

So You Think You Are Secure

Susan Orr
Susan Orr Consulting

Exploitations that threaten security are on the rise. Every day, news stories document the rampant growth of attacks and exploits. The types of attacks vary - Denial of Service (DoS), buffer overflow, identity theft, session hijacking, website defacements, email viruses, worms, phishing scams, and the list goes on. Experts estimate the attacks in 2003 more than doubled those seen in 2002 with billions of dollars in losses.¹ These same experts warn that 2004 will be even worse than 2003 - and so far they're right. This year the attacks have been even more frequent and more horrific. No matter which set of IT security indices you analyze, threats loom overhead, with financial services targeted more than any other industry. According to a 2004 Global Security Survey performed by Deloitte Touche, financial institutions are losing the war against hackers. Eighty-three percent of the survey respondents acknowledged that their systems had been compromised, many resulting in financial losses.²

Threats can originate from many sources including the Internet or from inside your institution, on the inside of your network, behind your firewall. The source can be as varied as a hacker scanning for vulnerabilities in your system or an unsuspecting employee or contractor connecting his infected laptop directly to the network, or there is the possibility someone has deployed a wireless access point on your network. What about your website, how quickly would you know if your site was defaced? Protection from the multitude of attacks requires deployment of security in layers – where each layer enhances overall security. What is “layered security”? Imagine slices of Swiss cheese. Swiss cheese, by nature, has many holes or entry points. Think of the holes as security risks. If you have one slice, you have many exposed holes. Adding slices, adds more exposure; however, layering the slices strategically, you begin to plug the holes. Eventually, with enough slices placed correctly, all of the holes are plugged. Equate this analogy to your environment. You add products and services, which by nature possess security risks, so you need to implement new security controls, monitoring, policies, and procedures to mitigate the risks. In other words layered security. A single layer of security will leave your systems exposed. For years, financial institutions have employed the layered approach for physical security, using vaults, locked computer rooms, and employee training and procedures. Furthermore, to ensure around-the-clock-protection, monitoring by means of security guards, alarm systems, motion detectors, and cameras are readily used. Layered network security is no different. Continuous monitoring is a vital component of layered security. Security best practices mandate

¹ 2003 CSI/FBI Computer Crime and Security Survey

² 2004 Global Security Survey, Deloitte

continuous monitoring to ensure protection of the whole environment, physical and logical, internal and external.

Many institutions inappropriately limit their security focus on the external environment and implement policies and controls consisting of firewalls and intrusion detection systems (IDS), only. A broader perspective is necessary; however, for Internet-exposed systems like web sites and e-commerce applications as well as internal network systems. Incorporating layered security provides a holistic and proactive perspective. Continuous around-the-clock monitoring of your whole environment, including transaction hijacking detection, website defacement detection, and unauthorized computer and wireless network detection is a vital layer of security.

Providing the appropriate layers of security is no longer just a “best practice” but a regulatory requirement. The Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to implement controls to ensure the confidentiality, security, and integrity of customer information and information systems. The Sarbanes Oxley Act of 2002 requires publicly traded companies to keep accurate records, implement appropriate internal controls, and provide an annual attestation on the integrity of financial reports and assessment of internal controls. For financial institutions that are \$500 million or more and not publicly traded, similar requirements exist under Federal Deposit Insurance Corporation Act (FDICA). The USA Patriot Act also requires institutions to ensure the identity of those performing online transactions. Financial institution regulators view the failure to provide an effective risk management program, which includes layered security as an unsafe and unsound banking practice. Furthermore, the FFIEC IT Security Handbook states that a reliance on a *single* control device or method creates a false sense of security, and institutions should consider layering controls. Industry best practices and regulatory requirements include sound risk management, acquiring adequate expertise, implementing adequate measures for authenticating and authorizing network users, regularly checking for vulnerabilities and addressing those vulnerabilities and monitoring remote users and third parties – in essence, layering security.

So if you think you are secure, unless you have implemented layered security and continuous monitoring, think again.

Susan Orr is a leading financial services expert with over 15 years of risk management experience as a bank examiner with the Federal Deposit Insurance Corporation (FDIC). She has held lead positions at the FDIC working on banking safety and soundness, information technology and security, and electronic banking risk management issues.

Susan was instrumental in key industry initiatives such as the FDIC E-Risk Strategic Initiatives Risk Monitoring Committee, the Chicago Region Interagency Technology Group, and the Federal Financial Institutions Examination Council (FFIEC) IT Handbook rewrites. She was also Vice President of Regulatory Compliance at Catbird Networks and holds the Certified Risk Professional (CRP) designation from the BAI Center for Certification and the Certified Information Systems Manager (CISM) designation from the Information Systems Audit and Control Association (ISACA).

Susan speaks regularly at risk management and security educational seminars and has authored numerous white papers on emerging information technology and security risk management topics.

