This story on SourceWire at
http://www.sourcewire.com/releases/rel_display.php?relid=47028
April 17, 2009

Security Managers Warned to Address Employees Flouting Rules

Employees Flouting Rules; Survey from (ISC)2 and Infosecurity Europe 2009 reveals issues with accountability and training

London -- Too many companies leave themselves vulnerable to employees' ignorance or purposeful flouting of the rules when it comes to information security, suggests a survey conducted by (ISC)2 not-for-profit global leader in educating and certifying information security professionals throughout their careers and Infosecurity Europe 2009, the number one Information Security event in Europe. Focused on the 'basics' of policy management, the survey revealed that organisations are becoming confident in their ability to comply with the policies and procedures set out to secure their organisations. Analysis of the results, however, reveal education efforts to be immature, with most concerns relating to accountability and company-wide understanding of what is required.

The survey questioned 737 information security professionals last month about their organisation's efforts in policy and awareness management. A great majority, 80 percent, said their company's ability to comply with security policy was satisfactory, good or very good, leaving only 20 percent saying they were dissatisfied. However, this confident stance was tempered by concerns from nearly half of the respondents over a lack of training (48 percent) and poor employee understanding of policy (46 percent); a lack of defined accountability (42 percent); and an unsupportive company culture (48 percent). These obstacles to compliance with policy were cited by significantly more respondents than other issues of traditional concern, including a lack of budget, which only 22 percent were concerned about, and the ability to procure the latest technology, which concerned only 19 percent of respondents.

"The challenges are shifting from the systems to the people," says John Colley, CISSP, managing director for EMEA (Europe, Middle East, Africa) for (ISC)2. "The relatively little concern expressed over budgets suggests security continues to be viewed as a business imperative, even in the current economic climate. Unfortunately, security requirements are not yet well understood, or worse flouted, often with management support, in order to get a job done. There is a colossal task ahead to ensure all employees understand the why's and wherefore's of what is being asked of them."

"A fifth of information security professionals are dissatisfied with their companies ability to comply with security policy, and this is where people can be your greatest asset or liability, says Tamar Beck, Group Event Director, Infosecurity Europe. Improving information security awareness and changing behaviour is essential in the new collaborative working environment. People, process, technology are the foundation of information security, it starts with educating people and that is why we place so much emphasis on providing a comprehensive free

education programme at Infosecurity Europe. When information security fails, it often does so spectacularly and with huge adverse publicity. Sadly it is often only once an organisations has suffered a public security breach that information security is given backing from the top to educate people, improve processes and implement technology to ensure it never happens again."

When asked whether their organisations tracked security policy, the majority of respondents, 63 percent, said yes, and a similar number, 60 percent, identified that there were sanctions for non-compliance, while only two percent felt that those sanctions were understood company-wide. The survey also queried efforts to educate employees about policies and expectations. The bulk of the efforts to educate employees formally were said to be online, with 56 percent of respondents identifying this method, while 35 percent are using an employee newsletter, and 35 percent said expectations were written into employee contracts. Only a quarter reported in-person training programs. A significant number are identifying the need to manage data, with 72 percent reporting they had a data classification policy, which according to Colley, is a first step toward understanding the human challenges ahead.

"Clearly, we are still in a very immature phase when it comes to security awareness. The generic program delivered by the company intranet cannot be adequate, because one size does not necessarily fit all. Stock must be taken of each business unit's objectives and dependencies and how they relate to the organisation's overall security controls that have been developed so that employees learn to respect rather than flaunt them," says Colley. "A better understanding of data will lead to a better understanding of what users are doing with it, providing richer context for information security strategy and the supporting defences."