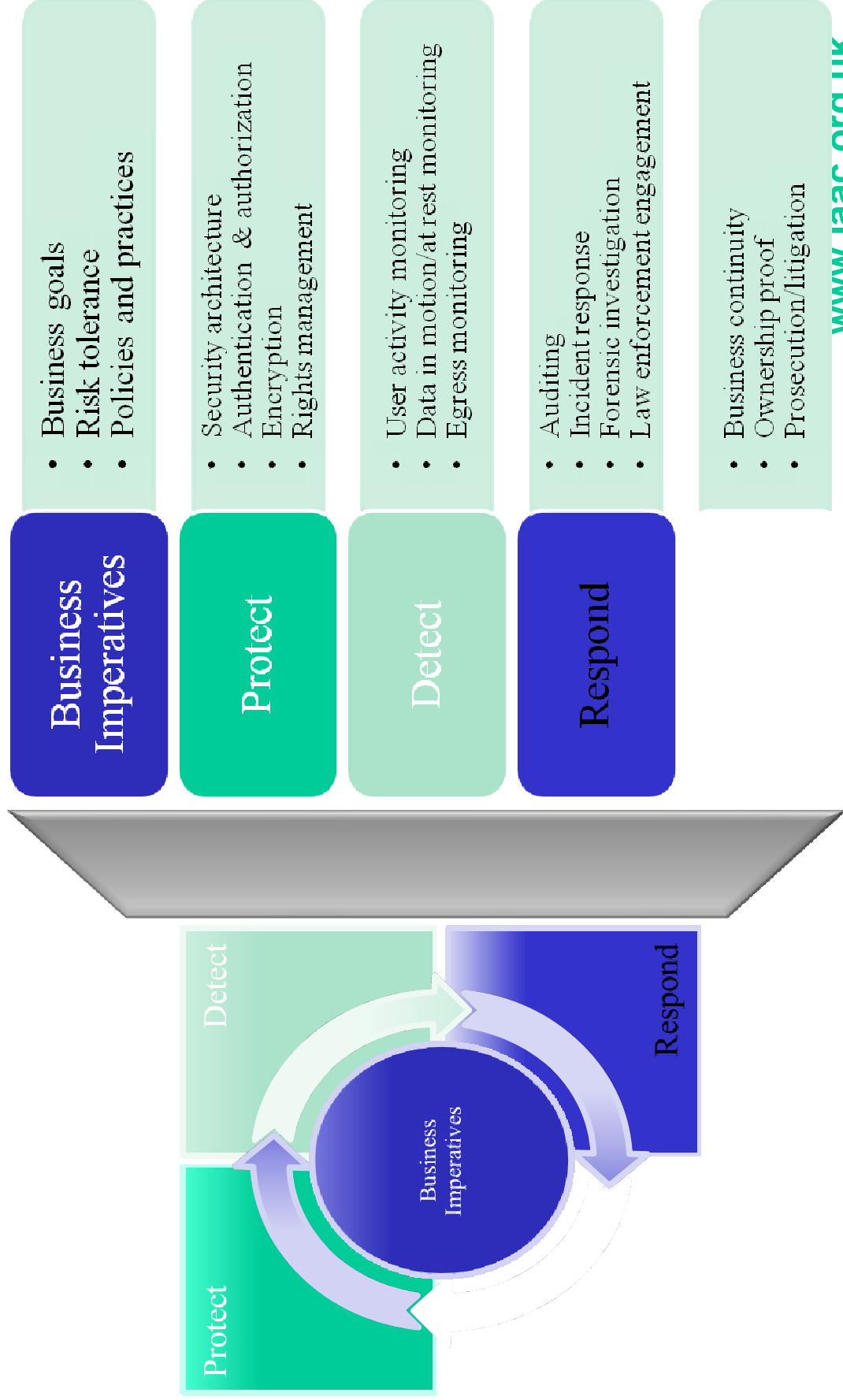
Automation is the only possible way to manage the explosion of mobile devices



IAAC

Information Assurance Advisory Council

MSI: Defense in Depth





Key policy elements

- Personal use of business-owned or business-provided resources must not involve something **illegal** or **unethical**
- Usage must not result in loss of productivity
- Any act of personal use of company equipment must not result in excessive consumption of other resources – not relevant in *all* countries
- Any act of moral turpitude using company resource is unacceptable
- Be clear about the expectation to privacy an employee will have if they use their own device to connect to the network
- Also consider health and safety issues – using small screens and keyboard for long periods.....



Future IT/IA approach

- Determine the level of support to provide for personal devices
- Determine what will happen if the employee leaves or a if a device is stolen or lost
- Monitor the integrity of mobile devices to ensure they start and stay in a known trusted state
- Enforce the use of access control systems when working with any company data or network resources
- Encrypt the device to protect data in the event the smartphone/device is lost
- Apply standard defence-in-depth security concepts
- Consider the future mobile payment threat landscape....
- Can IT become the driver of business or will the function be absorbed by lines of business as their leaders become digital natives?



Workshop Aims

To put together an initial assessment of the:

- Impact on IA of consumerisation;
- Extent to which consumerisation requires a re-evaluation of IA culture, policies and procedures;
- Challenges from consumerisation to established approaches to information ownership, governance, sharing, resilience, confidentiality, identity assurance and other accepted norms;

And ultimately:

- refine the following workshop themes and identify further workshop topics.



IA issues feedback (1)

- Enlightened leadership
 - Individuals, SMEs and corporates
 - Generic output
 - Decision making addressed
- Agility – need to enable protection within the products
- Interdependencies
- Interconnectedness
- Value systems?
- CSR
- Control and governance – collective impacts?
- Understanding the needs from cradle to grave (including the parents in the middle
- We live with and in risk



IA issues feedback (2)

- Valuation of data
 - Younger generation happy to “get it out there”
 - How do we value it?
 - And thus how do we protect it?
- Trust – eroded currently?
 - From business controlled device to personal?
 - SSL, bugs etc – what can we trust in terms of infrastructure?
 - Can we only trust the data?
 - Trusting the data on untrusted infrastructure?
- Unintended consequences of aggregation
 - Open data environment – different data sources revealing different things



IA issues feedback (3)

- **Trust**
 - Can we trust the device – it's point of origin/manufacture
 - Loss of control by information asset owner once the asset moves onto a consumer device.
 - IP ownership?
 - Keeping own device/handling it back in?
 - Need to educate what trust means
- **Authentication**
 - Four digit pin – not quite good enough?!
 - Cloud principle – more access from the consumer consuming – how trusted is the grey sphere
- **Freedom of Information**
 - Big Data / right to know versus need to know etc
- **Discipline – corporate vs personal**



IA issues feedback (4)

- Data tagging
 - Little info really needs protecting – reduce demand on technologies
 - Increasing demand on responsibility
 - Tangible consequences? Financial/social?
- Trust
- Identity
 - Information with different security circumstances and requirements



Information Assurance Advisory Council

IAAC



**Systems
Dtex**

Level(3)



NORTHROP GRUMMAN



pwc



The Security Division of EMC

SOPHOS



symantec™

UNISYS
imagine it. done.

www.iaac.org.uk