

FINANCIAL RECORD SECURITY

Posted on April 9, 2012

You might think that your small organization is not a target for malicious hackers. But, a survey by the Small Business Technology Institute reported that more than half of all small businesses in the U.S. experienced a security breach in the past year. Here are the steps you should take to provide basic security for your financial records.

1. **Protect Your Systems**—Equip all PCs and servers with a) an un-interruptible power supply to prevent corruption of data, b) virus detection software, adware/spyware detection and removal tools, and c) a firewall on all computers that connect to the Internet.
2. **Create Backups**—Make regular backup copies of all your important data. Store a copy away from your office.
3. **Use Effective Passwords**—Encourage non-obvious passwords and change them every three months. Use password protection for folders and files containing accounting information.
4. **Keep Software Up To Date**—Without updates, your anti-virus, anti-spyware and firewall software will not protect you against new cyber threats.
5. **Lock Your Records**—Lock file cabinets and access to computers that contain financial information. Block all unauthorized access to the QuickBooks data file.
6. **Be Prepared For Emergencies**—Create a contingency plan for your organization so you can recover if you experience an emergency. Test your plan annually.
7. **Use A Payroll Service**—Use a payroll service and keep employee names and detailed payroll information separate from the accounting system.
8. **Audit Trail**—Make sure that your accounting software's audit trail is turned on, allowing unauthorized changes in data to be investigated.
9. **Computer Checks**—Generate bill payment checks directly from the accounting system to reduce the risk of check alteration and duplicate bill payment.
10. **Educate Your Staff About Security**—Develop a “culture of security” in your employees and in your business. You might think that your small organization is not a target for malicious hackers.