

A FORSYTHE CASE STUDY

Security Vulnerability Assessment

A Public Power Authority

Business Challenge

As a public power authority, this organization falls within U.S. Department of Homeland Security's definition of "national security and economic critical infrastructures." As part of the national infrastructure, its security and operating policies and procedures are subject to federal regulations and scrutiny. Thus far, however, such regulations have been general, providing neither clearly established objectives nor models for compliance with such objectives. Nonetheless, the IT manager of the public power authority, which provides wholesale electric power to municipal electric systems in its region, felt it was imperative to understand and address its security issues sooner rather than later.

Solution

Forsythe performed an enterprise security assessment to provide the power authority with a picture of their overall risk, including risks they had already mitigated, and risks they would need to mitigate or assign elsewhere. The assessment examined technical vulnerabilities as well as policy and organizational issues.

Technical vulnerabilities were assessed both internally and externally. From the inside, a platform—or host—security assessment examined specific platforms and security configurations, and evaluated them against a set of known vulnerabilities. Internet connectivity was reviewed with respect to firewall and router configuration. External security assessment involved the simulation of attacks—or hacks, as well as "war dialing." War dialing involves systematically dialing all the phone numbers assigned to an organization, determining which have live modems attached, identifying all live modems, and trying to connect to the organization's network through them. In many cases, although an organization has secure firewalls, it may have some "rogue" modems it is unaware of, that can be easily accessed. These present a convenient "weak link" for hackers to exploit. Forsythe also conducted a wireless networking security assessment to identify exploitable vulnerabilities associated with the power authority's wireless access points.

On both organization and policy fronts, Forsythe made recommendations regarding the establishment of an information security program, and provided a roadmap for building such a program. As with many organizations, the roadmap called for increased commitment from senior management, a more responsive and proactive security organization structure, and the adoption of policies and procedures in keeping with best practices such as ISO 17799.

Results

As a result of the assessment, the power authority is planning to expand its IT risk management measures to include disaster recovery as well as security. The authority intends to conduct a business impact analysis (BIA) to understand its overall internal and external risks, so it can make conscious, strategic decisions as to which risks to mitigate, and how, which can be ignored, and which to transfer or outsource.

For more information about Forsythe's offerings, visit www.forsythe.com

