

● ● ● **How secure are you?**

Do you require your employees to use complex passwords and change them regularly? Is your virus protection software current and automatically performing updates? Do you regularly inspect your network traffic to uncover security problems? Do you have a written security policy that is actively enforced? Have you performed an outside scan of your firewall ports for accessible services? Are you meeting all the compliance standards for your industry?

As networks drive more business and are widely available to more users, they become more vulnerable to a broader range of security threats. Yesterday's security is no match for today's intruders, who are aggressively using sophisticated techniques to hack into systems and covering their tracks to make it more difficult for you to detect them. Network attacks can cause serious breaches in data confidentiality and integrity, as well as system downtime. They can be painfully expensive, and they can erode customer confidence.

● ● ● **Ensuring that your security shield is strong.**

Strong security is a compliance requirement of recent legislation, such as the Sarbanes-Oxley, Payment Card Industry, Gramm-Leach-Bliley, and HIPAA acts. What is strong security? The protection of your data, network equipment, and applications. Data protection means that company information is available when needed, is kept confidential, and maintains its integrity.

Our security review process not only looks at the security products you own, but digs into the policies and procedures that keep your defenses strong. We always start the review with a thorough discussion of your overall security posture so we can make sure that our recommendations fit your company culture and direction. We follow this with a series of activities you select from the list below.

continued

● ● ● A comprehensive security review.

Each review is a unique combination of activities chosen from the following topics:

BASELINE PERIMETER SECURITY REVIEW

DNS and TCP/IP publicly accessible information
Access to services from outside your network
Firewall configuration, rules, and log review
Router configuration and denial-of-service protection
Modem access
VPN configuration

INTERNAL CONFIGURATION INSPECTION

Network topology and protection of critical resources
Server configuration and log review
AS/400 and Unix/Linux host configuration
Internal scan for open services and intruder accessibility
Wireless review to check for “rogue” access points and security

COMPREHENSIVE TESTS

External penetration test to look for vulnerabilities
Internal servers and penetration test
Externally hosted Web server testing
Switch configuration review
Workstation configuration review
Remote access and laptop configuration review
Antivirus strategy and implementation review
Backup procedures and results review
Physical security review

CLIENT POLICIES AND PROCEDURES REVIEW

Logging/reporting/update
Security training and skill sets
Security policy documentation and user procedure
Security procedures for administrators, written and unwritten

● ● ● A result chock-full of specifics.

We often get feedback that our security reviews provide far more details and practical security recommendations than the typical audit. Our goal is to help you bridge the gap between your security goals and your current reality, so we leave you with a wealth of information that is easily turned into a roadmap for an improved security posture. The review results in two deliverables to help improve your network security:

- A summary of your current security environment and any areas of vulnerability we observed.
- A report with recommendations, including:
 - Product options, implementation strategies, policies, and configurations
 - Prioritized changes that will make your network more secure
 - Ongoing security enhancements



Our expertise.

NPI has been providing leading-edge security services since the inception of the Internet, anticipating the needs of businesses, testing the newest appliances and applications, and installing and monitoring “best-of-breed” products at security-sensitive businesses such as banks, insurance companies, health-care facilities, and law firms. We’ve worked with all the best firewall products and every type of connection available today. Our technicians hold coveted certifications from Cisco, Check Point, Juniper, and RSA, and attend national security conferences such as SANS. At NPI, we are committed to security as a core business.