This story appeared on Computerweekly.com

http://www.computerweekly.com/Articles/2010/06/17/241631/Data-security-too-technology-focused-says-PwC-report.htm

Data security too technology focused, says PwC report

Warwick Ashford
Thursday 17 June 2010

Businesses should be making employees the first line of defense against data leaks, according to a report by PricewaterhouseCoopers (PwC).

Many organizations are complacent when it comes to information security and assume it will not happen to them, while individuals tend to think it is someone else's problem, research by PwC has found.

The traditional response to improving protection and reducing risk has been strongly biased towards spending more money on technology.

But this approach of finding technical solutions to what is widely perceived as a technical problem is misguided, according to Craig Lunnon, OneSecurity, PwC. "Technical solutions are too frequently being prescribed for people problems," he said.

Although technical defense is vital, systems are inherently vulnerable to both negligent and malicious acts by people, said Lunnon.

"Ignorance, confusion, anger or even curiosity can all give rise to incidents," he said.

Only 48% of UK organizations have an employee security awareness program, compared with 64% in the US and India, according to PwC's 2010 Global State of Information Security Survey.

People within organizations typically by-pass security controls that create cumbersome processes that inhibit them from doing their jobs, the PwC report said.

What is required, the report suggests, is a new approach in which an investment in understanding and influencing the behaviors of all those concerned is balanced against continued investment in technology.

PwC recommends that better engagement between security teams and the business is needed as well as higher levels of engagement between organizations and employees.

The solution is to invest in people and make them the first line of defense, rather than the cause of security incidents, the report said.

"The goal is that all those working for an organization are alert to risks, will want to act to protect information and will be actively supported in doing so," said Lunnon.

As the first line of defense, security-aware employees are often best placed to identify a potential breach or weak link, he said.

"Equally, they can prevent and reduce the impacts of incidents when they do occur," he added.

Investment in security awareness can help in

- Reducing incidents of theft, loss and fraud
- Avoiding breaches of law and/or regulation
- Ensuring continuous availability of business-critical information
- Protecting brand and reducing the potential for reputational risk
- Enabling the use of security as a positive marketing differentiator.