



### CBI Quick Facts

Established  
1991

Growth (sales)  
+60% ('07 vs. '08)

Experience  
Collective 194 Years  
(Engineers & Consultants)

Footprint\*  
34 states, three countries  
& 198 engagements

**Symantec National Partner**  
**Symantec Consulting Partner**  
**Symantec Platinum Partner**

\* 24 month period

### Assessment Components

- Network Architecture
- Threat Environment
- Penetration Testing
- Social Engineering
- Physical Security
- Physical Asset Analysis
- Operations Security
- Policies & Procedures
- Impact Analysis
- Risk Characterization
- Infrastructure Interdependencies

## Vulnerability Assessments

You cannot afford to assume that your current network security strategy will be effective in the face of a growing number of vulnerabilities that include easy access to wireless networks, mobile devices and applications, and threats including hackers, computer criminals and even terrorists. Let our professionals help you to evaluate the weaknesses in your network to avoid putting your sensitive data and your information infrastructure at risk.

### Direct Benefits

**Build and broaden awareness.** The process of doing an assessment directs senior management attention to security. Awareness is one of the least expensive and most effective methods for improving the overall security posture of an organization.

**Establish a baseline.** If a baseline has been previously established, an assessment is an opportunity for a “check up” to gauge the improvement or deterioration of an organization’s security posture. If no previous baseline has been performed, an assessment is an opportunity to integrate and unify previous efforts, define common metrics, and establish a definitive baseline.

**Identify vulnerabilities and develop responses.** Sometimes, due to budget, time, complexity, and risk considerations, the response selected for many of the vulnerabilities may be non-action, but after completing the assessment process, these decisions will be conscious ones, with a documented decision process and item-by-item rationale available for revisiting issues intervals. can help drive or motivate the development of a risk management process.

**Categorize key assets and drive the risk management process.** An assessment can be a vehicle for reaching corporate-wide consensus on a hierarchy of key assets. This ranking, combined with threat, vulnerability and risk analysis is the heart of any risk management process.

**Develop and build internal skills and expertise.** A well-structured assessment can have elements which serve as a forum for cross-cutting groups to come together and share issues, experiences, and expertise.

**Kick off an ongoing security effort.** An assessment can be utilized as a catalyst to involve people throughout the organization in security issues, build crosscutting teams, establish permanent forums and councils, and harness the momentum generated by the assessment to build an ongoing institutional security effort.

### Methodology

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Our Vulnerability Assessment probes your information infrastructure for areas of weakness across the network perimeter, and throughout the enterprise, encompassing firewalls, FTP, DNS, web, routers and other systems where attacks are most likely to occur.

