

Release date: 22nd May 2006

Information Security Breaches Survey 2006 puts Corporate Britain's IT culture under the spotlight

The report released in April, sponsored by the Department of Trade & Industry, highlights the fact that most businesses are a long way from having a security aware culture.

Although three quarters of UK businesses rate IT Security as a high priority, with protecting customer information becoming increasingly important, worryingly just 1 firm in 8 has IT security qualified staff to put procedures in place. Businesses that rely on online interaction with their customers are advised to get a handle on Identity Management to counteract the growing threat of identity theft and fraudulent attacks.

These types of security breaches are ranked as having the most severe impact, with the average 'worst incident' ringing in at £12,000, up by £2,000 since 2004. The financial services sector and telecoms providers appear to be prime targets; several businesses reported daily attacks. The most obvious and valuable data obtainable from these attacks would be detailed customer information such as credit card and bank details, typically siphoned off by Keylogging software.

Corporate Britain is also still oblivious to the threat posed to their reputation and operations by poor access and identity management amongst staff. The DTI survey reports that three fifths do not block staff access to inappropriate web-sites and only one in six scans outgoing mail for inappropriate content.

Keith Cottenden, Senior Forensic Investigator at CY4OR Computer Forensics, comments on the possible implications:

MORE

“One of the most malicious and real attacks a company faces is from spyware. This software is most likely to enter a company’s computer network through internet downloads and email attachments; simple logic dictates that a free reign as regards accessing the internet and email will significantly increase the chances of this form of attack.”

He continues: “Having no Acceptable Use Policy in place for staff use of the internet combined with a naive culture relating to IT security is a recipe for disaster. Staff should be vetted during the recruitment process with full background checks administered. This should be followed up with an education session about their security responsibilities and regular reminders. The possession of USB drives should also be carefully monitored – they can go unnoticed and could ultimately be used to steal your intellectual property.”

The survey managed by PricewaterhouseCoopers does report however, in the event of a security breach, the actual number of incidents being reported is rising. This could be attributed to a strengthening relationship of trust between UK Businesses and investigation teams such as Police and Computer Forensic Professionals, and is undoubtedly a positive step forward in the fight against cyber crime.

info@cy4or.co.uk
www.CY4OR.co.uk
0161 797 8123

ENDS...

Contact Carrie Moss
0161 797 8123
Carrie.moss@cy4or.co.uk

NOTE TO EDITORS

If you would like to sample any part of this release do please let Carrie or any member of the CY4OR team know.

Copyright CY4OR