BYOD, Security Consequences and How to Deal With Them

BYOD (Bring Your Own Device) works by the user being paid an allowance usually with their salary to provide a device of their choice (smartphone, tablet, netbook etc.) for use in day to day work as an alternative to the traditional corporate desktop PC.

|  |  |
| --- | --- |
|  |  |

This is seen as a nascent trend by some but in reality it has fast gained acceptance as the de facto choice in many companies. Indeed many commentators see it as present and developing; here <http://www.thesecurityage.com/details.php?seo=eset-survey-the-byod-security-challenges> the author illustrates that 80% of employed adults use a personally-owned electronic device (laptop, tablet, smartphone etc.) for work-related functions.

The move toward BYOD has much in common with the shift to cloud based applications and much of the reasons underpinning its adoption are identical to those behind adopting the cloud. BYOD has many factors in its favour largely through reduced cost accrued through:

* Hardware savings (no network of PCs to deliver and support)
* Software licence costs (licences move to per user/PAYG model)
* Staff savings (onsite support is either minimal or absent under BYOD)

The user also finds this attractive, superficially at least as they can choose their favoured device rather than having a choice visited upon them.

Again, we can see the common ground between BYOD and adoption of the cloud and which shows the revolutionary change (paradigm shift) taking place.



Clearly this has implications for the organisation and their security policies and to appreciate the scale of this see <http://arstechnica.com/science/2012/03/99-percent-of-nasas-portable-devices-are-unencrypted/>. Here we see 99% of NASA's portable devices were unencrypted, 48 of them were lost/stolen between April 2009 and April 2011 with one holding algorithms to command and control the International Space Station. These lax standards are reflected across other US government departments with the potential for many potentially embarrassing consequences.

Referring again to the Security Age article we see a blind refusal to adopt even the most rudimentary security precautions:

* Data encryption is used on approximately one third of devices.
* Under 10% of staff using their own tablets enable auto-locking.
* Only 25% of smartphone users enable autolock.
* Only a third of laptop users utilise auto-locking, so by inference two thirds do not.
* Auto-locking plus password protection is used by less than half of laptop users, under a third of smartphone users, and one in ten tablet users.

This seems to be an education issue with most users attitude being that they will do as they please with their own device; it may be the case that it’s their machine but the data held on it is company property. In turn this would lead to significant legal implications for the organisation as they are required to operate within a specified statutory framework with regards to their won and client data, how it is used, who may and may not access it etc.



Security has until now been controlled by restricting what users may and may not do, so the challenge in a BYOD environment is dealing with the deep seated resentment from users and their habits.

The simplest mechanism of dealing with this is to separate the data from the device. By using virtualisation most "unmanaged BYOD" vendor offerings deliver offerings of this type which are achieved with web services, virtual machines, virtual desktop integration, and virtual application integration.

In the past attempts have been made to segment the data into 2 parts; typically red and green data with red data being the most sensitive and accessed on an as needed basis. Unfortunately these types of solutions have been impractical to deliver in real world situations.

Given that unmanaged devices have access your data anyway, the simplest solution prevents data from being collected or stored on the unmanaged device meaning attackers will have a much harder time accessing or compromising data not on the device.

It is possible to achieve this with the traditional client-server solution where all data remains on the server side and snippets of information are posted to the user using a browser. This works well until the unmanaged device is compromised when the attacker exploits this vulnerability and accesses all computers in the chain from front to back via the middleware.

An improved on this is to allow unmanaged devices to render only screenshots of data returns, which means there is near zero access to any of the computers in the chain holding the data. Examples include remote desktop software such as Citrix, Terminal Services, VNC etc. where a remote device transmits screen drawn updates in response to transmitted inputs. In this way, there is little for the attacker to compromise. It also means that even if a hacker were to steal an unmanaged device and somehow get the remote connection log-on information and so begin accessing the data like a legitimate user, data would be available only one screen at a time.

What we see here is that like the cloud BYOD is a fact of life and we need to understand the issues it presents and develop ways of dealing with them.

For more details on cloud computing services and products please refer to

<http://www.managedserviceexpert.com/>