

Success of mobile devices builds security opportunities

by Marcia MacLeod

microscope@rbi.co.uk

The growth of smartphones and increasing risk to wireless data is driving security specialists to strengthen their channels. Trend Micro, Siemens and ForeScout are all seeking additional partners to promote the need for security on handheld devices.

"Smartphones are growing at over 70 per cent," according to Paul Miller, US managing director of Symantec's mobile security division. "Viruses are spreading like a cold; as people travel, they use their laptops, PDAs and smartphones anywhere — at airports, in Starbucks, on trains and so on — and pick up and transfer viruses.

"Viruses have doubled every six months since 2004; today we know of 235 viruses for mobile devices and, while this compares with 600 for PCs, it is much easier to spread a mobile virus and much easier to lose a mobile device, increasing the risk to personal and corporate data."

The increased risk has, Miller said, boosted the mobile security and device management market from a \$1bn (£513m) business in 2004 to a forecast \$12bn business by 2009.

In addition to viruses that disrupt mobile services, corrupt data and — when the device is attached to a desktop — transfer the damage to the corporate network, criminal hackers can breach confidentiality

by obtaining private data.

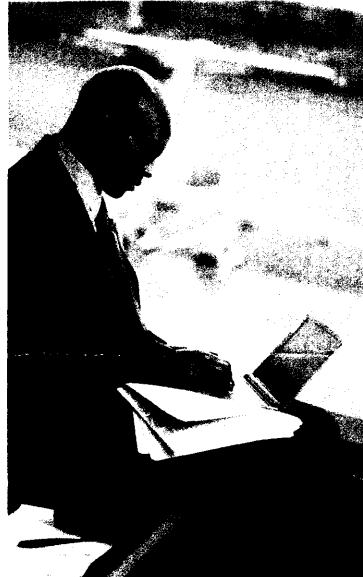
More individuals are hacking into mobiles for financial gain, not simply for the fun of it; in what Symantec calls Pranking4Profit, these criminals access financial and other data which they can use for criminal acts, such as diverting funds to their own bank accounts, Miller said.

Industrial spies use snoopware to gain corporate information. Where VoIP is used, they can even obtain details of meetings and, by inserting a microphone into the mobile, listen to these meetings to access confidential data.

"Enterprises are worried about lost productivity and the risk of lost data and privacy," agreed Todd Thiemann, director of device security for Trend Micro. "Consumers are also worried about lost data, breached privacy and lost productivity. And everyone is concerned about clean-up costs or being left with unusable devices.

"Channel partners can help add value to mobile sales with the configuration of security products. They can provide the user with a vulnerability analysis and help them to work out the most effective security for their needs. The configuration is always changing — for example, when a new mobile device comes on stream — so this is an ongoing requirement.

"The increasing need for security is a revenue opportunity for our partners. It's new, it's different, and not all the industry is focused on it as yet."



The growing popularity of mobile technology is fuelling the spread of viruses — and so the need for security

ForeScout is, said Ray Wizbowski, American vice-president for marketing, "always looking" to expand its channel with security-specific partners.

"We had a large channel network two years ago, but refocused on partners with security expertise. We have two so far in the UK — Axial and Convergent — but are now ready to take on more partners with CIS certification and/or a good networking knowledge. We will take a direct touch approach with channel fulfilment; we want our VARs to be able to help users configure security and develop security policies."

Siemens wants partners with mobile expertise to educate users about the need for security for mobile, particularly VoWLAN or VoWiFi. "If users aren't ready for VoWiFi now, they should be," according to Marcus Birkel, head of Hi Path Wireless, "because it will be well established within two years and enterprises will want to use it. But to feel confident enough to do so, they have to know the right security is in place."

Loss mitigation is an important consideration. According to Miller, data should be encrypted to prevent unauthorised access. Another option is to use software that wipes data when the device is turned on; this software can be activated by the network administrator once the phone or PDA has been reported lost or stolen.

Version 4 of Symantec's Mobile Security for Windows Mobile product, released on 1 November, includes some loss mitigation software. 'Real-time auto protect', for example, analyses data once a device is connected to the network and alerts the user if the device is infected or corrupted, while a scheduled scan checks for viruses and other security breaches on a regular basis. The Symbian version came out in October. Further developments could include 'wipe and kill' software.

ForeScout's CounterAct goes further: it can even stop a device from accessing the network or terminate an application within the device. ■

What's in your tank?

Faster Cleaner Greener

The NEW RoHS Compliant

UNLEADED

e-Series

Beware of Imitations!

RoHS Compliance ensures longevity of product life. Exemptions used by other vendors, are a short term solution.

WICK HILL

WatchGuard's Value Added Distributor of the Year

Call us TODAY to discover the difference

01483 227600

