

## Consumerisation – What are the IA Issues?

### Objectives

The objectives of the first workshop in the 2011/2012 Consumerisation Research Programme, held on 13<sup>th</sup> October 2011 in London, was to provide an initial assessment of the:

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

### Introduction

Consumerisation has been both a growing visible trend in organisations during the past 24 months and a subject of increasing rhetoric in all the IT related press, media and research. In 2009, Osterman Research forecast that “the proportion of the North American workforce equipped with employer supplied mobile devices will double, from 23% in 2008 to 46% in 2011.”<sup>1</sup>

Available definitions of consumerisation were provided within the pre workshop paper, available [here](#). Whereas there is no single definition, the emphasis in this paper is on the use of an individual’s own personal devices for work, with technical support from the workplace. This paper looks at some of the key issues, the interdependencies and interconnectedness of information risk management in relation to the ongoing encroachment of the use of personal mobile devices in the workplace.

The IT industry has a reputation for repackaging ideas; users have been using private devices professionally for years, ever since laptops started to replace corporate desktops. However, today’s environment is one of increasing pressure, decreasing resources and revenues and an ever expanding volume of information. Current information overload is creating a level of stress and tension - being referred to as *information anxiety*<sup>23</sup> - for our beleaguered workforce. Workforce stress affects the provision of effective information security awareness programmes as we need to bear in mind the culture and the motivations of the workforce when designing these to achieve the best outcome. We have *information glut*<sup>4</sup> - an issue relevant to those who portray consumerisation as being a positive benefit for both the organisation and its employees.

There are, as always, two sides. On the one hand, consumerisation – in the sense of allowing employees to utilise their device of choice - is believed to make for happier more productive staff, thus generating higher revenues. However, there is obviously the reality that consumerisation brings with is a new set of security challenges.

There is plenty of information based research available online that can point the reader to statistics galore. Apparently, we now produce the same amount of information in a single week – c. 23 billion gigabytes - as we did in the whole of 2002.<sup>5</sup>

<sup>1</sup> [http://zenprise.surprisehighway.com/assets/OR\\_white\\_Paper\\_final.pdf](http://zenprise.surprisehighway.com/assets/OR_white_Paper_final.pdf)

<sup>2</sup> <http://www.samberner.com/documents/KM/infoglut.pdf>

<sup>3</sup> <http://www-cs-faculty.stanford.edu/~eroberts/cs201/projects/technorealism/manage.html>

<sup>4</sup> <http://www-cs-faculty.stanford.edu/~eroberts/cs201/projects/technorealism/glut.html>

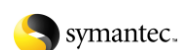
<sup>5</sup> <http://www.managementtoday.co.uk/features/1094844/Chartered-Management-Institute-Combatting-techno-phobia/>

Sponsors:

Registered Number 04326237



NORTHROP GRUMMAN



SOPHOS



## Bring your own device (BYOD)<sup>6</sup>

During October 2011, the world reached its 7 billionth birth – and yet already it is anticipated that there will be 6.8 billion mobile devices by the end of 2012 – which will amount to almost 1 per human being across the globe. The UK is already at saturation in terms of, by volume, appearing to be at a ratio of 1:1. China and India have more than 1 billion subscriptions. The scale of all this is phenomenal, as is the growth.

It is interesting to note that part of our research into consumerisation and its trends unearthed the finding, as reported in this [article](#), that few of the under 30s wear a watch to tell the time. They use their phone instead. However, as is often the case, a corollary could be found - watches can become a way of expressing oneself.

Either way, there is a younger generation, the ones for whom many of us will be designing policy and reworking our ICT strategies to support, who are:

- using their iPhone to access corporate e-mail;
- using Facebook, LinkedIn and Twitter to communicate with colleagues – both across and upwards;
- sending files using cloud hosted webmail accounts, particularly when they have large files that the corporate (Outlook) mail system won't forward;
- using a tablet PC they purchased because its lighter, more flexible and they “like it better” etc.

