



Mobile Devices May Pose Greatest Threat to Confidential Information: New ISACA White Paper

Mobile device protection should move to top of security agenda as usage, new features expand

ROLLING MEADOWS, Ill., USA (3 August 2010)—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 new white paper titled "[Securing Mobile Devices](#)," ISACA, a leading global association for enterprise governance of information technology (IT), noted that the use of wireless networks, typically less secure than wired networks, leaves information at greater risk for interception. From smartphones to USB sticks, many devices also store data that are unencrypted, which can result in sensitive information being compromised through interception and device theft or loss. Mobile devices can also be the targets of malware attacks as employees carry them beyond the protection of their company's network.

The white paper notes that a lack of enterprise control of physical devices, along with the growing practice of employees using personal devices for business, has increased mobile device risk levels.

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

"Ironically, many of the risks associated with mobile devices exist because of their biggest benefit: portability," said ISACA white paper project development team member Mark Lobel, CISA, CISM, CISSP, and principal, PricewaterhouseCoopers. "To help their company meet its goals of protecting intellectual property and sustaining 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."

A governance framework such as COBIT or Risk IT will help businesses ensure that process and policy changes are implemented and understood, and that appropriate levels of security are applied to prevent data loss. ISACA advocates that the following issues be considered when designing a mobile device strategy:

- Define allowable device types (enterprise-issued only vs. personal devices).
- Define the nature of services accessible through the devices.
- Identify the way employees use the devices, taking into account the organization's 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 all enterprise-issued devices into an asset management program.
- Describe the type of authentication and encryption that must be present on devices.
- Clarify how data should be securely stored and transmitted.

"Mobile technology can offer enterprises several highly valued benefits, from increased productivity to better customer service, but it is important to recognize that these benefits can be realized only if the enterprise manages the technology effectively—for both value and risk," said Adam Meyers, a member of ISACA's white paper project development team and senior principal at SRA International.

For a detailed discussion about risks and recommended strategies, download a free copy of the *Securing Mobile Devices* white paper at www.isaca.org/mobiledevices.

*SOURCE: ISACA Shopping on the Job: Online Holiday Shopping and Workplace Internet Safety, 2009

About ISACA

With more than 86,000 constituents in more than 160 countries, ISACA® (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

Contacts

Kristen Kessinger, ISACA, +1.847.660.5512,
news@isaca.org

Marv Gellman, Ketchum, +1.646.935.3907,
marv.gellman@ketchum.com

This communication, including any attachments, does not necessarily represent official policy of Seccuris Inc. Please see <http://www.seccuris.com/Contact-PrivacyPolicy.htm> for further details about Seccuris Inc.'s Privacy Policy. If you have received this communication in error, please notify Seccuris Inc. at info@seccuris.com or at 1-866-644-8442.