

# Don't leave your data lying around

The more reliant businesses become on mobile computers, the more data is at risk from theft or loss. It's taken a while for users to adjust to this very real threat, says *Paul Miller* but the security specialists are ready

In the first six months of 2006, 84,619 mobile phones, 21,460 PDAs or Pocket PCs and 4,426 lap tops were left in taxis in just one city – Chicago. Trying to magnify that to come up with a figure for the US, let alone the rest of the world, boggles the mind.

Chances are, very few of those careless cab customers had any kind of security in place to protect their lost devices. In a survey carried out by Symantec, 75 per cent of companies have not even thought about mobile security.

And while there have been few reported security breaches of mobiles as yet, as the use of PDAs explodes (and in particular, smartphones), the unsavoury will not be slow to exploit new criminal opportunities. Things like Bluetooth and Voice over IP (VoIP) just make it easy.

"By 2007/8, 65 per cent of enterprises will have wireless applications," says Jay Burrell, vice-president of business development, enterprise solutions at Nokia in the US. "By 2008, 80 per cent of smartphones will be capable of email and 77 per cent of organisations will be using it."

Todd Thiemann, director, mobile security for Trend Micro, agrees. "Analyst IDC forecasts a hundred million smartphones will be in use by the end of 2006. Next year they will account for 12 per cent of total wireless devices sold. The more devices out there, the greater the security threat."

"The use of Windows, Palm and even Linux operating systems on devices make it easier for security breaches to occur," adds

Paul Miller, managing director of mobile security at Symantec. "Many of these devices are no longer phones; they're computers. Viruses are spreading like a cold or flu."

So far, the threat has consisted primarily of malicious invasion by viruses, worms and Trojans created by geeks who do it for fun. But the wireless sector will almost certainly mirror that of the desktop, with happy hackers creating havoc simply because they can, turning into deliberate criminal attempts to disrupt the user's business and/or obtain confidential data.

## LIKELY TO SPREAD

"PC attacks only recently became highly targeted," suggests Antti Vihavainen, vice-president, mobile security for F Secure. "They are now more professional and criminally motivated. Mobile attacks are still 'proof of concept' – not motivated by money or corporate data. They can hit anyone who has a mobile device – and the more people in the area, the more likely it is for the virus to spread.

"We don't know how threats to mobiles will develop – but there is already an underworld for attacking desktops, with its own supply chain of wholesaler, reseller and user. Members of the underworld know who to talk to in order to get people to open a device and obtain data or infect the device. People are making a living from criminally



**It's all too easy to lose a handheld computer or even a laptop. A moment's lack of concentration and it's gone, as our pictures from Pointsec illustrate only too well. Pointsec is one of the world leaders in security and encryption systems for mobile devices, and claims to offer the most powerful and varied range of solutions on the market.**

hacking into computers – and there's no reason why this can't be extended to mobile devices."

Miller agrees. He names two serious threats to mobile: "pranking4profit" and "snoopware". "Mobile devices are becoming digital wallets and IDs; pranking4profit attacks are made for financial gain. A premium SMS text attack on a smartphone can drain a user's bank account. In Japan, mobile phones are being combined with a payment device to be used at the till, as well as over the Internet. This technology will hit the rest of the world, making these devices even more valuable.

"Snoopware puts a stranger in your bedroom and a competitor in your boardroom. As people keep more data on their devices, criminals do their best to take it, but since they are copying it, rather →

A number of systems suppliers are addressing mobile security. Below are some of them.

**AVANQUEST:** VirusGuard, developed by SMobile Systems, offers anti-virus protection for all major mobile platforms.

**FORESCOUT:** CounterAct network asset control. Detects and blocks self-propagating threats. The latest version (6.0) can terminate an application. Enforcement is tailored, so there is an appropriate response to each violation – from alerts being sent to the administrator if something untoward is detected to the blocking of a device.

**F SECURE:** Brought out its first version of F Secure Mobile Security, including firewall and anti-virus protection, in 2005. Initially for Symbian, but adding Windows shortly. Will add new functionality, such as anti-spyware.

**iANYWHERE:** offers encryption, device management and other protection, as well as means of backing up mobile data so an affected device can be "provisioned" (restored

to the same way it was before it was attacked).

**NOKIA:** Works with partners to offer protection, for example Sourcefire's Intrusion Prevention System, but purchase of Intellisync Mobile Suite gives company a greater presence in security market. Concentrating on device management and protection for VoIP.

