

Expert Reference Series of IT Security White Papers

Security Basics Check List

www.thesolutionfirm.com

Check List: Security Basics

Michael Gregg

It's a given that IT security is a critical component in today's business world. However, it's still hard for small and medium-sized businesses to apply the manpower and money needed to accomplish the job effectively. Here's a list of the Top 10 items you should check before you even start your security project. Note: These aren't in any particular order, as all 10 are important.

1. **Choose your platforms wisely.** Many small businesses suffered through the recent economic downturn, though business is improving. There couldn't be a better time to retire any remaining Windows 9x devices you're allowing on the network. These computers have absolute no security. Windows 2000 or XP would be a great replacement.
2. **Retire old network equipment.** Perhaps you are one of the few organizations that is still using hubs. If so, you should seriously think about replacing them. Not only are they robbing valuable bandwidth, they are also a security risk because they allow anyone on the network to easily eavesdrop on sensitive traffic.
3. **Patch your Web server.** Sure, you have some dedicated IP addresses and a computer that's capable of hosting your Web site, but should you really do it? This all depends on the amount of time and effort you can devote to this activity. It is important to remember that your Web site is the one thing that attackers can easily find and access. So make sure you update your Web server software regularly. Be sure you are always running the latest versions of software to stay ahead of attackers; otherwise they could potentially use your Web server as a beachhead into your network.
4. **Forget about peer-to-peer.** Maybe the small satellite office you maintain seems to work fine with a peer-to-peer network. Even so, get rid of it! Peer-to-peer networks should not be in any size of business. They lack security and have no centralized control. It is a security disaster waiting to happen.
5. **Change default passwords.** I am sure some of you are saying, "Everyone changes their passwords!" Well, it's not true. I cannot count the number of security assessments I have performed where unauthorized access was but one password away because the passwords had never been changed. Here is a [default password list](#). If you happen to see your password on this list, please take a few minutes to change it.
6. **Enforce a strong password policy.** Everyone likes easy passwords, but it is critical to enforce a strong password policy. Microsoft makes a free tool called [Passprop](#), which makes configuring strong password policies a breeze.
7. **Educate your employees.** So you can't afford this year's newest security gizmo? No problem. Many network security breaches are human-based. Spend time educating your employees on the importance of IT security. This process should start the day an employee is hired and continue throughout his/her employment. Contests, newsletters, tips and policy reminders are all easy ways to get the message out that security is everyone's job.
8. **Think total security.** I wish I could tell you that security is something that can be done and then forgotten about, but this is not the case. Security is a process, not a product. Practice really does make one perfect, or at least close to perfect!
9. **It is not just the outsiders.** While you may have installed a firewall or other border device to keep the bad guys out, just remember that firewalls only secure the perimeter. The best approach is "defense in depth." One idea is to install host-based firewalls on internal devices. Read more about firewalls [here](#).
10. **Beware of the cleaning crew.** It is unfortunate but true, that once everyone has gone home, the lingering employees and other after-hours crews are sometimes overlooked as being security threats. These people usually have full access to the facility and are aware that not many people are around. [Here is a good facility access control list.](#)

About the Author

Michael C. Gregg is the COO of Superior Solutions, Inc., a security assessment and training firm. His current responsibilities include performing security assessments and evaluations for corporate and government entities. He has served as the developer of high-level security classes, study guides, has taught classes for many Fortune 500 companies and contributed to many books, including the Que publication, *Certified Ethical Hacker*.

