ITS SECURITY PRIORITY ACTION STEPS

1. Address concerns about Outside-In traffic (spam, AV, updates/patches, getting rid of or securing default accounts). Limit your exposure; secure the number of access points. Installing and updating AV is critical.

2. Wireless Access – if you have wireless access point(s) and it/they is/are not secured, anyone within a radius of 300' can pick up your signal and be on your internal network. An employee who buys a wireless router and connects it to your LAN has in fact saddled your organization with a wireless access point and exposed your entire network to outside view.

3. Secure access to servers, both physically and logically.

4. Concerns relating to the establishment and maintenance of permissions (shares, folders, reducing administrative access).

5. Establishing and executing data back-ups (data backup, secured data backup, offsite security).

6. User training re: security (not leaving passwords out, don't bring in devices from home, don't open strange emails).

7. Concerns about Inside-Out traffic (web content filtering, spyware/malware removal. Includes email and email content filtering. HIPPA compliance, etc.)

8. Generating operations policies and procedures manual for distribution to employees. Must include process and data flow.

9. Group Policy Objects (GPOs) – for enforcing the ITS business policies of your organization (firewall turned on at the machine level or not, etc.).

10. Shared data or data to be accessed departmentally should not be saved on user PCs.