



Security Assessment for your IT Environment

Trojans, viruses, and worms... oh my! And if you are lucky, those are the only threats your IT environment will face on any given day. Unfortunately, most days are worse than that. On any day, hackers attack as many IT environments as possible, searching for weak spots in networks. Weak security may mean nothing more than minimal damage, but now that organized crime rings are involved in internet crime, companies without strong security may face financial ruin. Don't be a predator's next meal ticket. Instead, hire security experts to assess your IT environment, point out possible weaknesses, and recommend solutions.

What's at risk?

When your IT environment is insecure, your company is at risk on multiple levels. Besides the obvious virus that replicates advertisements for knock-off designer hand bags every time you launch a program, you risk much more insidious and covert damage that could financially ruin your company. Risks range from deletion of corporate data to exposure of proprietary client data to unapproved monitoring of financial transactions—when it comes to malicious attacks the sky's the limit.

Protect yourself

Limit your company's IT security threats by having your environment audited by security professionals on an annual basis. An annual security assessment will ensure that the necessary defenses are in place to protect your IT environment.

A comprehensive security assessment will usually challenge the following components of your IT environment:

- **External security-** your firewall and other similar devices will be purposefully attacked. A device that fails to block the attack is a security vulnerability that needs to be fixed.
- **IT network-** vulnerability scanning applications will be performed on your networked equipment. Key concerns are un-patched, out-of-date, or misconfigured applications which put your IT environment at risk.
- **Domain security settings-** your business domain will be attacked to locate weak configurations which might put your business at risk.
- **Wireless security-** your wireless access points will be “sniffed.” If access points are discovered, they will be attacked to test the network’s strength.

During a security assessment, other parts of your IT network will be examined:

- **Logs-** hardware and application logs need to be set up to detect security threats and notify system administrators whenever possible threats are detected.
- **Email servers-** improperly configured mail servers can be captured, used as spam servers, and ultimately, your business emails could be blacklisted.
- **Security policy-** a written security policy will ensure that your IT environment is not compromised through unapproved application installation or unapproved network activity and must be enforceable through security permissions applications.
- **Defense in Depth-** this final step in the security assessment will determine how many layers of security are available with your current network, and if needed, will also generate recommendations for additional security.



Next steps

IT security experts encourage that a security assessment be performed on an annual basis. In the case of major network restructuring, another assessment might be a smart choice. To learn more about security assessments and protect your company from becoming some predator's next meal ticket, please contact the security experts at [All Covered](#) or call 866-446-1133.