



## Protecting Against the Enemy Within

*By Len Filppu, with John Barchie, CISSP*

Recent news that several U.S. banks notified thousands of customers that their accounts may have been breached by bank insiders illegally selling screen shot data highlights a serious weakness in today's bank IT network security. While banks generally have done a good job of protecting their IT networks from external assault by hackers and cyberspace crooks, banks must now focus attention on protecting against *internal* malicious intent.

### **Internal Threat is a Widespread Problem**

The problem of internal threats to bank IT networks is widespread, and most banks are vulnerable. According to the August 2004 *Insider Threat Study* by the United States Secret Service and Carnegie Mellon University Software Engineering Institute's CERT Coordination Center, most banking and finance sector insider attack incidents examined required minimal technical sophistication or skill to execute.

Most of the cases studied involved the simple exploitation of non-technical vulnerabilities such as institutional business practices, policies and procedures. Most perpetrators were authorized users employing legitimate user commands. They planned their actions, sought financial gain and acted while on the job. In addition to financial losses, banks suffered damage to the integrity of their businesses, security and reputations.

To reduce the risk of malicious insider threat, banks must regularly and methodically protect their IT networks from internal exploitation by employing both technical and procedural reviews. Effective internal security requires several overlapping controls, so that one compromise of a control does not put an institution at risk.

### **One-Two Punch Protection**

There are two basic tools to use in this job: 1) An IT Audit that follows guidelines of FFIEC Information Technology Exam manuals, and 2) A Gramm-Leach-Bliley Act (GLBA) Risk Assessment & Audit. Essentially, the IT Audit examines overall general and technical controls, while the GLBA Risk Assessment & Audit focus on compliance with procedural/administrative controls. This one-two punch gives banks a fighting chance for protection against internal attack by examining detective and preventative security controls on both the technological and procedural fronts.

### **IT Audits**

A solid IT Audit should apply a multiple-security domain approach that looks beyond the bank's information technology and security to examine its overall business practices. Comprehensive IT Audits should examine a bank's:

- Security education process
- User and administrator activity
- Overlapping administrative and technical controls
- Host intrusion detection
- Encryption
- Malicious Code
- Security testing
- IT management
- Access and authentication controls
- Physical security
- Remote banking and intrusion detection systems

- Networking, host, and desktop technical and administrative controls
- Personnel Security
- Electronic and paper-based media handling
- Business continuity considerations
- Vendor management
- Process of regular risk assessments.

The majority of IT technical controls are geared toward protecting data integrity, confidentiality and availability. Because customer non-public information is ubiquitous throughout banks, special care must be taken to ensure its confidentiality. This is the strength of the GLBA Risk Assessment & Audit, which measures and strengthens administrative controls that prevent accidental or malicious leakage of personal data.

### **GLBA Risk Assessment & Audit**

Regulators expect banks to perform their own GLBA Risk Assessments on an annual basis. Whether performing the work internally or hiring outside consultants, banks should comply with GLBA by following a simple template that covers:

- Identification of data location
- Threat types
- Inherent likelihood and impact of threats
- Mitigating bank controls
- Residual probability and impact.

### **Certified Expertise for Increasingly Complex Technology**

Bank technology is rapidly changing, heterogeneous and increasing complex. Banks must be certain that their IT, information security and GLBA audit professionals - whether internal or outsourced - are technically qualified, credentialed and possess the depth of knowledge and expertise to drill down capably into the technology and systems to deliver informed assessments.

### **Immediate “Best Practice” Steps**

In addition to periodic, thorough IT and GLBA Audits, banks can take immediate steps today to help guard against the risk of malicious internal acts. These simple “best practice” steps include: regular reviews of administrator and user activity logs, ongoing security awareness training for employees, regular reviews of user and group access rights, locking down desktops, encouraging employees to take two-week vacations, and requiring the documentation of actual procedures.

Safeguarding against malicious internal threats to IT networks is a reality banks must face and act upon now. Increased security can be achieved by conducting regular, thorough IT and GLBA audits. Following these procedures will provide protection against the enemy within, reduce risk and help ensure the security and integrity of bank networks, data, businesses and reputations.

*Len Filppu is executive vice president of AuditOne LLC ([www.audit-one.com](http://www.audit-one.com)), in San Jose, Calif. He can be reached at 408-980-8099 or [len.filppu@audit-one.com](mailto:len.filppu@audit-one.com). John Barchie, CISSP, CNE, MCSE, is an AuditOne senior IT associate. He can be reached at [john.barchie@audit-one.com](mailto:john.barchie@audit-one.com).*

[http://www.wib.org/publications\\_resources/article\\_library/2005-06/aug05\\_enemy\\_within.html](http://www.wib.org/publications_resources/article_library/2005-06/aug05_enemy_within.html)