

## **Careless staff may play into the hands of hackers**

**Expert says they need to be educated that their laxity can hurt firms and affect jobs**  
**By Chua Hian Hou**

COMPLACENT and careless employees can unwittingly help hackers undermine their companies' security, and steal confidential corporate data.

This common failing could have disastrous consequences for the company - and the guilty workers' jobs, warned security expert Larry Detar, one of the speakers at the Hacker Halted conference organised by Informatics yesterday.

'Complacency is the reason many employees all over the world wind up becoming unwitting assistants to a hacker's attack,' said Mr Detar, a senior security services consultant at US-based security consulting firm Clifton Gunderson.

Hackers who steal confidential information could sell it to competitors. Even if they do not, should word of a lapse get out, the company could lose customers and even face disciplinary action if it is in a regulated industry like finance or health, he said.

Complacency arises because 'people who work with confidential documents all the time see these simply as 'pieces of paper', so they stop taking precautions to make sure these documents don't fall into the wrong hands'.

Similarly, employees who work with sensitive data eventually become so blase about the security of electronic files that they fail to take the necessary precautions to protect them.

In the course of conducting security audits at US financial firms, Mr Detar found that many employees doing highly confidential work - even senior managers - disabled their computer or document passwords to avoid having to log in when they returned from lunch. Some even downloaded unauthorised software like instant messaging or games - which may be computer viruses in disguise - even when they were instructed not to do so.

This is especially true, he said, at companies that have never been hit by any security breach before. 'They all think, 'This could never happen to me',' he said.

But lapses could be costly if a hacker with malicious intent managed to access an unprotected computer and read confidential correspondence or, worse, downloaded it. This is easily done with unobtrusive thumb-size storage devices.

'And nobody blinks an eyelid at someone connecting an iPod to a computer in the workplace any more - forgetting that an iPod has a hard disk and can be used to download the entire contents of an unprotected computer,' said Mr Detar.

Nor is it particularly difficult to enter an office these days and gain access to unprotected computers. 'Why bother to break in when the hacker can pose as a potential customer or work for the cleaning company to get legitimate access to the premises?'

The cure for complacency: understanding.

'Companies should explain the importance of these precautions to staff - and scenario play could be of tremendous help in this education process - by making them understand how their actions could hurt their company and thus, their own rice bowl,' said Mr Detar.

And once employees get this message, he said, they would be more than willing to take precautions.

**chuahh@sph.com.sg**