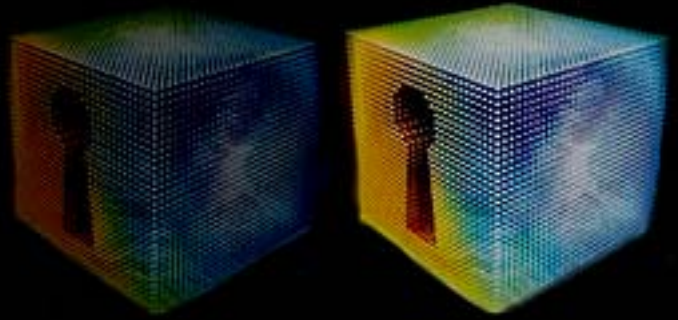




**MARVIN** IT Services

• Security Auditing  
• Penetration Testing  
• Compliance Testing



### ***I.T. Security***

When is the last time your organization conducted a formal security audit or penetration test? If a virus can breach your current defenses, this is clearly an indication that not all is well. As the multitude of cyber threats emerge, security regulations continue to evolve, and the demand for risk management accelerates, companies of all sizes are turning to security specialists to examine how secure their data really is.

### ***I.T. Services***

Marvin IT consultants offer a variety of services aimed at mitigating a company's risk. Risk is the likelihood of a given threat to take advantage of vulnerability, and the result of that adverse event on the organization.

- Penetration Testing:** A Penetration test is a very narrowly focused attempt to look for security holes in a critical resource such as an email server, web server, or firewall.
- Security Audit:** Security Audits are systematic, measurable technical assessments of how an organization's security policy is employed at a specific site.
- Compliance Testing:** Organizations are required by law to comply with a growing number of government and industry-specific regulations designed to safeguard the confidentiality, integrity, and availability of electronic data from information security breaches.

### ***Who needs it?***

Security threats, vulnerabilities, and exposures face every organization today creating risks that must be managed. Therefore, every organization that safe guards information and resources of specified value should assess the security employed to safe guard that information.

### ***How often should it be done?***

Security assessments ideally should be performed on a quarterly basis.

### ***Who should do it?***

Security Assessments must be completed by a reliable, non-interested party.

### ***How are the services performed?***

Marvin IT Services are performed in different segments depending on the depth of the assessment. Some companies may choose to only have one segment completed while others may choose the entire spectrum.

- Site Reconnaissance from the inside
- Hacking from the inside
- Site Reconnaissance from the outside
- Hacking from the outside
- Identify threats and vulnerabilities
- Translate and export findings into relevant reports for regulatory compliance

### ***What will be examined?***

Although the particulars will be established between the two parties, a basic assessment contains the following:

- Up to 3 Server scans (Application server, file server, web server, email server, DNS, etc.)
- 1 Domain
- Up to 2 network devices (router, firewall, switch)

A detailed assessment could include all devices on a network including printers, routers, switches, computers, and modems. Service plans can be set up to scan networks as often as once a week to identify any new threats and vulnerabilities. (Preventative security)

### ***How long does it take?***

Depending on the complexity of the environment and the depth of the assessment, projects can take between 1-7 days.

### ***What do I get?***

- Printout of your companies network topology
- Reports identifying security vulnerabilities, open ports, and vulnerable services
- Reports which ensure compliance with laws, regulations, and corporate security policies

### ***How much do these services cost?***

Cost is dependent on the service, size of the company, number of computers being evaluated, vulnerabilities found on the scanned devices, and numerous other factors. Contact us for more information.

**Marvin and Company, P.C.**

11 British American Blvd, Latham, New York 12110

Phone: 518-785-0134

Web: <http://www.marvinitservices.com>

For more information email [security@marvincpa.com](mailto:security@marvincpa.com)

