

# What, When and Where: A Brief Security Guide for Your Business

By Zachary W. Price [zachp@essentialsecurity.com](mailto:zachp@essentialsecurity.com)

With the inherent stresses that come with running a business, there is often little time to digest the complex intricacies of security software. According to recent studies, many business owners eschew the notion that their digital assets may be vulnerable to attack.

Although an attack or infection can be potentially catastrophic, many believe damage caused by viruses, hackers and worms only happens to others. They consider their data to be of little use or value outside of their organization. Even executives that acknowledge the existence of these hazards seldom have the time or the budget for security audits and/or an overhaul of their workflow procedures to comply with best security practices.

If you don't have the time or resources right now for a security audit, then read on. Below are some of the basic tools that can help your business take a proactive approach to data security. By implementing the following, your business and personal data will be less susceptible to financial damage caused by accidents and malicious attacks.

## Regularly Update Your Software

Although valiant efforts are often made to write safe software, the fact is that no software is ever bug-free. Hackers exploit these bugs for a variety of reasons, including fun and money. It is critically important that your software is updated on a regular basis. Most operating systems, firewall and antivirus can and should be configured to receive regular updates.

MS Windows updates visit: [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)

Mac OS updates visit: <http://www.apple.com/support/>

## Install Firewalls

Firewalls separate one network from another and are frequently used to separate a company's internal network from the Internet. Firewalls not only mask the identity of the individual computers behind them, they also examine and filter potentially damaging data entering or leaving the network. It is good practice to install both perimeter and client-side firewalls.

Some firewall providers include:

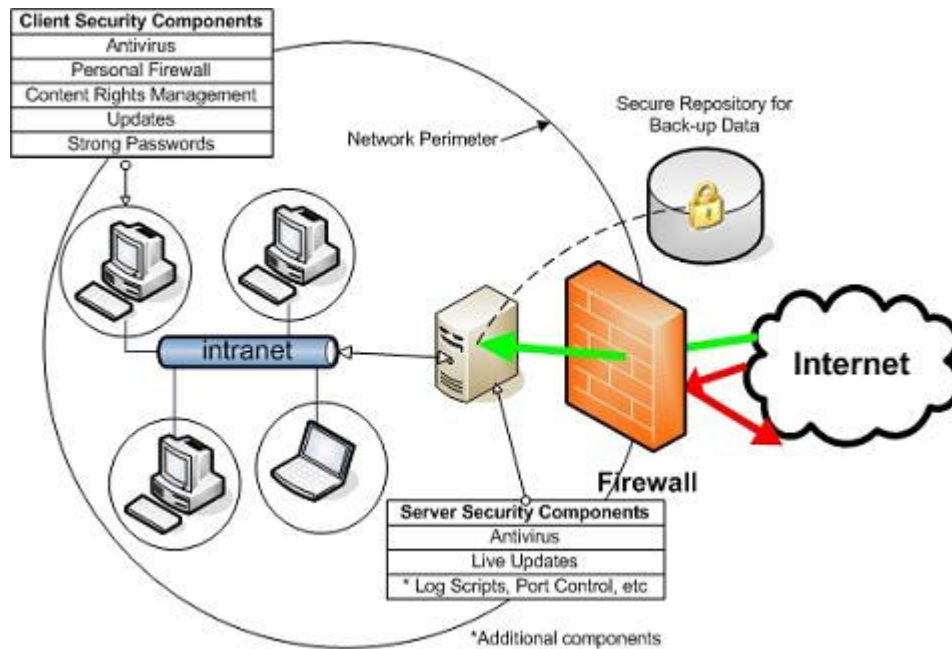
- Watchguard: [www.watchguard.com](http://www.watchguard.com)
- Cisco: [www.cisco.com](http://www.cisco.com)
- ZoneLabs: [www.zonelabs.com](http://www.zonelabs.com)

## Install Anti-Virus Protection

Hundreds if not thousands new malware programs are released each month. These include viruses, worms, Trojan horses and host of other programs. Symptoms of infection range from the annoying to the catastrophic. Because viruses can slip through firewalls posing as a legitimate email or program, installation of client-side anti-virus software is important. Install only the latest version of your chosen antivirus program and make sure to regularly update the virus definition files and scan your system.

Well established anti-virus providers include:

- Norton: [www.symantec.com/product/index\\_smallbiz.html](http://www.symantec.com/product/index_smallbiz.html)
- AVG: [www.grisoft.com/](http://www.grisoft.com/)
- Panda Software: [www.pandasoftware.com](http://www.pandasoftware.com)
- McAfee: [us.mcafee.com/virusInfo/default.asp](http://us.mcafee.com/virusInfo/default.asp)



### Protect the content of your sensitive files and email.

Most email isn't intended to be a public announcement, yet private messages often turn out to be just that. Email and files containing sensitive business information such as strategic plans, contracts, financial information, designs and more all too often spread beyond the individuals they were intended for. According to a recent report by the Computer Security Institute, loss of proprietary data was the third leading cause of financial damage to organizations last year.

To mitigate this problem consider using rights management software to protect your sensitive business data. Content rights management software not only encrypts files, but also serves to enforce access and limit usage privileges such as forwarding, editing and printing. These protections are persistent and remain with your files no matter where they travel. Any business that frequently exchanges medical, financial, legal or design data should make regular use of encryption and content rights management technologies

Some established providers include:

- Authentica: [www.authentica.com](http://www.authentica.com)
- Essential Security Software: [www.essentialsecurity.com](http://www.essentialsecurity.com)
- Microsoft IRM: Microsoft IRM:  
[www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.msp](http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.msp)

### Establish a periodic data backup strategy

Periodic backups are required to ensure business continuity in case of an accident such as a hard-drive failure or attack. In a networked environment, full and incremental data back-ups can be programmed to take place at regular intervals. Small offices environments should backup their sensitive data to an external hard-drive or CD at least once a week. It is good policy for companies to back-up email as well. Back-up data should be stored off-site in a secure location. Be sure to test your backup processes to ensure that indeed your data can be restored lieu of an operational failure.

Secure off-site data storage providers:

- Iron Mountain: [www.ironmountain.com](http://www.ironmountain.com)
- First Backup: [www.firstbackup.com](http://www.firstbackup.com)
- KastenChase: [www.kastenchase.com](http://www.kastenchase.com)

### **Use strong passwords**

Passwords are used to authenticate the identity of an individual user. Unless otherwise protected, once a password is broken your sensitive data is exposed. With free software that is readily available on the web, most passwords can be broken in a number of minutes. These programs often use known words and phrases to break passwords frequently beginning with “password” and “admin”. For good password security use a combination of upper-case and lower-case letters, numbers and symbols (i.e. eR8>!tJd ). Make sure that your employees memorize their passwords and that these are not written down anywhere on premises.

### **Hire a security consultant**

While tips in this article will help your company to be more secure; every business is different and requires its own security strategy. Consider hiring an independent security consultant to asses your individual security situation. They will be able to help you create a comprehensive security policy that will meet your business needs.

### **Educate your employees**

No security plan is effective unless followed by your employees. Measures can be taken to severely limit their privileges such as browsing the internet, reading email, or preventing the reading of files from USB drive or CD. However, draconian security measures can interrupt workflow and damage productivity. A better policy is to limit some user privileges while educating your employees about your company’s security policies.