**POINTSEC:** Offers a comprehensive range of security and encryption for PDAs, mobiles and laptops running almost all modern operating systems. The system is centrally managed, preventing users from altering their settings locally. Recently launched a version for Nokia's eseries Symbian-based phones.

**STILLSECURE:** Latest product, SafeAccess, offers network access and management, checking devices trying to access the network, monitoring data after log-on, blocking devices from parts of the network or shutting them down completely if need be.

Now evaluating product for SME market, combining security with device management.

**SYMANTEC:** Version 4 of its Mobile Security for Windows Mobile released in November, but also has Symbian version. Software includes network protection, anti-virus and spam protection. Covers Wi-Fi as well as cellular networks. Real Time Auto Protect analyses data once it is on the system and notifies users if a device is infected, and what with. Includes device level encryption, remote wipe and kill (thanks to purchase of Veritas). Offers a "try and buy" 30-day free trial.

**TREND MICRO:** Mobile Security 3.0, latest release, adds firewall and intrusion detection to its anti-virus and anti-spam for Windows. Also simplified user interface. Thirty-day trial available online, then just \$34.99 for a year's protection. Symbian version out early 2007.

**VERIZON:** Wireless Sync offers email synchronisation with wipe and kill and back-up.



COURTESY POINTSEC

Mike Oliver, iAnywhere

than removing it, the device's user won't always know it has been stolen. With the growth of VoIP, people can remotely activate the microphone in the phone and listen to private conversations – or even confidential meetings."

Worse still, if the device is used to access

a corporate network, any criminal hacking into the device can also hack into the network and, as Alan Shimel, chief strategy officer for StillSecure, points out, "once someone is on the network, who's to say where they can or cannot reach?"

A malicious hacker who does gain access to the corporate system can obtain customer details, shipment and delivery data, information on field service jobs, data on products and inventory and financial and other information about the company and its suppliers and customers. If any of this data is exposed, it not only threatens the company's business, but could also land it in trouble by causing it to inadvertently breach the Data Protection Act: confidential information is supposed to remain confidential.

It is easy to think that security issues don't affect *m.logistics* readers. After all, how much data does a delivery driver or a field engineer hold on their mobile phone? Well, according to the security companies, potentially a lot – and while one might expect those suppliers to be trying to drum up business for themselves, you should read on.

Nokia lists field service, parcels delivery and warehousing as big verticals for the growing mobile security sector. "We expect to see more customised applications and demand from customers in these sectors," says the company's Jay Burrell.

"Logistics and field service providers are early adapters of mobile technology," Miller points out, "meaning there are more 'smart' devices in use, increasing the risk."

And there are likely to be rich pickings for those who do hack in. Before you say "but

drivers only hold delivery data", think about what that means: customer name and address, details of items being collected or delivered and the route the driver is taking. The biggest rise in logistics crime is said to be organised theft and vehicle hijack. Give the criminals the right information, and you may as well hand them the keys.

"At the very least," says Mike Oliver, head of UK marketing for iAnywhere, "if the device is lost, stolen or infected with a virus, the disruption can be catastrophic. Drivers won't have any idea where to go; they will have to return to base for a new schedule – and, in many cases, the company will incur a penalty for failing to meet delivery targets."

While Oliver thinks logistics and field service sectors are perhaps the only ones in which the value of lost data falls below that of disruption (and the loss of the expensive device itself), Alan Shimel of StillSecure warns that many people store much more data than they need.

"A driver may only use a delivery name and address, but sometimes it's easier to transmit an entire customer file than pick out just the relevant details. If only the customer's name and address are downloaded to the driver's device, that information could be linked to other files which a hacker, once he breaches the device itself, can access." Remember how easy it is for the criminally-minded to use a stolen or hacked device to access the entire corporate network.

So what can companies do to ensure their device, and their network, remain safe? For a start, there are a number of security products

out there for mobiles (see panel on page 19). Data and storage cards should be encrypted; firewalls should be installed. Device management products enable users to "wipe and kill" data from lost or stolen devices or shut down devices, preventing fraudulent users from accessing an application or network. There apparently is even a product that causes a lost/stolen device to "scream" – making a high pitched noise if anyone tries to use it.

"Companies have to make sure their mobile users aren't introducing anything malicious to the network," Shimel adds. "At the same time, the mobile worker has to be protected from anything malicious on the network. Any device should be checked and authenticated before it is allowed access to the network. After log-on, traffic to and from the devices should be monitored to identify anything damaging or malicious which may be introduced and, if necessary, the device should be dropped from use."

