

# Network Protection:

## The First Step Toward Compliance

By Alan Simpkins

While Internet security solutions have become much smarter, threats continue to evolve and become much more sophisticated. In the past, viruses were predominantly transmitted when employees received a corrupt file attachment, opened it, and it infected their machine, as well as their company network. However, there has been a fundamental shift in how viruses are now transmitted and how they gain access to a company's network. These threats are especially dire in a climate where complex compliance requirements are holding financial services companies accountable for failing to protect customer data.

Perhaps the most notable piece of compliance legislation is the Gramm-Leach-Bliley Act (GLBA), which has two main components. The first is the need to protect nonpublic personal information (NPI) from unaffiliated third parties. Examples of NPI include credit card data, social security numbers, account numbers, addresses and information pertaining to warrants, summonses and other legal issues. The second component requires companies to maintain a "comprehensive written information security program," containing both technical and physical safeguards to protect customer information against a growing variety of threats.

Examples of these threats have been widely reported in the news, with the media giving ample coverage to viruses and worms, such as Blaster, Sasser and Bagle. Combined, the two worms, Blaster and Nachi, represented 24 percent of the August 2003 viral reports for Sophos, an antivirus company. As financial services companies enhance their security measures, they need to become experts on the threats lurking around every corner of the Internet and develop more effective methods for preventing these breaches.

So, how can your company mitigate the challenges presented by these new threats, and ensure the effective protection of customer data?

- **Rigorous Antivirus Use**

Once these viruses have been discovered, the way to contain them among network users is to launch regular virus updates to as many of the user population as possible.

- **Consolidation of Internet Access Points**

Consolidation of Internet access helps aid the enterprise in containment. It is easier to deploy intrusion detection technology, firewall rules, and spam protection at a few regional Internet gateways than in a highly distributed Internet environment.

- **Consistent Firewall Management Across the Enterprise**

A key to ensuring that basic threats are managed -- and that IT staffs avoid easily addressed threats -- is to ensure that firewall rules are consistent across the enterprise. It also ensures that the traffic being allowed follows corporate guidelines.

- **Quarterly Vulnerability Assessments**

Regular security assessments ensure that proactive security measures, such as caching and IDS are in fact working. Additionally, this type of testing evaluates the inherent vulnerability of the end systems and services -- whereas much of the security technology in existence today is directed at prevention. This helps you evaluate whether your security devices can be bypassed, and identify potential threats you may encounter if someone finds a way to bypass them.

- **Proper Patch Management**

This measure ensures that known issues with operating systems do not compromise network security, and that tools being used to secure the network are having the desired effect.

These types of assessments are key to meeting compliance requirements, such as those within Gramm-Leach-Bliley. While the above list of mitigating actions is not all-inclusive, it does address the core of the actions necessary to secure one's network against today's threats, as well as tomorrow's.

*Alan Simpkins is Practice Director of Security at Equant, 860-739-9951; email: alan.simpkins@equant.com; web: www.equant.com.*