

# I.T. Audit Can Save Your Business from Hackers, Careless Employees

**F**or many business owners, the economic downturn has brought a devilish new challenge in the form of increasing cybercrime. Sophisticated hackers have begun targeting vulnerable businesses, with the Internet Crime Complaint Center reporting that hacking crimes were up 33% in 2010.

With many small businesses lacking anti-virus software, even more deploying unencrypted wireless networks, and most having no security plan, too many organizations lack essential protection for their network and sensitive data.

From early viruses of the late 1990's to recent denial-of-service attacks which freeze networks by overloading them with outside data, cybercrime is exploding. And with many organizations having scarce resources and insufficient time to monitor cybersecurity, they are particularly vulnerable to web-based crime.

Yet it's *not only* cybercrime that organizations have to worry about.

Too many employees are negligent in protecting equipment and confidential information. With cybercriminals aggressively seeking victims to target, care is required to be well-protected from a data breach that can cripple your business.

Employee email is indispensable to business. But *unprotected* email can pose significant risk to your most sensitive intellectual property, financial information and customer data. The results can be catastrophic: monetary loss, company disruption and legal action.

Sixty-six percent of employees in a recent survey said they no longer worry about losing their laptop or portable device because data is encrypted, believing encryption fully prevents theft of information. Not so! Encryption is key, but other measures are called for.

And careless employees often disregard other security practices. In the above survey, one third said they frequently leave their laptops with strangers while traveling, or leave computers in insecure locations. Two thirds never use a privacy shield, and half admitted to turning off encryption capabilities or recording passwords on paper. *Whew!*

To protect your organization, consider retaining a reputable IT partner firm to conduct an IT Security Audit – a rigorous, comprehensive review of security which provides specific, actionable insight to mitigate risk.

Such an audit identifies critical information, security issues, and helps you develop a layered protection plan to strategically defend against both internal and external threats. And with threats – viruses, worms, Trojan horses, spam, spyware, theft and corporate espionage -- all around you, don't "hope for the best" ... especially when your organization is likely accountable for data security through regulation and contractual obligation.

## An effective IT audit should include:

- External vulnerability testing
- Internal vulnerability assessment
- Network review
- Wireless assessment

Once completed, you should receive a written summary of findings, full details of all reviews and assessments, schematics and scan reports detailing your network and vulnerabilities that need to be addressed, and specific recommendations for improvements and remediation.

## A Final Word

Too often in our industry, IT audits are conducted either by an in-house IT manager or an existing IT provider. Each has a vested interest in *not detailing shortcomings* – how would that make them look? – or may lack the necessary skills, tools and methodology to implement an effective audit. Consider an outside partner with appropriate credentials like the CISSP (Certified Information System Security Professional) or CEH (Certified Ethical Hacker). Chances are, you'll be glad that you did.



Since 1999, CEO Charles Johnson and EDTS have been providing networking, security and managed services support solutions to Southeastern businesses. The firm provides Experience, Dedication, Technology and Solutions (EDTS) to increase productivity and reduce cost associated with IT.

In the Upstate, call 864.250.9112 or visit us at [www.EDTSolutions.com](http://www.EDTSolutions.com)