The Enemy Within

Michael Barwise

It's conventional wisdom that 80% of security breaches come from inside the enterprise. Does that mean four out of five of your staff are potential terrorists? I think not.

Yes, we've all heard horror stories about sacked workers deleting the company archives. But how often does it happen? And how many staff do you sack per week anyway? I think the bulk of the 80% has to be explained another way.

In the battle for network security, idle hands *really* do the Devil's work. It's amazing how much time goes on private Internet access in working hours. Vast quantities of untrusted data and software are downloaded every day onto the corporate network by people who haven't a clue what they're doing, making complete nonsense of your firewall. MP3 files, movie clips, porno pictures and even device driver updates can hide nasties like "Sub7", "Chernobyl" and "911". Spam e-mails flood in, offering screen savers, pictures of naked tennis players or promises of the "Timothy McVeigh execution" movie. But do they carry a destructive payload? What about those active scripts buried in "must view" web pages? This is true "Social Engineering": fooling people into attacking themselves by running malicious programs or "malware". And it's an escalating threat.

Your staff are constantly compromising your network. But let's get one thing straight. There's no malice in this. They're thinking of themselves, not the company. And they probably don't know there's a hazard anyway. Did anyone actually explain "PrettyPark", "Sircam" or "Anna Kournikova" to them, or did they just get another "Thou Shalt Not" e-mail from IT Support? Did they even get that?

It's a human problem, not a technological one. Mopping up the symptoms with technical fixes can reduce the hazard, but not eliminate it. Even thoroughly up-to-date anti-virus tools can only address reported malware, which means if an attack is covered, someone has fallen victim already. And *it might be you.*

So how can you stem this tide of illicit and dangerous files? Well, for a start, who actually needs what facilities for their job function? Applying minimum privilege does wonders in reducing risk. But, ultimately, it's about educating people. Make sure your technical support understand the threats and can explain them clearly. Involve all your users: brief them; listen to their feedback. Provide incentives for them to pay attention. A bottle of wine and some public recognition is the least you could do for someone who reports a serious threat. Be cautious with ferocious penalties: they can backfire. But if you use them, make them stick, even if the culprit's the MD.

Get your workers on your side. Make sure they know it's their problem as much as yours. An attentive, security-conscious workforce is a powerful cohort in your army. Then, with the bulk of the risk under control, you'll just be left with the small core of crazies. Provided you're paying attention yourself, you can use the resources you've freed up from constant firefighting to identify these before they strike.

Think about this: if you had a house full of antiques, you'd get some good locks and an alarm system. Would you then invite in complete strangers and leave them there while you went to the shops?

So why do you do it on your computers?

Originally appeared in Computer Weekly, October 2001