

Network Security Best Practices
On-Site Computer Solutions
Brian McMurtry
Version 1.2 – Revised June 23, 2008

In a business world where data privacy, integrity, and security are paramount, the small and medium business owner has a responsibility to ensure that their data is well-protected. With years of successful SMB consulting under their belt, On-Site Computer Solutions is prepared to develop a personalized plan for your business.

A lack of planning can result in a security breach that destroys data or divulges sensitive data. In addition, without a disaster recovery plan, a single hardware failure can result in the loss of years of business data.

On-Site views security as a multi-layered, multi-walled plan, rather than a single gate with a single point of entry or failure. By building multiple walls around a network, prying eyes are discouraged. Even if one of the security checkpoints is compromised, other barriers will prevent the compromise of data.

On-Site Computer Solutions values these technologies as part of an overall security plan:

1. Physical Security - Physical security of the facility must be considered first, such as implementation of key management, access control to secure areas, and alarm systems. Changing alarm and door codes regularly is the beginning of an effective security plan.
2. File Encryption
 - a. Portable Computers - Stolen or lost laptops are a great security risk for a company if secure data is stored on them. On-Site recommends whole-disk encryption to prevent the viewing of sensitive files in case of a loss.
 - b. Desktops/Servers - The use of whole-disk or folder-based encryption can be utilized through Windows or third-party tools to add a layer of security to data.
 - c. Email – PGP signing can be used to encrypt e-mails with sensitive data that will be passed over the Internet.
3. Storage of Sensitive Data
 - a. Servers
 - i. Centralized Storage - Because On-Site recommends that all crucial data be saved on a central storage solution, servers are



- recommended. A Windows-based server provides centralized security through Active Directory to help close the door to intruders.
- ii. Physical Security - The server must be stored in a physically secure, locked location.
 - b. Workstations - Important data must never be stored locally on a machine in an unsecured area. Workstations are typically not stored in secure areas, so documents should be re-directed to a server or network-attached storage device. If data is kept local to a machine, measures should be taken to prevent theft of the tower, such as a security lock.
4. Backup Strategy - Regular backups are vital to the security of business data. These practices are strongly encouraged:
- a. Regular Backups - Backups should be performed daily, utilizing multiple media to prevent single storage failure. On-Site Computer Solutions recommends Symantec Backup Exec for server backups. Media must be changed daily.
 - b. Locked Backup Media - When considering a backup device, a keyed/locked media storage unit is preferable to discourage theft.
 - c. Daily Verification - Verification of backups through e-mail or physical visit to the server should be performed daily.
 - d. Test Restore - Full-system restoration should be performed on a quarterly basis in a test environment.
 - e. Encryption - Backup media must be encrypted so that media is secured if stolen.
 - f. Media Storage - Backup media not in use must be stored in a secure, disaster-proof, off-site location.
 - g. Workstations - A disk cloning product such as Norton Ghost should be used periodically to enable quick restoration of the operating system in case of failure.
5. Data interchange with 3rd parties
- a. Business E-mail should be encrypted with a third-party tool.
 - b. Insecure data transmission protocols such as ftp or telnet should be eliminated in favor of an encrypted protocol, such as ssh, scp, or sftp.
6. Managed Virus/Spyware protection – A single virus can destroy or compromise company data. Therefore, it is critical to install a centrally-managed antivirus/antispyware solution. On-Site is a provider of Symantec Antivirus for the corporate server and workstation desktop.
7. Email Filtering



- a. Virus Filtering - Mail servers should have a mail filtering antivirus solution to prevent infection of workstations by mass-mailed viruses. On-Site recommends Symantec Antivirus Enterprise Edition to protect mail servers.
 - b. Spam Filtering - Because many junk mail senders include links to virus-infected or otherwise compromised websites, On-Site recommends Symantec Premium Antispam to filter out junk e-mail.
 - c. Mail Relay - E-mail servers should be secured, disallowing the use of unauthenticated e-mail relaying.
 - d. Email Archiving – For some businesses, a full archive of all inbound and outbound email is required for compliance purposes. A full email archiving solution can be a lifesaver to track down information for compliance, or litigation.
8. Firewall Security
- a. Open Port Auditing - a check should be made for open ports on a firewall. Unneeded open ports should be closed. When possible, ports should be locked down to restrict external hosts to specific IP Addresses, especially for ssh or remote desktop ports.
 - b. Restrict Outbound Mail – Outbound mail access should be restricted to mail servers only. A mass-mailer virus on a workstation could result in the mail server becoming blacklisted, meaning days of undeliverable outbound e-mails.
 - c. Remote Firewall Access - Remote administration of the router should either be disabled or locked down to a specific IP address.
 - d. Granular Filtering - With a more advanced firewall device, firewall rules can be set to disallow certain outgoing protocols, such as peer-to-peer file sharing or instant messaging.
9. Workstation/Server System Hardening
- a. Secure shares- All file shares should be checked with a share enumerator to verify that security is locked down for all network shares. Unneeded shares should be disabled.
 - b. Account management – On the local workstations, the Administrator account should have a complex password set. All other local accounts should be disabled or deleted. The Guest account should be disabled.
 - c. Software Firewall - Enable Windows Firewall on workstations. Only allow needed exceptions.
 - d. Secure File System - All hard drives should be converted to the NTFS file system.



