SecurEye™

You've insured your business against physical disasters, but what steps have you taken to secure your data and the integrity of your IT assets? Could your business survive an internal or external attack of your computer network?

Identify vulnerabilities in your IT infrastructure.

- » **Find security problems before they impact your computer network.**
- » **Determine whether network security is up-to-date and effective.**
- » **Know if your IT security conforms to legal requirements.**
- » **Identify security policy and procedure shortcomings.**
- » **Get practical guidance on how to protect and defend your IT network, your information, and your customers.**

Today's computer networks are typically the result of years of expanding technical capabilities…new security measures, systems and software merged into existing IT. In the process, vulnerabilities and security lapses develop... Cebic's **Independent Security Assessment** (ISA) helps identifying the security posture of your organization by detecting weaknesses in your computer defenses to prevent IT problems from threatening the survival of your business.

Cebic's highly trained and certified security experts follow the strict standards of the INFOSEC and National Security Agency (NSA) Information Assurance Methodology (IAM),[1] and the NSA Information Evaluation Methodology (IEM) throughout all security assessments. These approaches have been endorsed by the Critical Infrastructure Assurance Office (CIAO) for compliance with PDD-63 (Presidential Decision Directive 63) to provide security assessments for all federal agency classified systems.

Cebic's ISA encompasses enterprise security issues in six critical focus areas: (1) Security policies and procedures, (2) LAN, WAN and SAN networks, (2) Servers, Storage and Workstations(3) External (4) Wireless (5) Telecommunications infrastructure, and (6) Physical security. Client companies can choose to have assessments conducted in one or more focus areas. Some tests can be conducted externally via internet access while others require on-site access, enabling Cebic technicians to evaluate administrative controls and the physical design of the network.

A customized ISA is available for a variety of specialized institutions – tailored to security aspects of the FFIEC, GLBA, SBOX, HIPPA, NIST and ISO examination compliance – as well as a Micro-ISA for smaller businesses. Assessments are also adaptable to the needs of larger organizations including government and federal agencies with unique requirements.

In addition, Cebic provides periodic "check up" assessments – a quarterly or annual review after an assessment, as well as certification reviews to validate post-assessment security fixes. Weekly or monthly baseline vulnerability scans can be used to help identify changes and alert businesses to new problems or vulnerabilities, as they appear.

Don't take a chance that your next assessment will be a forensic review to find out what went wrong. Call 303.987.3679 x 305 or e-mail sales@cebic.com for more information about Cebic Technology's Independent Security Assessments.

24|7

cebic TECHNOLOGIES

Safeguarding Electronic Business Assets

[1] NSA created the INFOSEC Assessment and Rating Program (IATRP) a vehicle for standardization of INFOSEC assessments. The National Institute of Standards and Technology (NIST) has incorporated IAM into special publications on compliance with the Federal Information Security Management Act (FISMA).

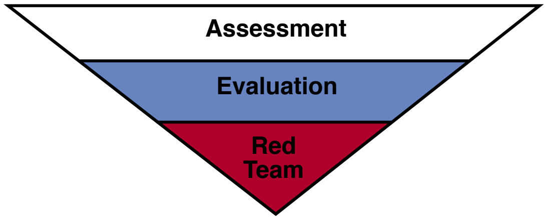
Cebic Security Assessment services are designed to identify and prioritize vulnerabilities and provide technical assistance and remediation support. These services can be deployed individually or combined to provide customized assessments or a complete security solution.

- » Enterprise Security
- » Technical Risk Assessment
- » Security Policy Review
- » Information Security Management Systems (ISMS)
- » SIM (Security Incident Management) implementation
- » Web-deployed Application Security Assessment
- » Attack & Penetration Testing (Red Teaming)
- » Business Continuity Planning
- » Disaster Recovery
- » Firewall Installation, Configuration and Updating
- » IDS Installation, Configuration and Updating
- » Incident Response Planning
- » Network Documentation
- » Anti-Virus
- » Content Filtering
- » Spam Control
- » Router Configuration

Level I - White Team – Assessment
Cooperative high-level overview
Information/mission-criticality analysis (includes policy, procedures, and information flow) No hands-on testing
Not overly technical

Level II – Blue Team - Evaluation
Hands-on process
Cooperative testing
Diagnostic tools
Penetration tools
Technical in nature

Level III – Red Team - Attack and Penetration Testing
Adversarial
External Penetration tests
Simulation of appropriate adversary
Specific Technical expertise



White Teaming:

An assessment that focuses on the non-technical security functions within an organization. In the assessment, the team examines the security policies, procedures, architectures and organizational structures that are in place to support the organization. Although there is no hands-on testing (such as scans), it is a very interactive process with the customer as the team works to gain an understanding of critical information, critical systems and how the organization wants to focus the future of security.

Blue Teaming:

This NSA Level 1+ assessment is a hands-on technical process that looks specifically at the organization from a system/network level to identify security vulnerabilities that can be mitigated through technical, managerial, or operational means. A Level II Blue Team assessment involves cooperative testing and technical analysis of the firewalls, intrusion detection systems, guards, and routers. It may also include some basic vulnerability scans of the customer's network.

Red Teaming:

Often called attack and penetration testing, the red team process imitates an adversary looking for security vulnerabilities to exploit. It is a non-cooperative effort to introduce security failure and constitutes the final step of a comprehensive security assurance program.

Typical scanning tools:

General: Nessus, nmap, GFI, Landguard, SuperScan, (wireless) sniffer, WIKTO
Protocol-dependent: enum, nbtstat, (MBSA), nslookup/dig, N-Stealth, nikto, Whisker, Airsnort, Netstumbler, TCPdump, THC rut, LC5.

Cebic Technologies, Inc. provides affordable, computer security and consulting services for Linux, Windows, Macintosh, and UNIX-based computers networks and is a managed IT Security Service Provider. As an active member of the leading computer security associations worldwide, the Information Systems Security Association (ISSA) and the Information Systems Audit and Control Association (ISACA), Cebic Technologies is on the forefront of computer security issues.

All services backed by IT experts with top security degrees and certifications in computer technology and security, including the NSA-IAM,NSA-IEM, CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), ISSAP (Information Systems Security Architecture Professional), ISSMP (Information Systems Security Management Professional) Microsoft MCSE 2003 Security+, MCSA, MC and MCP+1 designations.

• Securing the Future of Corporate Systems and Knowledge •