BYOD is a maturation of ‘deperimeterisation’, spanning some seven years or more. It is really more about evolution, than revolution, but at internet speed.

## IA defined

IAAC has been seeking to provide advice, guidance and influence in the arena of information asset protection for over a decade. The combined wealth of experience has led to a much broader and deeper understanding of what Information Assurance (IA) fully encompasses.

Information Assurance is the confidence that the information assets within an organisation are reliable, accurate, secure and available when required. It

- includes information held in every form (information systems, on paper, other records);
- should be ‘owned’ at Board level;
- should be 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 (because of close confidentiality links and Organization for Economic Co-operation and Development [OECD] guidance requirements) and physical protection;
- includes aspects of corporate governance, information risk management and business continuity;
- must be maintained throughout an organisation’s lifecycle in the face of changing threats, vulnerabilities and dependencies.

## Key concerns

Bearing the above comprehensive definition of IA in mind, there are a number of key information related concerns when considering the impact of consumerisation both on our workforce and in our workspaces.

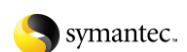
<sup>6</sup> <http://www.webopedia.com/TERM/B/BYOD.html>

Sponsors:

Registered Number 04326237



NORTHROP GRUMMAN



SOPHOS



Most people are blurring work and play – and this is only going to get more blurred over time. IT departments have been left to “support” users when it has been difficult to get corporate applications to operate on their home machines. Now users have migrated from using mainly business controlled devices to a greater emphasis on the use of their own personal – and in particular handheld - devices. IT used to have to deal with one operating system that changed every 3 to 5 years; now they have to deal with a new platform every 6 months over many OS'. The infrastructure and landscape is moving from focussing on the device to focussing on the platform – in other words, the IT departments are having to tackle the integration of many fast changing and updating OS platforms with legacy systems, seeking to ensure availability of systems for users on an “anytime, anyplace, anywhere” basis. This will be particularly difficult to manage in a small business environment where IT may be outsourced, or the internal team may be very small with a narrow skillset. For some, the easiest technical solution may appear to be moving data to “the cloud”. As a result of this, the data has been moved beyond an organisation’s current secure boundaries. Dealing with apps that are out of bounds is tricky (Apple and Google will never say no to an app).

Those responsible for providing information asset protection will need to know:

- what they’ve got
- where it is (which cloud/jurisdiction etc)
- who has it
- who uses it - the family? Also friends? Or just the “owner”?
- when they need it, where to go to find it
- how long they need to keep it for
- and that they are secure to the level capable of the specific device (throughout their lifecycle, including at their end of contract term or life – i.e. how is data removal or destruction managed when personal devices are traded in?).

## Value your Information

Thus, an important agreement reached at this workshop was the requirement to identify the values of data assets by means of an effective valuation and classification system. This is in the context of operating within an information society ecosystem where there are cascades of consequence. Hybrid thinking<sup>7</sup> will be required by management and leadership in order to tackle the challenges ahead. Personal data is the new oil of the information age – and there will be a lot of trading in it – across organisations, as there is already. There is also a lot of “data trading” being seen by users as personalisation on their devices and their online interactions, some naively and some knowingly.

The younger generation of users are happy to simply use information and “get it out there”. They also expect to access information any time, any place, anywhere and not necessarily with any level of checks and balances in place to establish the data provenance.

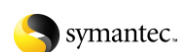
## Protection

But it is necessary to protect information, as required by legislation, regulation, statutory obligations and standards. Personal data should always be protected. Business data should be protected, in all its locations, but especially on personal devices, from leaking or becoming corrupted. For the public sector, this has to be done in the context of the Big Data agenda and the Freedom of Information Act. There may also be issues of IP ownership that have not been considered by users “on the fly” (downloading and accessing information without considering requirements to qualify or attribute the original sources).

