Best Practices for Security Management

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[[PC and lock](http://itmanagersinbox.com/wp-content/uploads/2008/04/pc-and-lock.jpg)](http://itmanagersinbox.com/wp-content/uploads/2008/04/pc-and-lock.jpg)  Protecting your Enterprise IT system from threats both external and internal becomes harder each day. There will always be new methods of intrusion and infection that threaten your system. Your Security Management group should develop a set of best practices to ensure that your IT infrastructure is secure and can continue to support your business.

**Best Practices to Consider**

* Monitor your vendors for security information and patch releases. Always keep your patches up to date.
* If a malicious code or other threat makes its way into your network, disable or block access to the affected services until you can apply a patch.
* Enforce a strict company-wide password policy and require passwords to be changed at least every 90 days.
* Configure your email servers to block or remove email that contains attachments that are commonly used to spread viruses. Examples are .EXE, .SCR, .VBS, .PIF and .BAT files.
* Use controlled testing of the capabilities of your security system to expose potential vulnerabilities.
* Monitor software installed on computers in the company to ensure that only authorized software is installed.
* Have an emergency response plan in place and test it on a regular basis. You should have a backup-and-restore solution in place so if data is compromised or you have a catastrophic loss you will be able to recover any lost data.
* Evaluate your off-site disaster recovery plan to ensure your organization can continue IT operations should an event or catastrophes occur. Include regular DR testing to ensure that your systems properly fail-over.
* Education of your employees and management on good security practices should be an ongoing program. Email, the Internet and unauthorized installation of software should be highlighted. Consider removing Internet access from employees that do not require it to do their job.

These are just a few best practices to consider as part of your IT departments overall security plan. In order to ensure your Enterprise wide system is protected your Security Management team should continuously review their systems. Management must also give them the budget they need to secure your network and your data.