



By Len Filppu with Marv Chen and Nigel Sampson

---

Technology marches forward at such blinding speeds that yesterday's innovations can quickly become routine, taken for granted, even overlooked. But as banking offers more complex online and remote services, neglecting any aspect of the Information Security operation invites risk from without and within, and may prove costly in terms of profitability and reputation. Here are seven information security issues easily overlooked by banks today, along with information on what problems to look for, how to diagnose them, and how to fix them.

**1: Third-party devices on the network do not have up-to-date security patches, service packs, or hot fixes.**

*Risk Considerations:* Some institutions use third-party applications that require a device on the institution's internal network. However, these devices are not part of the institution's patch management policy. The institution's network is only as secure as its weakest point. An intruder can scan the internal network and exploit the weakest point in the network to obtain information or cause a denial-of-service attack. Any device that permanently resides on the institution's network becomes the responsibility of that institution and must conform to the institution's patch management policy and internal security policies and procedures.

*Possible Solutions:* Confer with third-party vendors who have devices on the institution's network, and obtain verification that their devices will be maintained regularly and will have the latest operating system service packs, patches, and hot fixes.

**2: Contractors/consultants use a shared login account with administrative rights.**

*Risk Considerations:* Activity on the system cannot be traced back (attributed) to specific individuals because the account is shared among multiple contractors/consultants/people. If a contractor is terminated by the vendor company, that contractor may still have the account password. The risks are exacerbated because these accounts have administrative rights. Per FFIEC guidelines and international information security standards, treatment login account and passwords for contractors/consultants should be consistent with policies governing employee user accounts. Whatever high-technology information security systems the bank has in place will prove inadequate if any unauthorized person is given access and such access cannot be traced back to a specific individual.

*Possible Solutions:* Create individual logins for each contractor/consultant. Require vendors to inform the bank when any individual is terminated. Alternatively, if vendors consider the above process unmanageable, keep shared vendor accounts disabled and only enable them when they are actually being used.

**3: Default passwords are not changed when network-based equipment is put into production.**

*Risk Considerations:* This is common with network routers and switches, and especially common with voice mail and video surveillance systems. Some vendors install this equipment without changing the default passwords.

*Possible Solutions:* Ensure default system passwords are changed and secured with the proper persons (administrators) before equipment is put into production. Formalize a production checklist to include this step if necessary.

#### **4: Separation of duties (SoD) is not in place for authorizing and implementing users' access rights.**

*Risk Considerations:* The objective of separation of duties is to prevent fraud and errors. Banks must ensure that no one person can complete the task of authorizing and implementing users' access rights.

*Possible Solutions:* For obvious reasons, SoD is difficult and costly to achieve, especially for community banks. The job of authorizing users' access rights can be assigned to supervisors or Human Resources, with the security administrators implementing those access rights in the system. Changes made by the security administrators should be independently reviewed, or alternatively in small banks, a primary and secondary security administrator can review each other's activity.

#### **5: Too many accounts with administrator rights.**

*Risk Considerations:* The more administrator accounts that exist, the more likely it is for intruders to hack accounts with administrator privileges.

*Possible Solutions:* Limit the number of administrator accounts on the network. Plan access rights and focus privileges based on title, experience, and responsibilities. Create "sub-administrator" or "power-user" accounts with specific access rights to specific resources (i.e. password resets) instead of accounts with full administrator rights.

#### **6: Email security and encryption policies are not in place.**

*Risk Considerations:* Email is a critical business application, and is the preferred method of communication. Although some institutions may not regularly send NPPI (Non Public Private Information) via email, they may have a need at some point to use email as the method of sending NPPI to external destinations. Regardless, institutions that use email and have the ability to send email externally should have a secure email policy and a documented method of sending secured email.

*Possible Solutions:* There are a number of applications that can facilitate secured email transmission. Institutions should ensure that the application is easy to use, can be implemented easily, and does not require a third-party to relay the email.

#### **7: SNMP (Simple Network Management Protocol) community strings are set to "public" or "private."**

*Risk Considerations:* Intruders can use simple network scanning tools with these SNMP settings to obtain information concerning open shares, user accounts, printers, internal networks, and other IT data. SNMP can be configured on routers, switches, firewalls, IDSs (Intrusion Detection Systems), servers, workstations, and printers. Manufacturers configure the SNMP settings to these default settings to allow their devices to be monitored and managed by network management applications.

*Possible Solutions:* SNMP is a useful tool for managing and monitoring network equipment. The SNMP community string for each critical device should be configured to a setting unique to that corporation. Alternatively, SNMP services can be disabled.

*Len Filppu is director of marketing communications for AuditOne, LLC ([www.audit-one.com](http://www.audit-one.com)), a California-based independent internal audit firm specializing in banks and their service providers throughout the United States. Marv Chen ([marv.chen@audit-one.com](mailto:marv.chen@audit-one.com)) is AuditOne's director of product development and has 15 years high level technical experience in the banking and financial services industries. Nigel Sampson ([nigel.sampson@audit-one.com](mailto:nigel.sampson@audit-one.com)) is AuditOne's senior IT associate, and has over 20 years experience in computer operations and networking.*

[http://www.wib.org/publications\\_resources/article\\_library/2007-08/sep09\\_overlooked.html](http://www.wib.org/publications_resources/article_library/2007-08/sep09_overlooked.html)

---