

ERNST & YOUNG SURVEY

IT security goes by the board in bid to obey regulations

By Maija Palmer in London

Companies are spending so much of their IT budgets on complying with regulations such as Sarbanes-Oxley and the European Union's 8th Directive that they are neglecting other security threats, according to a new survey published today.

Ernst & Young's annual security survey found that compliance with regulations

had become the key driver for information security spending at nearly two-thirds of companies around the world, eclipsing concerns such as protection against computer viruses and worms.

Regulations stipulating that company executives take personal responsibility for the accuracy of corporate data, such as accounts, have caused many companies to

tighten internal IT controls, ensuring for example, that only authorised employees have access to accounts databases.

But the fact that executives can face prison sentences if companies fail to comply with regulations has led boards to focus a great deal of attention on the issue, to the detriment of other security problems, according to Anthony

Smythe, head of the information security practice at Ernst & Young.

"The rub in all of this is that there is so much money being spent on mundane remedial things that companies are missing other important issues," Mr Smythe said.

In particular, the study came to the conclusion that companies were still failing to assess security risks at

their suppliers and outsourcing partners.

Several high-profile cases have highlighted such risks in the past year, including press allegations in June that Indian call centre workers handling queries for UK banks were selling on customer account details for cash.

Despite such incidents, more than a fifth of companies are not looking at secu-

rity risks at suppliers at all. Of those that do have some risk management processes in place, most perform only an initial assessment.

Only 17 per cent carry out ongoing, independent third-party reviews of supplier security.

Companies are also failing to address security concerns related to emerging technologies, such as mobile computing, wireless networks

and internet telephony. Removable media in particular were becoming a problem, said Mr Smythe. Corporations had found it difficult to stop employees from downloading corporate data on to devices such as iPods or USB thumb drives and leaving with them.

However, less than half of companies surveyed identified removable media as a key security issue.