

Why Conduct an Independent Security Assessment?

The IT community realizes that security breaches, for whatever reason, can be devastating to an organization. When asked, most CIO's are confident that they are taking proper steps to secure their information. Yet each year, there are many instances of major organizations losing customer data, financial records, employee information, proprietary code, and other intellectual property.

The July 2008 issue of SC Magazine reported the total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005 is in excess of 227 million occurrences. Congress has legislated acts such as HIPAA (Health Insurance Portability and Accountability Act), SOX (Sarbanes-Oxley Act), Gramm-Leach-Bliley Act - with others on the way.

Organizations recognize it's time to address growing security concerns. A key component in security management best practices is the "independent assessment" function.

How can you be confident that your IT assets are secure? How can you be confident that your IT department will continue to deliver the right information, to the right place, at the right time and do it securely? Conducting a periodic **Independent Security Assessment** can provide you with this confidence.

What is an Independent Assessment?

An independent assessment is an evaluation of your security program and/or policy performed by a neutral entity. The scope of the work implies that the independent party performing the evaluation has the certifications, experience and expertise to review any and all aspects of your security posture.

Why "Independent" is Important?

The advantage of an independent assessment is one of complete objectivity – the ability to provide an unbiased agnostic evaluation of your security processes and practices. There are neither preconceived ideas nor hidden agendas when examining governance, compliance and risk.

Due Diligence

Exhibiting due diligence to lower risk demonstrates good business acumen – which can help exonerate your organization of negligence or wrong-doing. It's a good faith exercise that will carry weight in absolving your organization's public image should your organization encounter a security infraction that's publicized.

Governance

Reinforce the directives of your information technology policies and corroborate the security program you've established. Mitigation plans resulting from a third party assessment can affirm your stance within the company culture and help to eradicate any internal political influences that contradict policy.

A Third Party Security Assessment

Human Error

Being intimately involved with the day to day details of security can distort the view of any security engineer. An objective point of view will help overcome the difficulty of your security engineers to “see the forest for the trees”. It is rare for a third party assessment to not discover a vulnerability or weakness that can result in lost public, customer trust.

Security breaches generally occur before security engineers are aware of a problem. There are many instances where external sources (customers) deliver the bad news that a breach has occurred. An independent assessment identifies issues that have escaped the most competent security team.

Inappropriate Activity

Discover activity by employees or vendors that may compromise your security. It’s frequently assumed that employees and vendors are conducting themselves in an appropriate manner when connected to our network. This is not always true. While not necessarily a malicious act, it can be very damaging to your business. A third party assessment has the objectivity to ask the correct questions, to help discover inappropriate activity or situations that may lead to such activity.

Compliance Issues

An independent audit in contrast to an assessment goes a step further in performing a “gap analysis”. It is an evaluation that tests your posture against a particular compliance regulation (PCI, HIPAA, SOX, other), standard (ISO 17799, COBIT, other), or benchmark against an internal security policy. Depending on the type of business you operate, you may be required to have an independent party perform an assessment or audit on a regular basis. Even if this is not the case today, it’s likely a vendor partner will require you to do so as a condition to continue business in the future.

What to Expect?

Honesty, integrity, technical proficiency, and superior analytical skills are essential. These skills imply that the engineers have had years of experience not just in **Information Technology but in the Technology field.**

Also, defining the expectations in any consulting engagement is a key concept. Considerations should include:

- **Physical Security**
- **Information Security & Risk Management**
- **Access Control**
- **Cryptography**
- **Security Architecture & Design**
- **Business Continuity & Disaster Recovery Planning**
- **Telecommunications & Network Security**
- **Application Security**
- **Operations Security**
- **Legal, Regulations, Compliance, and Investigations**