Protecting from Technological Fraud and Intrusion

SMB Quick Reference Series

Steps to Keep Your Small Business in Business

Every business is at risk for fraud: From dishonest employees to unscrupulous customers to faceless hackers. Learning how to safeguard your company is essential.

But for small-business owners, preventing fraud can be especially tricky because of limited time and money. Often, a small business owner will skip steps that could have prevented the theft of trade secrets or credit card information or merchandise. Take no shortcuts. Identify risks ahead of time, and take action to protect your company.

- Authentication: Authentication provides identification by means of a previously agreed upon method, such as passwords and/or biometrics. Passwords must be strong and changed regularly to ensure the greatest security. Biometrics should be used where there is need for a secondary authentication. Create and enforce strong policies and mechanisms to ensure proper authentication to facilities, devices, and information.

- Firewalls: As an important component of network security, firewalls are effective in reducing the risk of a successful attack. The effectiveness of a firewall however, is dependent on its design and implementation. Eliminate misconfigurations, operating flaws and the means of attack that may render firewalls ineffective.

- Intrusion Identification: Real-time identification of an attack is critical to minimizing risk. Generally, this software scans for patterns or "signatures" that represent known intrusion techniques or unusual system activities. All businesses should consider the use of real-time intrusion detection software.

- Software Integrity: Copies of software and integrity checkers are used to identify unauthorized changes to installed software. Integrity checkers identify whether a file has been changed. Businesses should ensure the security of the integrity checklist and checking software. Where larger risk exists, the checklist and software should be stored away from the network, in a location where access is limited.

- Security Policies: Having a policy is the best policy. Many businesses don't. Set strict policies for the creation of passwords for your employees, customers, access to servers and routers, and ensure that everyone follows them diligently.

- Virus/Malware Protection: As an easy to implement and manage first line of defense, companies must protect against viruses and other malicious software by using automated virus scanning software and frequently updating the definition/signature file.

- Dishonest Employees: A 2006 study by the Association of Certified Fraud Examiners found that businesses with less than 100 employees were more prone to internal theft than larger companies; with an average cost of $190,000 per incident. Weak internal controls are often to blame. Implement internal policies and conduct codes when money and sensitive information is involved.

- Installation/Update of Systems: When new systems are installed it is time to review security procedures and adjust to accommodate new capabilities. Also, regularly keep your systems and software up to date (applying needed 'patches') to ensure that you minimize the risk of a security breach or data theft.

- Physical Technology Security: Take the appropriate steps to place critical information systems and information into rooms or facilities that cannot be accessed by employees and customers. Get your systems out of the broom closet and put all sensitive devices and information behind locks that require a key, password, or biometric authentication.

- Eliminate Intrusion Access Points: Restrict the use of USB flash storage devices, employee-owned devices, and non-tested/approved software within your business. All these tools are too easy to 'hide' and can store vast amounts of confidential information that can 'walk' out of your business; or, upload malicious code or information that can compromise sensitive systems and data.

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.getsmb.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!