Putting Management to the Security Test

By Lawrence Levine

ACB Business Partners aligns with best-in-class companies to provide member-advantaged business solutions designed to enhance your bank's competitiveness and to improve your bottom line. The ACB/SecurePipe Alliance delivers managed security solutions at a significant discount for ACB members. SecurePipe keeps your bank safe with fully integrated hardware and software solutions, managed from its secure operations center, to ensure the ongoing integrity of your bank's networks.

Perhaps the greatest myth concerning information security is that it is solely a technology issue rather than a larger management issue.

The more banks face the increasingly common and sophisticated techniques used to compromise network security, the more apparent it becomes that the corruption or theft of information assets should be part of the overall risk management strategy of all institutions, regardless of their size.

It's time to get top management involved.

The Gramm-Leach-Bliley Act brings the issue to the board table, but bank management needs to do more than just meet regulatory requirements. They need to engage actively in the information security decision-making process.

Any compromise of the integrity of your information assets will undoubtedly affect your bottom line—and this makes information security an issue for which all responsible senior managers must be held accountable. For most banks, purchasing flood or fire insurance, installing a building security system and even establishing day-to-day privacy practices, such as shredding sensitive documents, are all considered to be safety precautions against potential threats to the viability of your business.

Senior managers rarely question the need to outsource security monitoring of physical buildings and don't merely leave the possibility of physical damage by elements such as flood or fire to chance; network security should be no different.

Your data network is a virtual door to your information assets—property which happens to be more valuable than most of your physical assets, merely because a compromise to the integrity of your information may be irreparable. Even banks without on-site account processing and Internet banking have a lot to lose—a bank's reputation is intrinsically tied to security. Additionally, any compromise at the main office network will create an open path to off-site hacking; anything that a teller can do at his or her PC, an attacker could do remotely.

Just as an art museum that has a rare gem in its possession will seek to provide layers of security to protect it from theft or damage, your institution must create layers of security around information assets—and these layers must begin from the top of the organization and be instituted throughout.

The cost of a network security breach can range significantly depending on your bank. The consequences will vary according to the scope of the intrusion, but the net effect is a strike to your bottom line.

This includes:

- Lost business revenue due to employee downtime.
- Wages paid to workers during downtime;
- Consulting time or internal resources necessary to rebuild compromised systems.
- Loss of information which must be recaptured.
- Customer confidence damage.
- Regulatory impact and legal consequences for breach of privacy under the Gramm-Leach-Bliley Act.

When taking these consequences into consideration, any manager can relate to the detrimental result of a network security compromise. So what should be the role of senior management in managing the risk of your network security?

Clearly, technology plays its role in the overall plan of safeguarding information assets, but it should only be used as a tool for the savvy risk manager rather than the be-all and end-all.

The hypothetical community bank may have had the most sophisticated security

Any compromise of the integrity of your information assets will undoubtedly affect your bottom line.

technology available, but with new attacks constantly barraging your networks and new software vulnerabilities discovered every day, it is important to ensure that security is being managed as an ongoing process, one driven by highly-trained people following stringent policies.

Like any other risk management issue, developing a network security plan must start with a thorough risk assessment.

The misconception that small banks have nothing important to lose is pervasive throughout the community banking industry—and yet it has been proven false in this time of anonymous cyber crime where indiscriminate attacks are made on any business where network weaknesses are easily identifed. Look at all direct and indirect consequences of a network breach before evaluating the options to manage that risk.

As with any security safeguards, you should create a specific information security program that assesses risk and identifies reasonable and foreseeable damages that could occur. The likelihood of potential damages such as expensive employee downtime, the need to re-build computers, and the destruction or theft of confidential customer information should be taken into account and a plan designed to defend against such actions that could occur.

Upper management should be responsible for designing an information security program commensurate with the scope of the institution's business activities and value of its information assets, and should implement and test this program on an ongoing basis.

Weighing the overall business impact of a compromise is a critical, albeit cumbersome task. Yet it is necessary in order to enact appropriate measures to protect your assets. The technology solutions available are many, but no single technology can replace a thorough security plan. There are no silver bullets to solving these problems.

A high level of management commitment and awareness coupled with diligence in the security management process will put your institution in the best position to tackle the risk effectively.

Lawrence Levine is the managing director of SecurePipe, Inc. For more information on how the ACB/SecurePipe Alliance can benefit your bank contact ACB Business Partners at (202) 857-5575 or e-mail anewcomb@acbankers.org. Visit www.AmericasCommunityBankers.com/Partners *for a complete menu of business solutions from ACB Business Partners.*