Wireless World: Industry mum on attacks

October 14 2005

Who do most IT professionals call when there has been a breach of security -- an attack by hackers seeking to steal information from mobile phones and personal digital assistants? Is it the FBI or the CIA or the NSA or the Department of Homeland Security?

No, experts told UPI's Wireless World. They generally keep it to themselves, fearful of the repercussions of reporting the incident to authorities.

"Most security professionals are stuck in reactive mode," said Sanjay Uppal, vice president of technology for Caymas Systems, an IT security provider in San Jose, Calif. "They may not have enough information about where the attack came from, and they are often unsure of what damage has been done. So they remain quiet."

This can be demonstrated quantitatively, as well as qualitatively. According to a recent report from PricewaterhouseCoopers based on interviews with IT security professionals, 55 percent indicate that they notify no one when an attack occurs. Another report by the FBI was even more telling, revealing only 12 percent of those who are attacked by hackers seek legal advice as to how to deal with the security threat.

This is not the way it should be. "Network security is a vital piece of business information, and it should be a part of routine reporting," said Uppal.

Security for networked, wireless devices -- laptops, mobile phones and

PDAs -- is getting a lot of attention these days.

A trade show held this week at Chicago's Navy Pier, the 2005 Mobile Business Expo, held a number of panels exploring security risks faced by businesses as a result of employees using mobile phones, often without permission, for e-mailing and other data-transfer tasks.

"Your workforce is going mobile, with or without you, said Vicki Warker, a vice president of marketing at Sprint and keynote speaker at the conference.

A study commissioned by Symantec, the Silicon Valley anti-virus firm, indicates that the security risks posed by mobile phones will grow in the coming years. The study showed that 64 percent of respondents stored confidential business -- and client -- data on their mobile phones. They also sent and received confidential client e-mails on their cell phones and PDAs. They also used instant messaging on their mobile phones and downloaded files directly from the Internet, increasing the chances that they will be infected with viruses or attacked by malware purveyors.

Some mobile-phone purveyors are directly addressing the increased threat to businesses presented by mobile-phone hackers.

"Symantec and Nokia announced a partnership last week," said a spokesman from Nokia. "Nokia will be able to pre-load their Series 60 and Symbian OS-based mobile devices with Symantec's mobile security solutions -- anti-virus and firewall -- offering increased protection for consumer and business users against mobile malware threats."

Phone providers, interestingly, may not be the vendor of choice for those who manage complex corporate computing networks. A survey by Gartner Inc., the research consultancy, indicates that companies don't want technology alone; they want value-added services for mobile-phone

security. "Companies have strategic and technical concerns," said Warker. "They need to have someone make the technology work for them seamlessly, anywhere, from work or home, or while traveling."

There are some 162 million mobile-phone users in the United States today, she said, but 40 percent of companies don't even have a written security policy to prevent infections from mobile-phone-borne viruses. "Security is the biggest access problem for companies today," said Warker.