

**Expert Reference Series of IT Security White Papers**

---

# **Assess for Security Success**

---

[www.thesolutionfirm.com](http://www.thesolutionfirm.com)

## Assess for Security Success

Michael Gregg

It's no secret that many small and medium-sized businesses can't afford to hire full-time IT security professionals. Instead, SMBs often rely on their technology infrastructure to connect to customers, sell products, control inventory and manage day-to-day operations.

Relying on technology alone can actually make you more vulnerable to malicious acts. A significant security breach at a small or medium-sized company could totally disrupt your operations.

The most crucial security mistake that SMBs make is failing to perform security assessments. This may seem like a basic concept; however, it's often overlooked. An assessment is crucial. Without an assessment, good policies and procedures can't be designed. The assessment is what allows you to work through the process of determining what is important to the organization. Assessments can be performed in one of two ways:

- Quantitative -- This method places dollar values on the organization's critical systems and information.
- Qualitative -- This method uses non-dollar values. Confidentiality, integrity and availability are one set of attributes that can be used.

A typical argument against performing assessments that I hear is, "What's the point? I don't have anything of value to hackers, outsiders or others." This is not true. Every organization has something of value; otherwise, it would cease to exist. Good security usually follows the following five steps:

1. Assessment
2. Policy
3. Implementation
4. Training
5. Audit

Security is truly a multilayered process. Once an assessment is completed, policies will fall quickly in place, as it will be much easier for the organization to determine what's most important. Assessments should include policies on the following:

- Passwords
- Patch management
- Employee hiring and termination practices
- Backup practices and storage requirements
- Antivirus
- System setup and configuration

Finally, you need to convince management and staff that an assessment is really critical and that time and money must be allocated to it. Explain that being proactive can improve the bottom line. Of course, costs need to be considered, so explore all of your options. There are some excellent resources available. Here are a few:

Customers are of little value if a company's infrastructure gets wiped from malicious activity. Customers certainly won't be happy if their credit card data gets stolen or destroyed. Spend the time up front to assess your network. Failure to perform assessments is the No. 1 security mistake that SMBs make.

### About the Author

Michael C. Gregg is the COO of Superior Solutions, Inc., a security assessment and training firm. His current responsibilities include performing security assessments and evaluations for corporate and government entities. He has served as the developer of high-level security classes, study guides, has taught

classes for many Fortune 500 companies and contributed to many books, including the Syngress publication, *Emerging Threat Analysis*.