<sup>7</sup> <http://www.gartner.com/id=1505920>

Sponsors:

Registered Number 04326237



There is a blurring of requirements in terms of the “right to know” versus the historically sound security practice of operating a “need to know” policy. The model is moving from static (command and control) to dynamic (data centric) with the provision of information in as many formats as possible through whatever medium suits the requestor or user.

There may also be unintended consequences of aggregation of data sets that may not have been considered in their original dataflow construction. It will depend on where the request for data is started from and across which channels the sets are routed. In the Open Data environment, different data sources may reveal different things<sup>8</sup> – but you may have no clarity of this difference if you have no visibility nor understanding of your information assets and their importance throughout their lifecycle. Having an information asset register has always been a key requirement of information security management system implementation and thus of information assurance provision in the round – so no real changes there, just a greater need for perspective and situational awareness by everyone involved in the information flow chain. There is ultimately the risk of a loss of control by the information asset owner once the asset moves onto a consumer device.

## Trust

Another significant theme of our workshop was that of trust – from many angles. Trust in organisations has been eroded as a result of the many and varied data breaches and losses that have been both experienced and reported. Trust in technology itself has also been eroded as a result of breaches relating to the likes of RSA tokens, SSL, the plethora of bugs, malware, Stuxnet and “son of Stuxnet” – DuQu<sup>9</sup>. There are ongoing malware developments and increasingly these will target mobile devices.

This will make it more difficult for the organisation to trust the device – from its point of origin or manufacture through to the data on it. Organisations will have to consider whether to trust data on an un-trusted infrastructure that they do not own and cannot fully assure themselves of its quality, including the “cloud”. Perhaps the most that can be hoped for is reliance, rather than trust – we may *rely* on the availability of the device and the network across which it is running.

The future is most likely to include more access from the consumer consuming – organisations need to be clear as to how trusted the grey sphere in which they are operating is – and this may only be able to be done through contractual means. So the workforce will need to understand what trust and reliance means for the organisation, for them and for their device, and what requirements that brings towards devices and the way they are allowed to be used for work purposes. Agreement needs to be reached between management, ICT and the workforce as to what level of control would be best for them to implement in order to provide the appropriate level of assurance required.

## Risks and Issues

Most data breaches on mobile devices are typically due to basic security failures – weak (or no) passwords, failure to encrypt data, falling victim to phishing or other social engineering and failure to update the device (making it vulnerable to simple attacks).<sup>10</sup> The risks are as they have been in the last decade, but the threats, vulnerabilities and impacts have changed and shifted as a result of the technological and cultural shifts.

There are risks:

- of data leakage and data loss – which will increasingly expose organisations to reputational damage from, for example, email escaping from an organisation’s domain;

<sup>8</sup> <http://net.educause.edu/ir/library/pdf/ELI7059.pdf>

<sup>9</sup> <http://www.pcmag.com/article2/0,2817,2395861,00.asp>

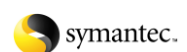
<sup>10</sup> <http://www.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/mobile-device-security-whats-coming-next.aspx>

Sponsors:

Registered Number 04326237



NORTHROP GRUMMAN



SOPHOS



and

- of up to £500,000 fines from the ICO, in the event of a serious data breach, are likely and the future may, at worst, include the risk of jail sentences.

The workforce is reliant on and actively using social media. Corporate policy needs to be able to audit activity to protect brand and reputation. This requires enlightened leadership – and good translators (those individuals who can help the leadership understand the risks and consequences and can equally educate the workforce on what the expected behaviour is and why), as there are read across requirements from individuals, through corporate boards to SMEs and beyond. In addition, it is crucial to foster a culture of information assurance as technical means alone will not suffice.

