

Article – IT Security for Small Business

February 24, 2006
Concerto Networks of San Diego
Written by: Eric Rockwell

IT Security for Small Business

Taking a closer look at 'big' security issues in Information Technology (IT) for small business today

When pondering the major security challenges and opportunities for security and small business, the first obvious one that springs to mind is what would pose a risk to your business.

The response would in all likelihood be password and policy related. It is accepted practice for smaller shops that everyone knows everyone else's business, and yes...passwords! Some believe in changing it every month. There is more at stake here than merely sharing a password – it is about inherent shared trust, business integrity and mitigating risk. Password complexity needs attention and user-id and logon, and access passwords, should remain confidential and not shared. Staying away from the 'ABC', '123' "generic" and free for all-type passwords are recommended. They are normally too simplistic, everyone knows each other's passwords and this is a totally unacceptable situation, that represents the most common breach of security. It might be as simple as someone seeing you use your password and/or knowing how to use it, that could pose the same problem.

Viruses and proper software patch management are other critical security issues (i.e. for operating systems, networks, e-mail, spam, and anti virus applications). Where there is technology, there are technical intricacies and complexities, access and security risks. With managed technology services and anti-virus strategy, you counter the ability of others, to gain access and/or do damage to your system, network and therefore your business.

So what can small business do to address these issues?

With comprehensive Information Technology (IT) services, this is included in 24/7, round-the-clock monitoring and notification, resulting in immediate corrective action. A "set-it-and-forget it" attitude and plan will not work, as the threat is constant and real. Keeping it updated and running, not 90% of the time, BUT all the time is what will afford you true protection and lower your risk and vulnerability to infection or even new virus or other malicious attacks. Effective active management is the answer, timing and updates are everything. With some of the newer Trojans and worms, you sometimes do not even know that they are there, until it is too late. **Proactive protection will safeguard your interests here too.**

A big no-no, is writing passwords down somewhere. We all have this relaxed mentality about this dangerous practice. We just trust everyone that works for and with us and do not make it a priority to keep our information and networks secure. As a test, if anyone phones and says they are from the IT helpdesk and want your password, most small business owners would just give it to them, sharing it without a moment's hesitation. Other occurrences of this might be new employees, maybe it has never been a priority or consideration for you before. Having a "we are all friends here" mentality is too trusting and naïve, never suspecting that anyone would be set on infiltration or stealing passwords or information. Where these practices are pervasive it is easy to gain access to your system, being slightly more prudent with it, tracking and not sharing passwords should be a small business priority, in their own vested interest to protect all your assets. Your IT partner should be able to offer you password management solutions for your business as part of a comprehensive support plan.

Another area of real risk, is dealing with the sale and/or purchase of older or used computers, technology and/or hard drives. Without proper archiving, reformatting, erased hard disks, all types of data are left on these, which might expose you and your business to significant risk. Taking a pro-active approach to protect your company information is deemed both prudent and necessary.

Article – IT Security for Small Business

Be sure to take care with unsecured wireless access (Wi-Fi) and hotspots. The public domain is no playground, there are dangers lurking. The biggest security risk is our own mobile, digital enabled and driven world. Secure and protect yourself when using that airport or coffee shop (hotspot) is critical. Most of us have not even figured out how to enable the protection, but we are using it to conduct our business, inviting everyone in through a wide-open and unlocked access-door! Beware of uninvited, unwelcome guests, drop-ins and visitors, who should not be prowling around – do not give them the keys to your information and network by not enabling protection on your mobile devices or with relaxed password protocols. Your IT partner should be able to assist your business by training employees on how to keep their information secure when using public and unsecured wireless access points.

Regular back-ups of your information are crucial too. For more information on how to prevent possible loss and protect your businesses critical data, see our article, “**Back-ups: A Quick Case Study**”.

For more information on Concerto Networks and our solutions for your business, visit www.concertonetworks.com today.