

Cost-Justifying Managed Security For Financial Institutions

By Lawrence Levine, Managing Director, SecurePipe Inc.

Securing your financial information assets is no longer just good business sense, Gramm-Leach-Bliley makes it the law. With budget and staff limitations, what is the best way to secure your institution?

The obvious method is to utilize your existing information technology infrastructure. Firewalls, intrusion detection systems (IDS), and even virtual private network (VPN) devices can easily be had off the shelf at your local electronic superstore. While anyone can plug these devices into their network, the challenges come in the area of configuration, maintenance, and the subsequent monitoring, reporting, and analysis of generated logs and alerts.

Compounding the problem of interpreting the information delivered from your security appliances is the fact that intruders operate around the clock, not just during normal business hours. Therefore, if you do not have staff onsite every day, 24 hours a day, at the very least your people need to be on call during off hours.

Even that would be insufficient, however, since reports from various security Web sites and mailing lists of new vulnerabilities and attack vectors are streaming in all day long. In many cases, a prudent response to this information mandates an immediate

update of IDS signatures or a change to the firewall rules. And, of course, your staff needs the expertise to discern which of these vulnerabilities truly represent a risk for your particular environment.

Given the burden of monitoring and responding to this ongoing assault, many organizations are turning to Managed Security Service Providers (MSSPs). By using an MSSP, a community bank is effectively outsourcing its security to specialists.

A typical MSSP will have a 24/7 network operations center staffed by trained security professionals. These security engineers configure and maintain security hardware by applying software patches and upgrading equipment. They also monitor and respond to generated logs and alerts. Their analysis helps them filter out the “false positives” that appear to be attacks but are not. The engineers work directly with their client banks to define and enforce security policies.

In considering the use of an MSSP, the issue of return on investment (ROI) arises. Initially, for straight comparison of in-house vs. outsourced security, the bank can calculate the inside expense by summarizing the cost of hardware, software, networking, ongoing hardware and software maintenance, and testing. Add in a dedicated secu-

rity person who can monitor your systems, apply the necessary hardware and software vendor patches, and review the firewall logs to look for security anomalies, daily.

Security engineers also need vendor training time and training classes to keep current and provide for the ongoing support of the systems. Don't forget that in addition to keeping the hardware and software patched, the security engineers must monitor and respond to incidents as they occur. And, they must stay current, on a daily if not hourly basis, with the current security threats. Larger financial institutions run three Internet security shifts a day, seven days a week.

Since an MSSP will either sell you hardware or have some sort of start-up fee, the infrastructure costs tend to equalize, leaving the largest consideration to be the monitoring function. What a bank is really purchasing from an MSSP is its staff: trained security professionals working around the clock to keep client companies secure. This leaves the bank's employees free to do what they do best: manage the bank's own environment.

Quantifying the benefit of this protection can be difficult. What is it worth to have a secure environment? Often, it is easier to measure the cost of insecurity.

What a bank is really purchasing from an MSSP is its staff: trained security professionals working around the clock to keep client companies secure.

What is the value of lost customers? What is the impact of damage to your integrity or your brand?

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

- 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.

Therefore, when considering the most effective solution for managing security, price cannot be the only metric. When an attack is mitigated or prevented, the money saved by limiting exposure can easily exceed the annual cost of the managed security provider. **6**

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 partnership offers 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 banks networks.

For more information on how the ACB/SecurePipe partnership can benefit your bank, contact Sam Lisker at (202) 857-5081 or slisker@acbankers.org. ACB Business Partners offers a complete menu of business solutions in mortgage, technology and payments, and financial and capital markets. Visit www.AmericasCommunityBankers.com/Partners to learn more.



ACB's 2004 National Spring Management Conference & Marketplace

April 25-28, 2004
Hilton Head Marriott Beach & Golf Resort
Hilton Head, SC

Register for
ACB's Popular
Golf Tournament

Get value-added solutions to improve your bank's bottom line.

Topics include:

- Best Human Capital Management Practices
- Identity Theft and Fraud Prevention
- Moving from Strategic Planning to Action Planning
- Profitable Commercial Banking
- Mutuality in the 21st Century
- Check 21 issues

Experts examine today's issues and help you tackle them head on. See the latest developments in banking technology at the Marketplace and gain invaluable contacts.

Earn 16 CPE credits!

To register, visit www.AmericasCommunityBankers.com/mtg or call (888) 872-0275, ext. 3153.