@ISACA
RELEVANT, TIMELY NEWS
Volume 3, 2 February 2011

5 Ways to Limit Data Leakage and Exposure

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

1. **Develop a clean-desk policy that includes a clean-white-board policy for conference rooms and public areas.** Data leakage and exposure can come from the most obvious and innocent of oversights by personnel who have access to or handle sensitive data. A clean desk policy will ensure that sensitive information that is being used during the business day is not viewed or removed by unauthorized personnel when not under the direct control of the authorized personnel. A clean-white-board policy (which includes nightly cleaning of conference rooms and public areas) will ensure that sensitive information is not viewed by personnel who are appropriately using facilities but are not authorized to view sensitive data.

1. **Implement secure printing.** Even in the age of the paperless office, more and more people are printing sensitive materials than ever before. Sensitive documents are often left at communal printers for long periods of time where anyone can read them or collect the printouts. Using secure printing capabilities, such as follow-me printing or PIN-required printing for sensitive documents, will ensure that the printer only activates when the authorized user is near the printer and ready to pick up the printout.

2. **Implement and maintain an asset inventory.** Data leakage and exposure often occur when sensitive or controlled data are unaccounted for and not in the direct control of the data owners. Implementing and maintaining an asset inventory of both physical and logical data assets will allow an organization to identify and classify data and apply appropriate controls.

3. **Implement trust-but-verify policies and procedures for sensitive data.** The unfortunate reality of data leakage often is the fact that an insider either knowingly or unknowingly contributed to the incident. Individuals are less likely to act upon a malicious action, such as data theft, if they know their activities are being monitored. Implementing trust-but-verify policies and procedures for access to and handling of sensitive data will provide protection to both the individual and organization. The individual with privileged access will not have to

worry about wrongful prosecution and the organization can quickly identify the scope as well as methods and practices used if a data leakage incident were to occur. Examples of trust-but-verify policy and procedures are pervasive and consistent logging and monitoring of all access and activities to technical infrastructure and environments that contain sensitive data.

4. **Establish hardware configuration password protection.** The ability for data leakage and exposure to occur has been greatly enhanced by the advanced technologies organizations deploy to their users and the vast amount of data that they store on these technologies. One area that should be protected in these situations but is often neglected is the hardware configuration's basic input/output system (BIOS) settings. Once an organization has established the settings for its users, the settings should be password-protected to prevent the user from changing them. This is especially important in the case of Bluetooth-enabled devices, which can allow a user to establish a short-range data network connection to mass storage devices (including smartphones) without being detected by typical network or application controls such as network-based intrusion detection or data leak prevention tools.

More information on data leak prevention is available in ISACA's **Data Leak Prevention** white paper, as a complimentary download to members and nonmembers.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.