Global Security Survey Finds Internal Information Security Attacks Out-Growing External Security Attacks at World's Largest Financial Institutions

Published: 22/6/05

Internal information security attacks are out-growing external attacks at the world's largest financial institutions, according to the 2005 Global Security Survey released today by the Financial Services Industry practices of the member firms of Deloitte Touche Tohmatsu (DTT). Thirty five percent of respondents confirmed encountering attacks from inside their organisation within the last 12 months (up from 14% in 2004) compared to 26 percent from external sources (up from 23% in 2004). The third annual Global Security Survey acts as global benchmark for DTT and its member firms for the state of I.T. security in the financial sector and consisted of interviews with senior security officers from the world's top 100 global financial institutions.

Phishing and Pharming (luring people to disclose sensitive information by using bogus emails and websites) were two new additions to the top security threats financial institutions faced in the past year, highlighting the human factor as a new weakness in the security chain. The trend shift from external to internal attacks and tactics which exploit human behaviour vs. technological loopholes can be explained by the improved utilisation of I.T. security technologies, mainly by the increased use of anti-virus solutions (98% vs. 87% in 2004), Virtual Private Networks (79% vs. 75%) and content filtering and monitoring (76% vs. 60% in 2004).

"Financial institutions have made great progress in deploying technological solutions to protect themselves from direct external threats, however the rise and increased sophistication of attacks which target customers and internal attacks, indicate that there is a new threat that has to be addressed," says Adel Melek, a partner in the Canadian member firm and Global Leader of I.T. Risk Management & Security Services within the Global Financial Services Industry. "Strong customer's authentication, training and increased awareness can play a significant role in narrowing this gap."

However, as survey results show, security training and awareness has yet to top the agenda of Chief Information Security Officers (CISO), as less than half (46%) of respondents have training and awareness initiatives scheduled for the next 12 months. Training and awareness was at the bottom of the security initiatives list, far behind regulatory compliance (74%) and reporting and measurement (61%). These findings also align with financial institutions' future investment plans in security, with the most money targeted for security tools (64%) compared to only 15% for employees awareness and training. There are very few financial institutions who have any plans for customer's security awareness.

"In an attempt to minimise the human risk factor, financial institutions have been focusing on enterprise-wide solutions." Gerry Fitzpatrick, Enterprise Risk Services

Partner at Deloitte in Dublin. "With threats such as identity theft, phishing and pharming on the rise, organisations should be implementing identity management solutions, encompassing access, vulnerability, patch and security event management. These solutions should be augmented by security training and awareness if organisations are to minimise the number of human behavioural threats."

Additional Key Findings of the Survey:

- While close to half (48%) of respondents perceive lack of employee awareness as one of their top challenges, security training and awareness measurements implemented in the past 12 months declined from 77% in the previous survey to 65% this year

- Almost three-quarters (74%) of respondents choose to outsource at least one I.T. function, but (27%) do not conduct regular assessments of the security outsourcer's compliance with security requirements

- While 86% of organisations with a CISO indicated that this function reports directly to the board or to the C suite, only about one-third of the organisations interviewed feel that security has been similarly recognised as a critical area of business

- Unrealistic timelines and budgets (56%) topped respondents' list of common reasons for security project failures, followed by integration problems due to poor up-front design and architecture (48%) and lack of buy-in from business owners (34%)