

Securing Your Critical Infrastructure

Network Vulnerability Assessment

- **ASSESS NETWORK AND SYSTEM SECURITY**

Determine whether the networks and systems are resilient to unauthorized access or malicious attacks and afford adequate protection.

- **ASSESS NETWORK SECURITY ARCHITECTURE**

Determine whether the network architecture is adequately configured to mitigate probable attack vectors, as well as afford client's sufficient knowledge and notice to adequately respond to any attack.

- **ASSESS EXISTING PROCESSES AND PROCEDURES**

Analyze whether existing processes/procedures are adequate to prevent a reoccurrence of vulnerabilities.

- **ANALYZE AND DOCUMENT FINDINGS**

Analysis and documentation, including findings and recommendations at both a technical and procedural level.



Service Offering

Details

Relay Security Group, LLC (Relay) was founded in 2007 by information security professionals with over twenty years of cumulative IT security experience in a wide range of markets. Our mission is to provide our clients—through actual validation of vulnerabilities and with minimal impact on their often-sensitive operations—with the most accurate information about security threats to their environments and their readiness to meet current industry standards and regulations. Relay's validation methodology, processes, and recommendations take into account the complexities of these environments, which translate to recommendations that are both reasonable and actionable.

Relay's Network Vulnerability Assessment services are based on proven assessment methodology, which incorporates the Open Source Security Testing Methodology Manual (OSSTMM) v3.0 in combination with Relay's proprietary techniques that, not only takes into account industry specific requirements, but also provides a detailed review of the client's systems and networks. In addition, our methodology also helps identify inter and intra-system trust relationships for critical systems/networks within the infrastructure that can pin point single points-of-failure in an otherwise secure environment.

The testing consists of a broad review of a pre-defined sample set of systems, controlled vulnerability validation, as well as determining how these vulnerabilities indirectly or directly impact the environment. In addition, the assessment may require an additional review of system and network device configurations. The vulnerability assessment can be conducted both externally (from the Internet) and internally (from the corporate environment) and will be undertaken as a cooperative (with specific information) task.

In brief, the network vulnerability assessment will assist a client in determining:

- Deficiencies in their information security and risk posture at both the perimeter and internal environment;
- Deficiencies in the implied and formal documented policies and procedures;
- What the overall operational and business impacts are due to the discovered information security issues;
- What the overall operational and business impacts are due to the discovered information security issues; and
- The most reasonable and expedient path to address these issues at a business, technical, and operational level.

