

# The trouble with



The sequel to the horror movie 'Jaws' carried the tag line, "Just when you thought it was safe to go back in the water". Managing information technology can be like that. Just when everything is under control along comes a new gadget to cause you a headache. This time it's smart phones. They're mobile. They're smart. And people want to connect them to your network. John Costello investigates.

Mobile phones are adding another layer of complexity to the task of those of us managing computer networks. They are the latest in waves of technology we have had to contend with.

In the beginning it was PCs and the task of controlling their proliferation on computer networks. Then along came laptop computers and Wi-Fi.

Now there are mobile phones. Adding to the headache is the fact many of the people likely to demand access to your network via the new generation of smart phones could be senior people in your corporate hierarchy — ahead of you in the corporate food chain.

Brad Reed is the marketing manager for Nokia Enterprise Solutions. "Typically, the smart phone has not been treated as an IT device," he said. "But rapid developments in mobile phone technology will mean the need to deploy encryption and firewalls and have the ability to disable a mobile phone over the air if it has been stolen or compromised."

He said the industry was still very much at the early stage of connecting mobile devices to networks. "But it is likely to come on with a rush," Brad Reed said.

Underlining the move to mobile phones was the release of recent figures from IDC, the market research company. It said mobile phone shipments worldwide grew by 34% in 2004 over 2003 — the strongest year-on-year growth the industry has seen.

IDC estimates almost 700 million devices were shipped in the 12-month period fuelled by the demand for camera phones and colour displays.

About 692 million units were shipped in 2004. The massive expansion was driven by the demand for colour displays and camera phones throughout the world, according to the market research company. IDC said there are now 1.7 billion mobile phones in use throughout the world.

Ian Gilchrist is a senior systems engineer with TippingPoint. A division of 3Com, TippingPoint is a provider of network-based intrusion prevention systems.

The 3Com division recently announced protection for all vulnerabilities disclosed by Microsoft for its Explorer web browser.

"There are a plethora of devices that can turn rogue," Ian Gilchrist said. "The whole issue of detecting intrusions in your network is a bit like a smoke alarm. It can tell you smoke is there but can't put out the fire."

Adding to the vulnerabilities of an increasingly mobile workforce is the spread of so-called hotspots.

# smart phones



Ben Teh, Australian manager for Fortinet, said most mobile users do not realise once connected to a wireless hotspot, they are a member of a connected community of users — most or all of whom are strangers.

"There is often little or no control of what can pass from user to user via a wireless access point and that can have disastrous consequences.

"A web surfer can become infected easily with a virus or worm that has been picked up by a neighbouring user." He said the real damage occurs when the newly-infected user returns to work and connects to the corporation's wireless access point, causing the worm to run unhindered into the user's corporate network.

Wireless hotspots are also spreading and growing in popularity because they provide high-speed internet access, mobility, flexibility and improved productivity.

For example, Optus recently announced an expansion of its Wireless Connect service to cover almost 600 sites across Australia.

"While advantageous, wireless hotspots pose significant security risks," Ben Teh said. "For all the effort going into wireless security standards, none provide protections against the spread of content-based threats. Preventing the spread of viruses, trojans, worms, banned content and spam via wireless access points is left as an exercise for the user."

And the users are largely ignoring the threat is the message from Gavin Matthews. He is CIO of Seccom Networks, a provider of managed security services. "It's been estimated there have been more than 60,000 viruses and other security threats aimed at Microsoft products over the past few years," he said.

"The problems with mobile devices come when they are running on Windows CE.

"The smart phone may pick up a virus from downloaded email and it doesn't show. But when the phone reconnects with the corporate network the virus enters that system.

"One of the key problems today is many organisations — a lot of them from the top end of town — don't understand the real threats facing their networks.

"They are burying their heads in the sand."

Gavin Matthews said there were very low threats from the previous generation of handheld devices such as PDAs.

"Demand for PDAs is falling as many of their features are built into the new generation of mobile phones along with additional features such as a camera."

Managed security service providers, such as Seccom Networks, are proliferating as the need for more sophisticated security defences arises. These service providers not only offer bandwidth, but security services for firewall, intrusion detection and prevention, anti-virus, spam filtering, web content filtering, and VPN services.

McAfee, the major intrusion prevention and security risk management company, has also identified mobile viruses as a growing threat.

Its researchers have discovered a technique for compromising Bluetooth authentication protocol and potentially gaining control of Bluetooth-enabled mobile phones, even when the handsets have security features switched on.