Regulators are also paying more attention to these devices. It is therefore essential to address the security and operational issues relating to mobile devices **now**, rather than getting caught out. Losing sensitive data on a laptop or a mobile device are not particularly different in the eyes of the law, but the security controls required may well be.<sup>11</sup>

Also, management needs to adopt appropriate corporate social responsibility, managing its health and safety obligations and ensuring that all employees have a happy and healthy workspace in which to be productive and effective. However, they also have a requirement to ensure that there are sufficient controls in place to assure stakeholders that the appropriate governance structures are in place.<sup>12</sup>

## Solutions for consideration

**Technology:** Key information security controls relating to access, remote or otherwise, threat management, desktop virtualisation – providing a “work” and “play” environment, loss prevention and detection all still hold true and there are mobile device applications available to address the specific equipment challenges organisations are facing. It should also be appropriate to enable protection (remote or otherwise) within the products.

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

In the UK, the Information Commissioner has long been “banging the drum” for encryption of data. This should certainly be considered as part of the armoury of control in all circumstances – for data at rest and data in transit – and for data in virtualised environments. There are so many points at which the user may be interacting with their device and an infrastructure and exchanging data that these may need to be mapped and then the appropriate controls deployed to ensure the provision of protection runs throughout the lifecycle of the data.

But obviously, technology is only *part* of the solution.

**People:** There is benefit to be found, particularly in these austere times, in not rebuilding wheels but rather in returning to first principles and ensuring that the user population is bolstered up as the first line of defence. Clued up employees are less likely to make mistakes.

<sup>11</sup> <http://www.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/mobile-device-security-whats-coming-next.aspx>

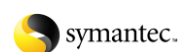
<sup>12</sup> [http://www.ostermanresearch.com/whitepapers/or\\_or0311.pdf](http://www.ostermanresearch.com/whitepapers/or_or0311.pdf)

Sponsors:

Registered Number 04326237



NORTHROP GRUMMAN



SOPHOS



User responsibilities on appropriate use of devices is an important element of the solution space. Users don't currently adhere to the usage of authentication on mobile devices<sup>13</sup> – this will probably need to change in the future in order to better protect the organisation, the user and the information. There are other technology layer solutions available.

Corporate and personal discipline and internet hygiene<sup>14</sup> are what is required moving forward.

**Process:** Policy amendment is therefore vital – in order to tell the users what is expected of them. The necessity needs to be understood, and the impact on usability needs to be acceptable for users - non offensive, and not draconian. There has to be a bottom line for all employees - if you are using a personal device with company data on it, **you are responsible for it and hold the risk**. When an employee leaves the organisation, what happens to the device and/or the information on it – do they keep their own or hand it back in? These considerations will need answers by way of policy edicts.

## In Conclusion

Whether you like it or not, personal devices will be used for work purposes.

- You can **ignore it**, as this could result in people developing their own solutions for how to benefit best from the technology in order to do their work effectively.
- You can **forbid** the use, which would require taking measures to enforce a ban, and which could also keep a lot of convenient and useful means for carrying out work related tasks on private devices away from your workers.
- Or you can **embrace it**, by offering your workers the tools they need, support to use those tools and by training them on how to use those tools in a responsible way.

IAAC recommends *the latter*. Often there is too much to be gained by embracing the use of consumer devices, so they will be used. It would be better to make sure it is done in the best possible way.

From an Information Assurance (IA) standpoint, addressing the information identification, labelling and handling challenges means:

- working out what information can be shared by whom and with whom, through what channels
- controlling access to sensitive data ensuring that only authorized people gain access to the data
- verifying that the data is only being used for the purpose intended
- discovering and documenting what data types they have (producing information asset inventories), where it is stored and where it travels to (including through which jurisdictions)
- validating that the data has not been compromised
- insuring that no one is altering the data
- complying with auditor requirements and
- providing proof of data protection compliance

Ultimately, the IA task is as it has always been – understanding the information needs of both the organisation and its individuals from cradle to grave.

