CM BRIEFING

CMb 2012–04

Plan for BYOD

Historically, bigger organisations provided staff with a corporate phone, often a BlackBerry or equivalent. Generally several generations behind the best of consumer devices, these phones were great for basic connectivity (email and calendar) but little else.

These days, many staff now have a modern smartphone and/or iPad as their personal device, and want to jettison their old corporate device.

Thus 'bring your own device' (BYOD) was born. Pushed by senior and junior staff alike, organisations are increasingly expected to allow staff to access corporate information on their personal devices.

This is not without its risks, and should be approached in a measured way.

Benefits of BYOD

There are a number of clear benefits in supporting BYOD:

- personal devices are usually more modern
- staff get greater choice
- the number of devices is reduced
- staff may be more satisfied
- staff connectivity and availability may be improved
- more functionality can be provided for mobile and field staff
- cost of providing and supporting corporate devices can be reduced or eliminated

BYOD risks and issues

These are matched by a number of obvious risks:

- security risks, relating to lost devices, theft of data or viruses (security is the big concern!)
- complexity of having to support a myriad of devices
- infrastructure issues in giving access to devices not on the corporate network
- danger that work use will lead to excessive costs being borne by staff (such as data costs or replacing lost/damaged devices)
- potential impact on the work/life balance of staff

Have a plan for BYOD

Organisations can unpick the complexity surrounding BYOD by taking a step-by-step approach:

1. Clarify the purpose of supporting BYOD, and write a simple positioning paper for general readership.
2. Determine which devices will be supported.
3. Document usage guidelines, addressing common scenarios and risks.
4. Determine what costs will be covered by the organisation (if any).
5. Use one of the mobile device management (MDM) solutions to mitigate device issues.
6. Provide basic connectivity services, such as access to email and corporate calendar.
7. Determine what other functionality is required, such as intranet access, collaboration tools or business systems.
8. Provide tutorials and help materials on the intranet to assist staff when connecting their personal devices.
9. Determine what IT support, if any, will be provided beyond basic documentation and self-service discussion areas.
10. Launch and communicate BYOD support!
11. Establish ongoing monitoring and management to identify and address issues as they arise (security-related or otherwise).

It's early days

While BYOD is shaping up to be at the forefront of major changes in the corporate landscape, many of the practicalities still have to be fully understood and resolved.

Security is an ever-present and legitimate issue, made only more important as devices are used more widely, and for more critical work.

There are also questions about the long-term viability of expecting staff to support the costs of devices that may be primarily used for work purposes (in this workaholic age).

Still, organisations can't afford to wait, and should provide basic functionality quickly, learning lessons from other early adopters.