This story appeared on Itwire.com at
http://www.itwire.com/content/view/27400/53/

**Social networks pose security risks for enterprises**
by Peter Dinham
September 2, 2009

Employees accessing social networking sites like Facebook and Twitter while at work pose a problem for their bosses as they grapple with the dilemma of allowing them to use Web 2.0 tools responsibly, without sacrificing their business security and regulatory compliance requirements.

The problem arises as Facebook and other social network sites – once considered to be only consumer applications – are now moving quickly into the enterprise environment, creating both a risk of data leaks and new channels for malware.

In its latest report on the enterprise security market IDC suggests that organisations need to balance the business value of Web 2.0 technologies with the risks and security implications of many "non-secure and uncontrolled Web 2.0 environments."

According to IDC, the advances in Web 2.0 technologies require a new generation of Web security tools that go well beyond traditional URL filtering, and it says its latest survey of the market found that investments in security continue to be a priority for companies and organisations, with four out of 10 companies in IDC's Nordic and Benelux region expected to invest more in security moving forward — more than for most other IT investment areas.

IDC also says that compliance with industry regulations, such as SOX and HIPAA, is still a key driver for the adoption of mobile security software, "particularly solutions centered around information protection and control (IPC), vulnerability management, and secure access to corporate networks from mobile devices." IDC expects this trend to accelerate in the wake of "the lack of transparency that led to the current financial conditions."

The research firm says there has seen a growing trend among businesses to allow users, beginning at the executive level , to select the make and model of their choice when buying a business-critical device — laptop or converged mobile device (CMD), with the iPhone a prime example.

IDC warns that the proliferation of consumer devices housing or accessing corporate data is a cause for concern among those responsible for complying with regulatory statutes and securing sensitive corporate data.

**Nevertheless, IDC says that companies are in little doubt what the top and foremost challenge is when it comes to security – user awareness and behaviour – and it found that 42 percent of companies surveyed believed that "this is a key challenge now and in the future — a share significantly higher than any other security threat out there."**

And, the "threat" is real, according to users, says IDC, with its research revealing an "amazing" 81 percent of companies have had security issues because of user behaviour, and within this group, every third company reports having had "significant experiences" with security breaches because of user behaviour.