

## IAAC 2011-13 programme: 15 February Workshop Governance and Consumerisation

### **Updated context:**

Since we began focusing on Consumerisation in October 2011, the pace of change has not stopped. Apple's iPhone business is now worth more than the *whole* of Microsoft. Think on that...

We are operating in a veritable "Information Spring" and our journey so far is taking us all beyond our own bounds of experience, knowledge and understanding, to a certain extent. The way we interact with our devices, each other, our employers and our governments is changing beyond all recognition and so Governance and how we imagine it should be shaped has a huge role to play.

### **"consumerisation" transforming...**

"Bring your own device" (BYOD)/ Consumerisation, is about a belief in the power of the individual user to choose their own working conditions and operating environment. However, if this is to be the case, then they will need to understand what it means to take ownership of and responsibility for:

- Data storage, including emails, spreadsheets, documents, presentations etc. which will cause problems for 'legal discovery' identifying what has been done on behalf of the organisation;
- Information classification – in order to be able to identify what is personal information, and how it is to be excluded from storage, transfer, usage etc; other data types including GPS tracks, photos etc may also be subject to discovery

The growing integration of devices and services needs to be understood and scoped. Smartphones and other personal mobile devices may be synchronised with a home PC; users may be utilising services such as Dropbox etc; they may also, in the mid term be using their TV for remote access. Their phone may have been plugged in to an in-car display system. All of these situations will make it hard for organisations to know where their information has gone, even if the user is still working for them, and, of course, produces a very large attack surface. There are implications for both the individual and the organisation with regard to managing this future.

### **What needs to be Governed?**

**Information assets** – but the organisation may not know that the devices exist. The following are a list of potential challenges for which solutions will be required in this space:

- *if you provide remote access users will set up all their devices to talk to it;*
- *you can't insist on a particular make/ software/ configuration;*
- *you can't insist on central or standard management;*
- *you can't be sure whether support is being done by a trusted third party or a friend in the pub;*
- *the user is likely to have admin rights;*
- *you may not be able to install standard security software (the licence may not allow for it?);*

Sponsors:

Registered Number 04326237



- *the device is likely to be shared with family (?friends too);*
- *the user is likely to want to download own software (applications etc);*
- *the user is likely to want to store their own data (e.g. the address book will be a mix of personal and business information);*
- *bill management may require changing from the present structures and limits;*
- *if the organisation is using remote virtualised desk-tops, who "owns" it? The user may be using a corporate laptop or mobile device to gain connectivity and optionally private use may be allowed by users who are told that the equipment belongs to the organisation, which retains the right to monitor and forensically inspect them; but if the device is NOT owned by the organisation, if it is seized by police or bailiffs in a civil case, who has authority to conduct analysis or denial of access to a hard disc?*
- *remote monitoring/wiping may be available technologically but may not be culturally acceptable – this will definitely need a strong strategic governance steer;*
- *the user will want to keep it when they leave;*
- *the device(s) probably can't be wiped or destroyed properly either when they leave or when they are replaced (the user probably wants to pass it to their children..... ☺)*

There is a different risk profile for smartphones/mobile devices and this will need to be understood. They have almost the same capability as a laptop but are much easier to lose or have stolen and are less likely to use encrypted storage/communications channels.

Completely tangentially to all of the above, what about the retrieving of privacy and identity data following its release? For example, you give credit and travel details to a travel company, they seek a deal for you by passing those details to other companies seeking best offers. How do you retrieve your details from those third parties?

## **This Workshop**

Our aim at this fifth workshop of the IAAC Consumerisation Programme is to look at the Governance requirements for addressing consumerisation.

The workshop will aim to answer:

1. What should government do for public sector?
2. What should private sector/Centres of Excellence do for their 'parishes'?
3. What other solutions/controls are available to assist in delivering Governance?
4. What is academia's role here - how can they provide inputs that would be fast-to-market?

The end game is to fulfil a need to create a Good Practice Guide (GPG). As IAAC already produces the IAAC/DIAN Directors' Guides, we may just add in an extra page on this. This would hit our main target audience and should complement any Busy Readers Guides issued by CESG on the subject of Consumerisation.

Andrea C Simmons, 7<sup>th</sup> February 2012

Sponsors:

Registered Number 04326237

