



Hack Attack! Thwarting Electronic Break-Ins

By Len Filppu with Marv Chen, CISA & CISSP

Today's bank networks, websites and online transaction systems are under constant attack by devious hackers, those technically proficient computer criminals operating anonymously in cyberspace. Hackers employ sophisticated automated technologies that systematically scour bank IT systems on a relentless search for weak points to penetrate illegally. This modern scourge of hack attacks grows.

Viruses abound, creating havoc, crashing systems, flooding mailboxes, and causing other denial of service nuisances that reduce productivity and profitability. "Phishing" attacks use fraudulent emails and websites designed to fool recipients into divulging personal financial data such as passwords and credit card, account and social security numbers. And banks must especially guard against Trojans, malicious software that exploits an IT security hole, implants internally on the system, and is designed to steal data and gain access to the network.

A new form of high tech blackmail is now being perpetrated on banks quietly, below the attention of news and even law enforcement organizations. Hackers are breaking into bank networks and demanding cash payments to keep quiet about the details of a bank's compromised network security.

How can banks deal with the variety and virulence of these attacks? In addition to constant vigilance, the answer is updated technology, informed security controls and procedures, and proper testing.

The minimum basic IT security controls that banks should have in place are:

- Strong passwords (8 characters or more—numbers and letters and expiration dates)
- Password protection for all servers (hosts) and network communications devices such as routers and switches
- Regular review of firewall and IDS (intrusion detection system) logs
- A properly designed Internet perimeter or in-depth defense architecture
- Automated tools to update patches on servers and virus signature files
- A secure remote access environment requiring users to have firewalls, virus protection, two-factor authentication
- Periodic independent network vulnerability and penetration testing.

In addition to basic technology security controls, banks should develop and implement comprehensive information security policies and procedures, such as an Incident Response Plan. Typical IT security policies and procedures include:

- Education of bank personnel on IT security issues
- Periodic review of firewall, IDS logs and router configurations
- Establishment of a Computer Emergency Response Team (CERT)

- Development of an Incident Response Plan
- Identification of the steps to take and the personnel to contact in the event of an incident
- Proactive customer education on security issues (prevention of “phishing”).

Another method of enhancing IT security is to make certain that bank workstations and remote user systems cannot be used as vectors for attack by malicious software or even insiders with dubious intent. Internal desktops should be “locked down,” meaning that users cannot download executable files, cannot install programs, and cannot change workstations settings. Remote user access to the network should be limited, and their systems secured.

In the event of a substantial IT network security compromise, banks are advised to deploy and follow the process designed specifically for the bank by the Computer Emergency Response Team. Typical CERT steps might include:

- Shut down the network
- Review the IDS logs
- Locate the intrusion
- Close security holes
- File a SAR or appropriate report
- Contact the FBI and/or local authorities
- Notify appropriate bank executives and clients.

Testing and auditing of bank IT systems is essential to maintaining proper network security and to staying ahead of the evolving technology employed by hackers. Network vulnerability testing checks a bank’s system against a known database of existing vulnerabilities. It is also critical that banks subject their applications to direct penetration testing, in which an IT expert with advanced knowledge about hacking techniques attempts to compromise specific bank applications. It is also now recommended that internal testing of bank personnel be performed to ensure that information security education is effective.

Because of the growth of electronic banking networks and the sophistication of hackers, bank industry regulators are focusing greater attention on the IT security area. The 2002 FFIEC Information Security Handbook increased emphasis on IT security procedures, training, business continuity planning, and back up. Additionally, regulatory expectations are high and focused on bank compliance with the Gramm-Leach-Bliley Act’s protection of non-public personal information.

Technology is creating for banks a new world of increased productivity and profitability. But it’s also a world of increased exploitive opportunity for criminal hackers. To protect the bottom line, maintain the competitive edge and preserve valuable reputations, banks must fight back against hack attacks by employing proper technology, security procedures and testing.

Len Filppu is executive vice president of AuditOne LLC (www.audit-one.com), a San Jose, California-based independent internal audit firm with a specialization in IT auditing and network vulnerability & penetration testing for banks and their service providers throughout the western U.S. He can be reached at 408-980-8099 or len.filppu@audit-one.com. Marv Chen, CISA & CISSP, is an AuditOne IT Associate. He can be reached at marvin.chen@auditonellc.com.

http://www.wib.org/publications_resources/article_library/2005-06/dec04_hack.html