

## **Cross Current Corporation Penetration Testing Services**

**Background:** Automated tools and widely-distributed information give virtually anyone the ability to search for potential targets on the Internet, examine them for vulnerabilities, and allow them to exploit those targets. The results can range from crashed systems to denial of internal or customer services to total compromise of your data and networks. Within an organization penetration risks can be exposed to vulnerabilities. The awareness and effort to manage this risk lies not only with IT personnel, but with business management and owners.

Internal and external penetration testing is an active effort by security professionals to assess the information security measures that you have implemented. The basic methodology for penetration testing is to discover exposed systems, evaluate them for weaknesses, determine how those vulnerabilities can be exploited, and report on solutions to improve your security.

**Objective:** Cross Current's objective in performing penetration testing on your network security is to discover system and network weaknesses, determine how they could be exploited by a malicious attacker, and identify network security improvements. For our penetration testing engagements, we adhere to the standards of the Information Systems Audit and Control Association (ISACA).

**Scope and Goals:** Cross Current will meet with you to finalize the scope of the penetration test and to decide such parameters as:

- exploratory or targeted testing
- the period of active testing
- what initial access the tester will have
- whether physical security attacks are allowed
- whether social engineering attacks are allowed

The goals of a penetration test can vary and may include:

- denial of service
- accessing protected information
- determining network administrator alertness and response
- gaining physical access to a device or location
- gaining administrator access
- showing potential for direct financial damage to an organization

If not specifically selected as a goal, we suggest also performing a broad assessment of protections against: social engineering, trashing, physical intrusion, passive surveillance, targeted equipment theft and equipment security, equipment returns/disposals, and additional accesses (wireless, dial-in).

**Deliverables:** Cross Current will deliver an Executive Briefing explaining the risks found and recommendations for solutions, as well as comprehensive reports that will be presented to technical managers and system administrators that will contain:

- details of the systems tested
- the methodologies and resources used in discovery and assessment
- vulnerabilities that were discovered and their implications
- specific solutions to improve information security