- e. Remove Insecure Legacy Computers - Windows 95/98/ME machines should be phased out due to their inability to communicate over secure protocols or secure local files.
 - f. Disable Unnecessary Services - Unneeded services that are running, such as IIS, FTP, SMTP, or SQL server, should be uninstalled or disabled.
10. Least-needed security privilege / Sanctity of administrative privileges
- a. User Permissions - Users should run their local workstations as Users or Power Users rather than administrators. This prevents unauthorized changes to workstations or data. This also limits installation of rogue programs and devices.
 - b. Administrator Password - The password for administrator accounts should be held in the highest sanctity. Only authorized users should have access to this account.
11. Group Policies – Workstations should be locked down using group policies. Practically every setting can be governed by Windows Server group policy. Most common settings are:
- a. Removal of use of CD-RW, USB devices
 - b. Prevention of software installation (such as remote-control or file sharing software)
 - c. Screensaver Lockout Policy – after X minutes’ inactivity, the PC goes to a password protected screensaver.
 - d. Scheduled logon lockout hours. A policy to lock out unauthorized logons apart from normal business hours should be implemented.
 - e. Prevention of running unauthorized applications, such as instant messengers or Windows Media player.
12. Wireless Security
- a. Wireless Encryption - All Wireless access points must be secured with a minimum of 128-bit encryption by WEP or WPA. On-Site prefers WPA over WEP because of its superior encryption capabilities.
 - b. Wireless Group Policy - A wireless security GPO should be implemented to prevent internal wireless clients from accessing rogue, unsecured, or external wireless access points.
13. Internal Communication Restriction - IPSEC should be implemented as mandatory via server policy.
14. Audit Logs - Auditing should be a part of an ongoing policy to detect intrusion attempts.
- a. Firewall – If deemed necessary, a firewall with ability to log access attempts should be installed.



- b. Server – Auditing the changes of system security should be monitored with a third-party tool.
- 15. Centralized Patch Management – Windows System Update Services (WSUS) should be implemented on the local Windows Server to enforce a centralized solution for patch deployment. Machines that are missing security updates are vulnerable to compromise. If no Windows server is in place, the workstations should at least have Automatic Updates configured to download and install updates on a daily basis.
- 16. Ongoing Network Auditing - On a quarterly basis, servers and workstations should be audited for security using the Microsoft Baseline Security Analyzer and other tools to ensure that security standards are being kept.
- 17. Biometric Devices – Fingerprint devices help to authenticate a user’s identity before allowing logon to systems.
- 18. Password Policies and Retention – should be implemented and customized according to the client’s needs.
 - a. Minimum password length of 7 characters.
 - b. Password complexity (usually involves letters, numbers, and symbols, case-sensitive). Users should think in terms of passphrases, rather than passwords. This complexity will assist to keep unauthorized users from cracking an easy password by brute force.
 - c. Password expiration – after 42 days, accounts require a new password to log on.
 - d. Password history – enforces that users cannot revert to an older password until 24 passwords have been used.
 - e. Account lockout – After 3 failed logon attempts within a 24 hour period, accounts should be set to lock out. Only an Administrator should be allowed to re-enable the account. This is the strongest deterrent against brute force hack attempts.
 - f. Users should never divulge their password to other users, or write it down on paper within their personal workspace.
- 19. Standard Policies and Procedures
 - a. Procedures - When internal procedures are standardized and documented, there is a process in place for most expected and unexpected events, ranging from the setup of a new workstation to termination procedures for an employee. Standardized procedures help employees avoid making costly mistakes.
 - b. Disaster Planning - In addition, a plan for a “natural disaster” should be in place, should the physical workplace be destroyed. Disaster planning is an integral part to securing your business.



- c. **Acceptable Use Policies** - Last, a clear acceptable use policy should be created, so that users know which activities are allowed or disallowed on the company's information systems. All employees should read and understand the acceptable use policy. Clear communication in this area will substantially reduce employee abuse of the computers and network.