

Internet Security Best Practices

1. **Conduct a risk assessment and include more than just your internet site.** Analyze your internet site, access to the site, and internal systems that communicate with your site to identify potential intrusion, corruption, and destruction risks. Assign a criticality level to each. High priority components would include systems that, if attacked, would have a major disruption to your business; medium, a moderate effect, and low, a minor effect.
2. **Create an information security policy.** Security policies will outline your employees' roles and responsibilities for each system they access. It also defines which systems are off limits. Extending this policy to contractors and suppliers will inform them of the security protocols they must follow.
3. **Identify ways and create a plan to secure each system.** Starting with the high priority systems, determine the systems, applications and processes needed to make them secure, being careful not to lock them down and, thereby, impacting desired business usage.
4. **Create and manage a vulnerability program.** Security needs to be considered across all areas of your organization, not just eCommerce. Internal systems, networks and processes, offsite backups, laptop and VPN access, internet and intranets -- all can be sources of security breaches. Ensure they are current.
5. **Develop a security team with adequate resources and processes.** As you consider systems to secure data, you will need to also consider the resources, responsibilities, and processes to use and manage the security systems. Who will manage the systems? Who will monitor and address intrusions?
6. **Create a security response plan.** Develop a plan to respond to security violations; a plan to shut down, fix, and restore services; and a post mortem process to identify ways to prevent security breaches. . Ensure your legal team has signed off on this response plan, as 45 out of 50 states now have "Data Breach Laws" and associated penalties
7. **Design your security plan to work with your business processes.** Security is critical to the survival of some businesses. However, so is actually running the business! Make sure that each security measure is planned out to consider the impact to business processes.
8. **Make sure your network is secure.** Locking down all access points and only opening up the ones needed is a good starting point in network security. Microsoft SQL, FTP, and SSH servers are popular targets for password guessing attacks because of the access that is gained if a valid username/password pair is identified. SQL Injection, Cross-site Scripting and PHP File Include attacks continue to be the three most popular techniques used for compromising web sites.
9. **Determine the right level of website content security for you.** Many times, retailers feel that they must encrypt product data going to their eCommerce site. Why? All of this data is available on the web anyway. Make sure you really think about the pros and cons of securing website data and have a solid rationale or business case for each.
10. **Hire an outside internet security firm to routinely test your systems.** There are many firms that help 'certify' your website as secure. These services typically test your network, insure SSL usage, and provide a visible 'seal of approval' to give your customers higher online purchase confidence. =