



AuditOne Advisory

From Bud Genovese, CEO

The proliferation of mobile computing devices may be increasing bank productivity but it is also creating major network security and management problems for the Information Technology department. For this month's AuditOne Advisory, I'd like to share an article on this subject recently published in *Western Banking* magazine and written by two AuditOne executives, Len Filppu and Marv Chen, CISSP, Technology Practices Manager.

Moving Targets: How to Manage the High Risk of Mobile Computing Devices

Imagine you've lost your Blackberry which contained the last 17 customer loan applications you were working on and internal e-mails regarding a proposed merger of your bank. Making matters worse, it was your own personal Blackberry, not one provided to you by the IT department!

The explosion of mobile computing devices (MCD) such as laptops, smartphones, and handheld personal digital assistants in today's banking industry has created a risky security environment. Banks face the issue of lost or stolen MCDs that contain private and sensitive financial, personnel, business, and customer information. Additionally, bank staff routinely use personal MCDs for bank business, plugging them into the bank's systems without explicit permission. The need to manage and secure MCD use is paramount today.

MCDs are productivity enhancers. They allow bank staff to be mobile and to get the job done on the go. They allow for more off-site visits to clients and vendors, improved customer response times, real time team and distance communications, and faster decision making.

But MCDs can be misplaced, stolen or their contents "sniffed out" via wireless communications hack attacks from hundreds of feet away. Devices can become infected with viruses that threaten the bank's entire IT network. Attackers can install spyware programs that capture the keystrokes of passwords and sensitive emails. And because customers often send banks confidential personal information, the risks are high for costly Gramm-Leach-Bliley Act (GLBA) information security violations.

What can banks do to manage the growing risk? The first step is to conduct a full IT risk assessment that methodically determines what devices (both authorized and unauthorized) currently exist in the environment, which staff use them, and for what purposes. Consider this a snapshot of current MCD usage.

Banks should then develop a Mobile Computing Device Policy which defines standards, procedures, and best practices. Since different products have different security feature sets, and too many diverse products become unmanageable, most banks start by standardizing on products. Then it's important to develop an authorized use and user policy that spells out who can use the devices, for what legitimate purposes, and makes MCD users aware of their professional and regulatory responsibilities.

Per GLBA information security guidelines, banks should develop a lost device policy/ incident response plan that includes:

- Procedures to limit the negative impact of any lost devices (for example, activate a remote “kill switch” to delete data);
- Investigative procedures to ascertain whether non public personal information has a reasonable chance of actually being compromised;
- Written procedures for customer notification according to the requirements of GLBA and local laws.

Digging deeper into technological security solutions, banks should consider implementing these recommended industry best practices:

- Require that MCD users not be allowed to install software not approved by the IT department;
- Remind users to keep MCDs secure and out-of-sight when not attended;
- Require the use of strong passwords/PINs in order to log into the system;
- Require entry of passwords/PINs after a certain period of inactivity;
- Require installation of personal firewalls for all laptops and MCDs;
- Use encryption/turn on encryption for both data storage and data transmission;
- Implement enterprise software that can push down security settings to MCDs;
- Enterprise software should provide robust end-to-end encrypted data transmission and feature a remote “kill switch” that deletes all data if the MCD is lost or stolen;
- IT should require regular back-up of MCD data;
- Keep firmware and patches up-to-date on all devices.

Although wireless technology security has improved over the years, it is still vulnerable to remote hacking attacks. Wireless communications should be sent via tried-and-tested end-to-end encryption protocols such as SSL (Secure Sockets Layer), SSH (Secure Shell), IPSec (IP Security), and Virtual Private Networks.

Bluetooth is widely used as a wireless communications technology. Because of inherent risks with any wireless technology, banks should enable Bluetooth only if really needed. Additionally, banks should regularly check the list of paired devices to ensure there are no unknown devices on the list, require long and hard-to-guess PINs (not 9999) for devices, keep devices in “hidden” mode, and reject all mysterious un-requested pairing requests.

By following these basic guidelines, banks can minimize and manage the risks associated with the use of productivity-enhancing MCDs. Remember that Blackberry you lost in the opening paragraph? Well, you should now have a backup copy of all your data, and you can remotely delete all the information contained on the device.

Bud Genovese is founder and CEO of AuditOne LLC, a California-based internal audit firm that focuses only on banks and their service providers. Mr. Genovese pioneered the concept of providing comprehensive, affordable, independent internal audit services by gathering wide-ranging, world-class expertise within one firm. AuditOne now serves over 110 clients throughout the Western United States, and nationally. Contact Bud Genovese at 408-980-8099 or bud.genovese@auditone.com