Mobile Management in Financial Services

Choosing which mobile devices to assign employees used to be an easy choice for financial services companies. The requirement for secure communications and complete control over mobile devices made Blackberry the obvious choice. Much lower roaming charges sealed the decision for many.

All that has now changed. We have a wide variety of devices to choose from including smart phones and tablets and there is a choice of operating systems for these devices. The requirements for security are still there and only likely to increase giving a greater challenge on how all these devices are controlled and managed.

Aside from the legal requirements put in place to protect information, professional ethics and the need to protect the reputation of your company dictate that every effort is made to protect data.

The Value of Mobile Data

Most companies need mobile technology to compete. Gartner predicts that by 2014, 90% of companies will support corporate applications on personal mobile devices, and 80% will have a mobile workforce equipped with tablets. The finance industry is no stranger to this trend. Helping travelling staff access information in the field, or helping executives view business documents while outside the office, are just two examples of how financial services companies are already benefiting from anytime, anywhere access to corporate systems.

Employees in every industry are now asking to carry around a single device for both business and personal use, a trend known as bring your own device (BYOD). Locally this often translates as choose your own device (CYOD) where an employer provides a choice of devices. This variety of device types holding both personal and company data and applications guarantees a host of security challenges.

Mobility Concerns

Even before the shift towards BYOD/CYOD began, financial services companies have had to address several security issues whenever they moved corporate information outside company premises. When using mobile technology in business, these organizations have been concerned with a myriad of challenges:

- **Complying with regulations:** To protect clients and the market, each local jurisdiction has a set of requirements regulated companies must abide by.
- **Preventing data loss**: Given how easy it is for handsets to be misplaced or stolen, data loss prevention is of utmost importance for any company supporting the use of smartphones, tablets, or even laptops.
- **Enforcing security policy on mobile devices:** With handsets in the field transmitting data over wireless networks, companies need to amend their corporate security policies, and they also have to make sure the rules and guidelines are being followed.

- **Ensuring the use of passwords on mobile devices:** Since employees frequently look for workarounds to avoid having to use long or complicated passwords on mobile devices, it is challenging to ensure password protection on all devices is consistent with corporate policy.

If these concerns were not enough, companies also have to overcome challenges resulting from two things inherent to the BYOD concept:

- **Personal and professional data and applications sit on the same device.** You need to disable a device when it gets lost, but you can only disable company data, leaving the employees private data and applications untouched. The same applies where workers leave the company. By no means can you allow enterprise data or applications to remain on the device, but it's just as important to leave private data intact.
- **Devices from different manufacturers and running different operating systems have different built-in features.** Configuration and security are two major aspects of enforcing corporate policy, but the variety of components and features makes configuring and securing a wide array of handsets very challenging.

Costs Savings and a Productivity Boom
Nevertheless, companies in all industries are opening up to BYOD for at least four reasons:

1. Employees at all levels want to carry just one smartphone for personal and professional use, and to ensure employee satisfaction, companies accommodate it.
2. There are some cost savings when employees bring a device they purchased on their own.
3. By giving workers a wider choice in which handset they use, training and support costs are reduced because they will usually pick a model they are already familiar with—or bring the one they already have.
4. Professionals who use one smartphone tend to be reachable at just about any time and can therefore respond more quickly to business emergencies.

BYOD is part of a bigger movement towards a general "consumerisation" of mobile technology. People like to download apps from app stores, or their equivalents, for personal and business use, and they like to run those apps on their feature-rich smartphones. People are buying applications that perform important business functions in the same way they buy applications for personal use.

Forward-looking companies are opening up to BYOD, and the consumerisation of mobile technology in general, and allowing their workforce access to best-in-class applications. How are these companies standing up to the challenges mentioned above?

They, or their IT suppliers, are scanning the market in search of mobile device management (MDM) platforms to mitigate security risks but allow the creativity and productivity bonus that can be provided. They are looking for a platform that will allow them to offer BYOD/CYOD while helping them meet the security requirements of the regulator and their business.

There are many different systems available but matching the business and regulatory requirement to the feature set of the products can be an in depth process.

Conclusion

Resisting the adoption of BOYD/COYD is really not an option. There are potential benefits to both the employer and the employee provided the devices can be managed in a powerful, effective but simple manner. Exploring and choosing the best technology to support this is a complex issue that requires good IT skills as well as an understanding of the business requirement.

About the author

Tim Roussel has worked in the information management industry for over 20 years. He has experience of working with public bodies and commercial organisations across the UK and EMEA. He has been working for Alternative Solutions Limited for the past three years advising and assisting a variety of organisations on improving business process with a specific interest in managing information. Tim can be contacted on 01481 701234, 07781 140353 or by email tim@asl.gg