"The technique allows an attacker with specialised equipment to connect to a Bluetooth handset without authorisation," McAfee said in a report on current threats to computer networks.

*"Adding to the headache is the fact many of the people likely to demand access to your network via the new generation of smart phones could be senior people in your corporate hierarchy — ahead of you in the corporate food chain."*

"Once the connection is established, the attacker could potentially gain access to resources of the handset to make calls on the target's handset, siphon off data, or access data services via a compromised handset," McAfee said.

Fortinet's Ben Teh notes today's wireless security standards, such as WEP and WPA, are concerned primarily with the privacy of wireless connections, via encryption, and with ensuring that only authorised users can connect to a wireless access point, via authentication. "But once a user is authenticated and connects to a wireless access point, the wireless channel — even if encrypted — can easily deliver content threats into the wired network, from inside the organisation's typical perimeter defences such as a firewall."

Fortinet has developed a check list on network security issues. This starts with the need for change to traditional security devices and also the way in which network segments are designed. "Developing security zones to move and layer security closer to corporate assets is now mandatory to safeguarding corporate resources within the corporate," the Fortinet check list says.

It also says security management needs a method at a gateway level, to distinguish bad from good content. Bad content should be

defined as anything inconsistent with corporate policy.

Firewalls and other technological solutions are also needed to supplement corporate policy.

"Attackers are also leveraging code

produced by earlier attacks to reduce the time it takes to create a new attack," the checklist says. "The time a new vulnerability is found to the time it is exploited by attackers is rapidly decreasing," the checklist says. "IT professionals must move much quicker to patch their systems before the next attack on their network."

It notes viruses are no longer targeted at individuals or single computers. Intrusions are no longer single-point, nor can they be traced back to a single IP address. "They are now distributed and can originate from anywhere in the world, from a single source, or multiple sources.

It also notes complexity of attacks is growing, as is their ability to bypass traditional point-based security.

Although establishing all those barriers of security might sound like a daunting task, there are a number of ways to accomplish this, each

## Don't let a user become modern-day Typhoid Mary

Proud of their latest smart phones, your fellow employees run the risk of becoming the modern-day equivalent of Typhoid Mary. Her real name was Mary Mallon. She was the first person found to be a 'healthy carrier' of typhoid fever in the US.

In the early 1900s, Mary was attributed with infecting 47 people with typhoid fever, three of whom died. Her position as cook in a large family meant she came in contact with food and unwittingly spread typhoid to members of the family and other domestic staff. She was not affected by the fever.

Health officials tried to cure her but failed. She was eventually isolated on a small island for 26 years. Immunisation for typhoid fever became available after 1911.

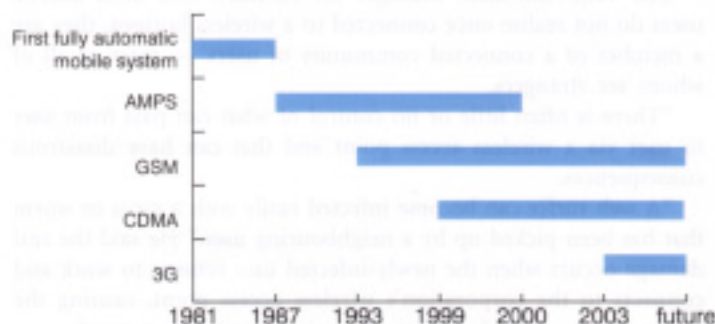
Mobile phones could be the modern equivalent as a threat to your network. They are not affected themselves but will carry security threats into your network.

"About 90% of these mobile devices are owned by the employees themselves," said Gavin Matthew of Seccom Networks.

"They use them to collect emails and then reconnect with the corporate network."

Gavin Matthews said he knew of several large well-known companies that had been infected by viruses and other malware in this fashion.

*"...most mobile users do not realise once connected to a wireless hotspot, they are a member of a connected community of users — most or all of whom are strangers."*



Mobile Telecommunications Timeline, Australia

of which begins with education. Ian Gilchrist said companies need a three-stage approach. "Establish a policy on security. Educate employees, especially those that work off site, of the security threats posed by accessing wireless networks, even if they wrongly assume they are doing so securely.

"Finally, enforce the policy."

Obviously technology must also play an important role, because hackers are continuing to escalate the security arms race. Multiple layers of security — residing at the network gateway, on internal servers, and on individual clients/endpoints — are required to truly offer complete protection. More than that though, these technologies must go beyond traditional authentication and encryption, and detect and eliminate content-based threats — but without degrading network performance. After all, the speed of wireless is one of the technology's most attractive qualities.