

The use of consumer technology such as smartphones is becoming common in corporate IT and recently even the iPad has emerged as a popular choice for executives and IT staff alike. Users have access to business-ready devices in their personal lives, so the line between personal computing and work computing is blurring.

Security professionals are being challenged to permit personal devices to connect to corporate networks and to find a way to secure them. Just saying "no" doesn't work when the pressure comes from the top, so better to embrace the inevitable and build secure architectures that support these devices. The use of technologies like ActiveSync¹ permit users to manage their mail, contacts and calendars on their smartphones and iPads without a direct connection to the corporate network. Apple's iOS products (iPhone, iPad and iPod touch) support Cisco IPsec VPN protocols, proving a secure option for remote access. With the release of iOS 4, iPhones and iPads offer enterprise-quality access controls and policy enforcement² comparable with those offered on a BlackBerry, although some security vulnerabilities are still emerging on these new platforms.

A deal needs to be struck which enables adequate security controls to be applied to consumer devices in return for permitting access to corporate data. The trick is to identify the controls which will enforce your corporate security policy without driving a wedge between the business and its users. The 'sexy' nature of recent consumer technologies has captured the imagination of users, encouraging them to use them as more than phones and PDAs and really explore their capabilities. This can be great news for organisations who embrace the technologies – giving better productivity, more creative results and flexible working. Rather than permitting this wave of consumerisation to sweep over your organisation, research the technologies available and the controls they offer. Perhaps start by offering access to mail and diary systems to a trial group, monitor behaviour and build your experience before committing further. Limit VPN access to devices you know offer secure client software, and ensure you deploy strong authentication to compensate for the potential weaknesses in consumer platforms. Most importantly experiment with the technologies yourself and ensure you understand the strengths and weaknesses of each platform.

Peter Wood is CEO at First Base Technologies, an ethical hacking firm based in the UK, and a member of the ISACA conference committee. Peter founded First Base in 1989 and has hands-on technical involvement in the firm on a daily basis, working in areas as diverse as social engineering, network penetration testing and skills transfer. Peter is also a world-renowned speaker and security evangelist.

Peter Wood
peterw@firstbase.co.uk
www.firstbase.co.uk
www.white-hats.co.uk
www.peterwood.com

¹ http://en.wikipedia.org/wiki/Exchange_ActiveSync

² http://images.apple.com/iphone/business/docs/iPhone_Security.pdf