

## The Real Key to a Robust Security Posture!

### Coincidence, or Foul Play?

*A fierce competition has been brewing between you and your closest competitor. The challenge is to launch the best product to the marketplace in the least amount of time. After carefully constructing a plan to ensure no “snoops” or unnecessary information is distributed outside the company walls, you are confident that this product launch will be successful. A few days before the product goes to market, your competitor not only beats you to the marketplace, but they have produced a product that is identical to your company’s product! Have you guarded your enterprise against any form of intrusion? After concluding that there is a definite leak in your system, how do you locate the security breach and protect yourself from future occurrences?*

### Keeping Up With The Jones’

*According to your boss, it’s time to reevaluate the security controls in the company. This project has been placed on the backburner until recently, when your boss realizes the level of risk associated with poor security in lieu of the latest attacks, threats and computer viruses discussed in the media. How is the rest of the industry reacting to the security threats? How do you prepare a security budget? How do you know if you are employing enough security or too much security compared to the rest of the industry?*

### What is a Security Assessment?

The Security Assessment is an independent assessment and evaluation of existing controls and services that includes identifying business critical information in order to make relevant security decisions based on your needs and trends within related industries. This assessment will display your current security status, the desired status based on industry standards and best practices, and the steps to implement in order to achieve your security goals. In addition, we will provide guidance on how to prioritize information security initiatives and budgets. The Secure IT Experts will work with the client to develop a Future Strategies Plan that provides the client with a strategy to prioritize the necessary steps to take the client from its current information security posture to an acceptable and secure environment.

### Levels of a Security Assessment

The Secure IT Experts Security Assessment, at a minimum, consists of a high-level security policy review, data gathering interviews, identifying and rating business risks and technical vulnerabilities, recommending solutions to mitigate the risk, and completion of the Secure IT Check™. The Intermediate/ Mid-Level Assessment tool includes each of those items as well as benchmarking against peer groups and best practices and the development of a Future Strategies Plan. The Full Security Assessment includes all items mentioned in the Mid Level Assessment as well as internal/external vulnerability scans; and firewall, router, and/or system configuration reviews.

Do you have a compliance requirement?

- ✓ Local ?
- ✓ State ?
- ✓ Federal ?
- ✓ Corporate ?

Do you answer to the Board of Directors?

Stock Holders?

Private Investors?

How does your security posture compare to your competitors?

Having an unbiased “Third Party” assessment of your entire technical enterprise and risk mitigation capabilities is imperative to the well being of your enterprise. Or, are you content taking the word of your employees, that “everything is fine”

**“World Class Security Expertise for Everyone”**

© Secure IT Experts – All Rights Reserved

[www.SecureITExperts.com](http://www.SecureITExperts.com) \* [Info@SecureITExperts.com](mailto:Info@SecureITExperts.com)

### What is Secure IT Check™?

Secure IT Check™ is an automated tool that will quantify the results of a Security Assessment in a numeric and color-coded format. The Secure IT Check™ results are determined by answering a set of customized questions that fall under 17 categories including:  
 The results are calculated into an algorithm that weighs the answers based on best practices for information security.

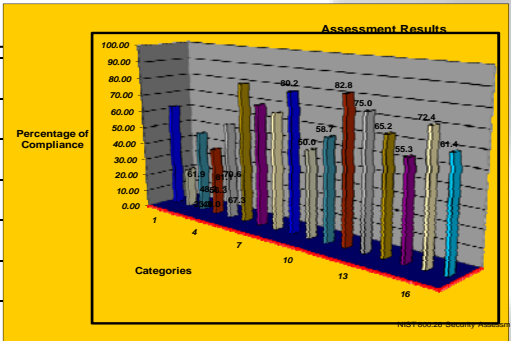
### What Is Benchmarking?

In order to effectively measure your information security posture; the Secure IT Experts will conduct a peer comparison of your information security policies, procedures, organization, and technology architecture with organizations similar in nature and security characteristics. This peer comparison will include both similar industry organizations, as well as organizations similar in size, IT complexity, and location, regardless of the industry. The same criteria is used to measure each organization, therefore comparisons are fair and easier to distinguish among best practices.

### What Are Best Security Practices?

A representative criteria for determining the existence of the fundamental or best security practices are as follows:

Security Criteria	Criteria Reasoning
1. RISK MANAGEMENT	<i>Risk Assessment and Reduction</i>
2. SECURITY CONTROLS	<i>Evaluation and response of Security Controls on a Regular Basis</i>
3. LIFE CYCLE CONTROLS	<i>The integration of security into the IT System Life Cycle</i>
4. AUTHORIZED PROCESSING (C&A)	<i>Assurance for the Security of the System</i>
5. SYSTEM SECURITY PLAN	<i>Overview of the Security Requirements of the System</i>
6. PERSONNEL SECURITY	<i>The Human aspects of Security</i>
7. PHYSICAL AND ENVIRONMENT PROTECTION	<i>The Measures taken to protect systems, buildings and related supporting infrastructure</i>
8. PRODUCTION AND I/O CONTROLS	<i>Help desk issues and media controls</i>
9. CONTINGENCY PLANNING	<i>Backups, Contingencies, Emergency Response &amp; Disaster Recovery</i>
10. HARDWARE AND SYSTEM SOFTWARE	<i>Installation of and updates to hardware and software</i>
11. DATA INTEGRITY	<i>Protection of the Data and programs</i>
12. DOCUMENTATION	<i>Description of Hardware, Software, Policies, Standards, Procedures and approvals</i>
13. SECURITY AWARENESS TRAINING AND EDUCATION	<i>Awareness, Training and Education</i>
14. INCIDENT RESPONSE CAPABILITY	<i>Response to computer security incidents or adverse events</i>
15. IDENTIFICATION AND AUTHORIZATION	<i>Technical Measures that prevent unauthorized access to an IT System</i>
16. LOGICAL ACCESS CONTROL	<i>System Based mechanisms used to designate who or what is allowed to have access to a specific resource</i>
17. AUDIT TRAILS	<i>Maintain a record of system activity by system, application and user</i>



### What Differentiates The Secure IT Experts from our Competitors?

The Secure IT Experts utilizes a sophisticated approach when calculating your company's security posture. This approach encompasses business-specific objectives, requirements and concerns with vendor neutral recommendations. We don't just identify problems – we help define a solution balanced around your business objectives.

**“World Class Security Expertise for Everyone”**

© Secure IT Experts – All Rights Reserved

[www.SecureITExperts.com](http://www.SecureITExperts.com) \* [Info@SecureITExperts.com](mailto:Info@SecureITExperts.com)