14<sup>th</sup> December 2011

<sup>13</sup> <http://blogs.telegraph.co.uk/technology/adrianhon/100006736/phone-hacking-really-isnt-that-difficult/>

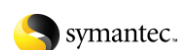
<sup>14</sup> <http://blackwidows.co.uk/clients/imp-guide/www/virus.php>

Sponsors:

Registered Number 04326237



NORTHROP GRUMMAN



SOPHOS



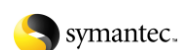
## References

1. **Consumerisation worries public sector IT managers** - <http://www.scmagazineuk.com/consumerisation-worries-public-sector-it-managers/printarticle/211444/>
2. **What have we learned from six months of consumerisation?** - <http://www.scmagazineuk.com/what-have-we-learned-from-six-months-of-consumerisation/printarticle/205547/>
3. **Users should be engaged to enable mobile device management and consumerisation to work** - <http://www.scmagazineuk.com/users-should-be-engaged-to-enable-mobile-device-management-and-consumerisation-to-work/printarticle/205929/>
4. **Infosecurity Europe: Can consumerisation be turned to a business advantage?** - <http://www.scmagazineuk.com/infosecurity-europe-can-consumerisation-be-turned-to-a-business-advantage/printarticle/201052/>
5. **Could a BYOD policy be the solution to your consumerisation problems?** - <http://www.scmagazineuk.com/could-a-byod-policy-be-the-solution-to-your-consumerisation-problems/printarticle/208302/>
6. **Amid social networking security issues, companies block Web 2.0 apps** - [http://searchsecurity.techtarget.co.uk/news/2240081268/Amid-social-networking-security-issues-companies-block-Web-20-apps?asrc=EM\\_NLT\\_14854368&track=NL-988&ad=847692](http://searchsecurity.techtarget.co.uk/news/2240081268/Amid-social-networking-security-issues-companies-block-Web-20-apps?asrc=EM_NLT_14854368&track=NL-988&ad=847692)
7. **Bank Info Security** - [http://www.bankinfosecurity.com/articles.php?art\\_id=4047](http://www.bankinfosecurity.com/articles.php?art_id=4047)
8. **UK Business and Government Dangerously out of tune with cyber threats says Chatham** - <http://www.computerweekly.com/Articles/2011/09/15/247896/UK-business-and-government-dangerously-out-of-tune-with-cyber-threats-says-Chatham.htm>
9. **The future of Malware** - [http://www.computerworld.com/s/article/9220459/The\\_future\\_of\\_malware](http://www.computerworld.com/s/article/9220459/The_future_of_malware)
10. <http://www.tabletdia.com/news/3546.html>
11. [http://www.toshibadirect.com/content/pc/b2c/downloads/MS\\_Healthl\\_WP\\_FINAL.pdf](http://www.toshibadirect.com/content/pc/b2c/downloads/MS_Healthl_WP_FINAL.pdf)
12. <http://thinkprogress.org/yglesias/2010/10/22/198874/tablets-in-hospitals/>
13. **The "Big Five" IT trends of the next half decade: Mobile, social, cloud, consumerization, and big data** - <http://www.zdnet.com/blog/hinchcliffe/the-big-five-it-trends-of-the-next-half-decade-mobile-social-cloud-consumerization-and-big-data/1811>
14. **Young adults shun smartphone security** - [http://www.scmagazineuk.com/young-adults-shun-smartphone-security/article/213538/?DCMP=EMC-SCUK\\_NewsWire](http://www.scmagazineuk.com/young-adults-shun-smartphone-security/article/213538/?DCMP=EMC-SCUK_NewsWire)
15. **Hacked!** - <http://bit.ly/r8IupQ>
16. **Generation Y and Technology – till death do us part** - [http://itknowledgeexchange.techtarget.com/cio/generation-y-and-technology-till-death-do-us-part/?track=NL-973&ad=849831&asrc=EM\\_NLN\\_15293966&uid=1041980](http://itknowledgeexchange.techtarget.com/cio/generation-y-and-technology-till-death-do-us-part/?track=NL-973&ad=849831&asrc=EM_NLN_15293966&uid=1041980)

Sponsors:



NORTHROP GRUMMAN



SOPHOS



Registered Number 04326237