Mobile Devices May Pose Greatest Threat to Confidential Information

ROLLING MEADOWS, Ill. -- (BUSINESS WIRE) -- ISACA today released a white paper detailing how the increasing popularity of mobile devices poses a significant threat of leaking confidential enterprise information and intellectual property.

In the complimentary “Securing Mobile Devices” paper, ISACA, a global association for enterprise governance of information technology, notes that wireless networks, typically less secure than wired networks, leave information at greater risk. From smartphones to USB sticks, many devices store unencrypted data, which can result in sensitive information being intercepted, stolen or lost. Mobile devices are also targeted by malware attacks as employees carry them beyond the protection of their company’s network.

“Ironically, many of the risks associated with mobile devices exist because of their biggest benefit: portability,” said ISACA project development team member Mark Lobel, CISA, CISM, CISSP, and principal, PricewaterhouseCoopers. “To help their companies protect intellectual property and sustain competitive advantage, information security managers need to create an easily understood and executable policy that protects against risks related to leaking confidential data and malware.”

According to the Ponemon Institute’s Global 2009 Annual Study on Cost of a Data Breach, 32 percent of data breaches in the study involved lost or stolen laptop computers or other mobile data-bearing devices. While the average organizational cost of a breach was US $3.4 million, all countries in the study reported noticeably higher data breach costs associated with mobile incidents.

Governance frameworks such as COBIT or Risk IT will help businesses ensure that process and policy changes are implemented, and appropriate levels of security are applied. ISACA’s recommendations for a mobile device strategy include:

- Define allowable device types (enterprise-issued vs. personal).
- Define the nature of services accessible through mobile devices.
- Identify the way employees use devices; address corporate culture as well as human factors. (For example, one in 10 Americans who use a mobile work device plan to use it for holiday shopping.*)
- Integrate enterprise-issued devices into an asset management program.
- Describe the authentication and encryption that must be present on devices.
- Clarify how data should be securely stored and transmitted.

"Mobile technology can offer enterprises valuable benefits, from increased productivity to better customer service, but they can be realized only if the enterprise manages the technology effectively—for value and risk," said Adam Meyers, member of ISACA's project development team and senior principal at SRA International.

For details, download the free Securing Mobile Devices at www.isaca.org/mobiledevices.