Cybertrust "How the Heck Did This Happen" Presentation
Case D
Full story available at http://www.vnunet.com/archives
28/07/2003

Sacked staff turn to sabotage

By Claire Pope [28-07-2003]

Failure to revoke access to corporate networks could prove very costly

IT departments that fail to revoke access rights to critical systems risk exposing their firms to security breaches by former employees, new research has found.

More than half the UK workforce would be prepared to seek revenge on former employers by exploiting continued access to corporate systems if they were unhappy at losing their job, according to research by software vendor Novell.

Security experts stressed that this shows the importance of having good policies in place to deal with staff leaving and to provide legal protection.

Half of those questioned indicated that they would continue to access the corporate IT network, and 55 per cent would continue to use their company laptop if it was not taken back.

More worryingly, six per cent said that they would delete important files, and four per cent would let a virus loose in the corporate email system.

Sixty-seven per cent would be prepared to steal sensitive information that would help in their next job, and 38 per cent said that they would steal company leads.

Fifty-eight per cent would continue to use company mobile phones if they were not taken back, costing UK industry an estimated £1m a week.

According to the Department of Trade and Industry, not even a third of UK firms have the security policies necessary to ensure that staff access to company resources is terminated when they leave.

"If an employee has permission to access a customer database, user policies must be worded very carefully," said Neil Barrett, technical director at security specialist Information Risk Management.

"If access is properly specified the employee would no longer have the right to read the records, let alone take or change them."