



Identifying the Risks Before They Become Reality

On any given day we may find ourselves reading headlines on the latest attack to a corporate network, a hacker gaining access to sensitive customer data, or a new virus wreaking havoc worldwide. These headlines have become common place, but they remain a disturbing reminder of how vulnerable many organizations continue to be in this era of cyber crime.

Not only does an attack cause immediate and measurable damage to an organization in the form of system downtime, lost or corrupted data, and strain on IT staff, the long-term effects to consumer confidence can be felt for months and can ultimately lead to the downfall of a business.

Furthermore, the requirements of legislation such as Sarbanes-Oxley, HIPPA and Gramm Leach Bliley make it even more important for organizations to understand where they may be vulnerable when it comes to securing their data and systems.

GEOBRIDGE Corporation offers comprehensive assessment services to allow organizations to proactively identify the risks and vulnerabilities that make them susceptible to attack.

The vulnerability assessments GEOBRIDGE has performed have been used by smaller companies looking to safeguard against attacks, as well as large enterprises that need to ensure legislative compliance. Clients are able to choose the services that best meet their requirements to deliver a rapid return on investment while meeting the objectives of the organization.

GEOBRIDGE works closely with the client during each phase of the assessment. At the end of the assessment, a full report detailing the findings and recommendations is delivered to the client. This serves as the foundation for implementing the necessary security policies and solutions to mitigate the risks identified during the assessment and to strengthen the overall security of the organization.

GEOBRIDGE Assessment Services

Information Technology Audit	Determine compliance with security policies, standards and guidelines.
Security & Vulnerability Assessment	Review of physical security, communications and network architecture, and hardware/software configurations to identify threats and recommend controls or protective measures.
Information Security Policy Design & Review	Management's role in security; policies, standards, and procedures; employment policies and practices; contingency planning and disaster recovery.
Asset Identification & Valuation	Identification of all hardware, software, data, storage media, networks, access, and key people to assess each assets worth and identify risks.
Software Development Security Review & Training	Review software life cycle and determine security Risks, recommend secure methods for software development and testing, and train engineers on these methods.
Security Education	Programs to provide security fundamentals, network security vulnerabilities and defenses, and management of computer security.
Information Security Awareness Training	Training on the need for computer security and security administration, tailored to a variety of levels, including Senior Management, Department Security, and Security Function Personnel.
Legal Security Review & Implication Training	Full legal review including forms of protection, trade secret and copyright protection, security techniques to protect proprietary rights, computer abuse and fraud, and legal liabilities.