#### DOUBLE-PRONGED SOLUTION

"Companies need a double-pronged solution," says Oliver. "They need to be able to authenticate users; protect data as it travels across the network, whether it is wireless LAN, Bluetooth, infrared or any other; protect data on a device; and disable lost or stolen devices."

"Devices should be allocated to a named individual, not a department or a route or a job. A named 'owner' is more likely to take better care of the device. In addition, users

Todd Thiermann, Trend Micro

should only be able to access data relevant to their job."


"Whatever the size of the company, it should establish a policy for buying and using mobiles," says Todd Thiermann of Trend Micro. "Who buys them? What devices are acceptable? What data/applications are allowed on the device? What use of the device is acceptable? If the company doesn't allow employees to download games on to a desktop, the same should apply to PDAs."

"Personal and corporate devices should be kept separate," adds Burrell. "Devices taken home for personal use are open to a greater risk, as games, videos, music and other content are downloaded." And if the kids get hold of it, don't even think about the potential consequences.

Personal awareness and staff training are vital. "Staff must be given clear rules about how to use their device and how to look after it," emphasises Graham Cluley, senior technology consultant at Sophus.

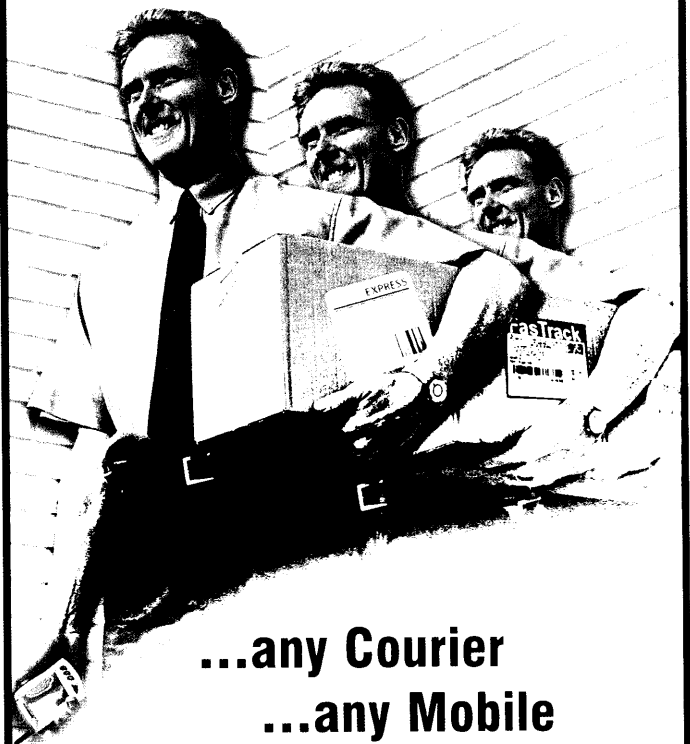
All devices must be treated like gold dust: they can never be left in a cab, on a counter or in a coat pocket hung on the back of a chair, even for a minute. And employees who disable passwords should be disciplined.

For many, mobile security remains something for everyone else but them. "Unfortunately," says Peter Machine, publishing manager for Avanquest's VirusGuard, "until there is a serious virus or other incident on a mobile, no one will do anything to protect their devices."

But the result of a storm of security breaches could be extremely damaging, to the point – especially for a small company – of leading to the firm's downfall. Cleaning up after a hurricane is much harder – and more expensive – than fixing the levees before they break. 

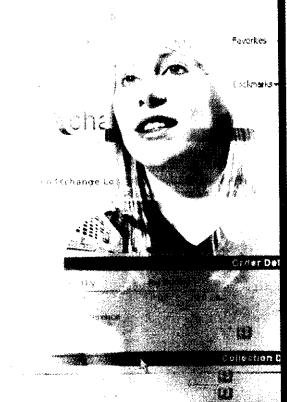
# PODXchange

The Signature Courier Portal



...any Courier  
...any Mobile  
...any Customer

**PODXchange** is a new web portal designed to receive status updates and signatures from couriers, using any mobile device, or easy to use web forms. Delivery information is immediately available on the web and can be automatically transmitted on to any major parcel carrier or customer web site.



To find out more go to [www.netdespatch.com](http://www.netdespatch.com) or call

 net  
despatch®