

IT

By Charles Mandel

MANAGING THE IT SECURITY THREATS*It starts with the three pillars of security: people, process and technology, observes an industry expert*

Most businesses know about spam, but are they prepared for spit? Tom Keenan, an adjunct professor in computing science and an I.S.P., defines spit as spam over Internet telephony, something that may become increasingly common as more companies switch to VoIP. And while firms are aware of hackers, do they know much about Googlehacking? The latter occurs when people use the advanced search functions of Google to unearth things on the web such as lists of ports, printers, passwords and even sometimes corporate security vulnerability reports that haven't been secured properly on company intranets.

As technology has evolved, so too have threats to IT security. Now, more than ever, information technology professionals need to be prepared to ward off a constantly changing array of viruses, hacks and other intrusions. Keenan says the classic threat is malware, consisting of viruses, worms and so on. But while all the high-profile viruses make the news, Keenan says he's a lot more worried about the ones he

the focus has been on technology and its weaknesses — concentrating on flaws in and attacks on the network side.

Because of encryption and other security technologies, it is no longer so easy to target networks. Now virus writers concentrate on exploiting weaknesses in software applications and use social engineering techniques such as e-mails to convince people to trigger deadly payloads that will infect corporate systems or to surf to web sites where malware might be downloaded onto their browser. One of the key things organizations should be looking at is educating their employees not to open attachments or surf to web sites when they receive e-mails from individuals they don't know, Wong says. They should delete such e-mails and report any questionable in-box arrivals to their IT department.

Wong says process is all about patch and update management and that it's the IT department's responsibility to ensure everything is kept current. Keenan adds that one of the

gets access; what kinds of devices are allowed access; and what sort of encryption will be used? He warns about "wireless phishing," wireless networks specifically designed to steal information through bogus hot spots, and says companies must take precautions to protect mobile devices against theft since the hard drives can be cracked for information.

Keenan adds to the list of security breaches "the threat from within." He says companies need to beware of "rouge" employees who send information out, adding that while you don't want to be suspicious of your people, adequate controls are necessary. Keenan says it's well within the rights of company to take such action as they own the computers. "In at least one case, I know of the loss to a company where the information that was being leaked could have been in the many millions of dollars. You have a lot of confidential information. You want to make sure you protect it."

OBSERVES KEENAN: "I THINK WE'RE SEEING MORE OF THE ONES WHERE THEY ATTEMPT TO GET INSIDE YOUR MACHINE SILENTLY AND LOOK FOR CERTAIN THINGS: CREDIT CARD NUMBERS, PASSWORDS AND SO ON, MAILING THEM OUT"

doesn't hear about. "I think we're seeing more of the ones where they attempt to get inside your machine silently and look for certain things: credit card numbers, passwords and so on, mailing them out."

Keenan stresses the importance of being scrupulous about using virus-checkers to ensure computers are clean. He says the machines could be infected silently and doing bad things and no one would ever even know. "It's malpractice not to have your virus checkers, firewalls and other software, like that up to date." Derick Wong, a senior security product manager with Microsoft Canada, talks about the three pillars of security: people, process and technology. Up until recently, he says,

new movements is to keep track of what's been done, so if something goes wrong the IT department can back it out. New configuration management software helps track which version of any given program were running on particular days. "I guess the high-level view is the IT people don't just need to do their job right, they need to be able to document they've done their job right."

Stephen Ibaraki, I.S.P. and a director-at-large for CIPS, cites a Symantec study that places the average value of intellectual property on laptops at nearly \$1-million US. According to Ibaraki, mobile and wireless technology are the next wave of devices IT professionals need to ensure are secure against outside threats. Among the questions IT staff need to consider are who



DERICK WONG