

Keeping Your Business Safe

SMB Quick Reference Series

Reducing Technology Associated Risks

It is an unfortunate reality that technology, while bringing unprecedented productivity and communication, brings new threats and security challenges to business. Smart businesses proactively understand such risks and have instituted plans, policies, and procedures that virtually eliminate the risks associated with cyber crime, thereby allowing them to focus on the business and its success.

The good news is that there are a number of practical actions that any business can adopt that close security and threat challenges. Some may seem obvious while others may not. Either way, if you aren't doing these you may be compromising your business, your employees, and your future success.

- **Virus Scanners:** Make sure that you utilize virus protection/scanning software on ALL devices that your business uses. Take advantage of the 'auto update' feature to ensure you have the latest virus definitions. Don't let your virus software licenses lapse, keep them current for the best protection.
- **Spyware/Adware Scanners:** Protection against spyware and adware is critical in today's connected environment. Install and regularly update spyware/adware scanning software on all devices and establish regular scanning intervals. Keep the profiles and licenses up to date.
- **Back Up Important Data/Information:** It can't be stressed enough that backing up business information is critical to the survival of your business. Install the necessary devices, software, and automated policies to back up business information regularly and often.
- **Business Continuity/Disaster Recovery:** Create, test, and institute a business continuity and disaster recovery plan – no matter how small your business may be. Store backed-up information off-site, have a few 'back up' computer/cash register devices ready to go should your primary office location be affected by a disaster. Make sure that you can handle unwanted fire, theft, floods, or hurricanes/tornados without going out of business.
- **Encrypt Sensitive Information:** Encryption is one of the most secure methods for maintaining confidentiality of information/data. This is especially true when you keep personal customer information such as social security or credit card information that could easily be used for identity theft.
- **Portable Device Security:** When your business uses laptops or PDAs, the issue of security is most acute as these portable devices are often lost or stolen. These devices should be backed up on a near-daily basis, have full encryption installed and utilized, and enforced policies for physical protection.
- **Network Security:** Networks are proving to be one of the greatest security threats to business. Hastily installed and rarely managed, these provide excellent entry points into the business systems for hackers and cyber criminals. Make sure that all routers, gateways, access devices, and user devices are properly configured for maximum network security.
- **Employee Access to Information:** Data theft by employees is a growing concern. Restrict access to sensitive information, including confidential documents, customer information, business contacts/customers, sales leads, and proprietary product/service information to only those employees that need to access such data. Implement strong data protection policies and procedures that minimize potential breach and theft.
- **Website Security:** Websites are common to almost every business. Websites are also used to gather and store confidential customer and financial information. Keep all sensitive data stored on secure systems and not web servers. Implement SSL (secured socket layer) security between your website and your users. Use certificates for authentication to ensure highest levels of security.
- **Device/Information Disposal:** There always comes a time to upgrade to new hardware and software. Always discard old devices after erasing all data from them. Where this isn't possible, remove the storage drives and physically destroy them to minimize the ability to capture sensitive data. Create and institute policies for the elimination of security risks when disposing of old, unwanted devices and information.

Your business can easily and quickly eliminate all of these risks with one call. The SMB IT Manager, from NextCorp, is a fully turnkey IT management service that ensures that your technology is always managed, secured and optimized for the greatest productivity and business protection – keeping your business safe.

Discover how you can overcome these challenges with the SMB IT Manager by simply visiting www.smbsuite.com or by calling 1-800-525-NEXT. Best in class and cost effective technology management is one call or click away! Go ahead. You have nothing to lose and everything to gain!

1-888-525-6398

©2008 NextCorp, LTD.

www.smbsuite.com

