STEP 3 VALUE EDUCATION

BE IN THE KNOW
Training staff on the dangers of security breaches can limit the risk of slips occurring.
PHOTO: FIREBRAND

Education, education, education...

■ **Question:** Why are so many companies affected by their own employees making silly mistakes?
■ **Answer:** Because they haven't been properly trained.

HOW WE MADE IT

Information security, and, indeed, the virtual world of business, is so new that companies and their employees are having to develop their skills and knowledge at a rate that would have been inconceivable a generation ago.

Nowhere is this more the case than in the world of IT, and with good reason, according to Robert Chapman, co-founder of Firebrand Training. "In the near future, I believe it may be grounds for an employee to lose their job if they cause a security breakdown," he says. "They themselves might not realise that when they are signing employment contracts, the small print might specify such a penalty. Or, say one organisation has been hacked, and is then used as the vehicle to attack a third company. That first organisation could be sued for allowing itself to be used as a weapon." And, of course, there is the business loss if a company is attacked, leading to loss of reputation, profit meltdown and ultimately putting the very company itself at risk.

Robert Chapman
Co-Founder,
Firebrand Training

"It is usually people that are the problem, not the IT," Mr Chapman says. Companies can spend a fortune on security, but just one rogue user can cause havoc by shoving a memory stick into the system that was picked up on the street. Firebrand conducted an experiment, offering to give commuters a cheap biro in return for their password: the majority complied.

The obvious answer to deal with this is to employ well trained staff and keep them up-to-date, but even then there are problems, with the virtual world developing all the time, "nobody knows what they don't know," as Mr Chapman puts it. Just about all standard courses will include security elements, but after that they range wildly, from how to write secure computer programmes to how to perfect a secure code.

But an increasing number are also teaching IT operators how to be hackers, the thinking being that if they can enter the mindset of the enemy, then they are one step closer to knowing where their own organisations may not be secure: it is now possible to become a certified hacking forensic investigator.

VIRGINIA BLACKBURN
info.uk@mediaplanet.com

QUESTION & ANSWER

James Young was a lead technical architect on a multi-billion pound defence project when he attended a Firebrand course on ethical hacking in November last year.

■ **What problems were you suffering with when you attended the week-long course?**

"Working in defence, it was crucial to ensure the IT systems couldn't be penetrated by hackers (or anyone else) and since I was working on significant projects, I had to stay up-to-date in the subject matter. I have attended three of Firebrand's courses, starting some years ago when they were still called The Training Camp, the ethical hacking course being the most recent. I have quite a history with them.

■ **How did the course help you?**

"Knowledge of ethical hacking is essential in my business: you have got to know the methods an attacker will use to gain access to a system in order to establish a defence for that system. It also reinforced the knowledge I already had, building on the most up-to-date developments in information security.

■ **What results did you see after attending the course?**

"It had a huge effect on the work I do as the infrastructure designer of an information system. It allowed me to build a defence with in-depth measures, fully aware of hacker threats and insider threats. These latter are also to be taken very seriously: companies might guard themselves with firewalls and encryptions, but once you actually get inside the company's system itself, it's a complete mess."