Top 5 security issues for small/starter companies.

The pressures of setting up a new business are hard enough today without the perceived added hassles of Information Security.

There are a lot of confusing messages being delivered in the media on a constant basis with regard to the increasing security risks associated with using the Internet, and IT in general. What is very important to note at the outset is that while there are risks and pitfalls, with a little effort at the beginning, we can minimise many of these.

This article is focused on providing the list of the top 5 steps that a small, or start-up, company can take to ensure that it's IT resources and data are protected. The rest of the steps listed are important to follow as well, but the first 5 are the most critical.

1. Install Anti-Virus software, from a reputable brand such as McAfee, Symantec, Sophos and Kaspersky Labs. There are many providers of Anti-Virus software in the marketplace, but these are acknowledged as the marker leaders. It is not sufficient to install Anti-Virus software, and then ignore it. The success or failure of Anti-Virus software protecting your computers is based on keeping it up to date.
2. Apply the latest patches to your PC. Many of the viruses and worms that exist on the Internet and are being written as you read this article are using bugs or vulnerabilities in the software you are using. The manufacturers of this software, such as Microsoft, are producing patches, or fixes, for these vulnerabilities almost as soon as they appear. However, if you do not apply these patches to your PC, you will be affected by these vulnerabilities.
3. When connected to the Internet, always make sure that you are protected by a firewall. A firewall is a device/piece of software that will prevent network connections that have not been permitted. They typically are based on a set of rules that define incoming and outgoing network traffic. There are different types available, ranging from the software based ones that are installed on the PCs connected to the Internet to the hardware or stand-alone machine based firewalls. Various factors such as the size of the organisation and number of people accessing the Internet will determine the most appropriate firewall.
4. Do not open email attachments. If you receive an email, even from someone that you know, that contains an attachment that you are not expecting, do not open it. Verify with the sender that they intentionally sent you the attachment, and what it is. With many of the viruses in the wild, they will forge the From address in the email and insert a random email address that the virus has found on the infected PC. That means that an infected PC can send a virus to a user and forge the From address, and that From address will possibly be known by the person receiving the virus.
5. Steps 1-3 should be repeated every time you connect to the Internet. This should become as routine a task as putting on your seat-belt every time you get into your car.
6. Patching of software on servers is as important as that on PCs.
7. If you must deploy wireless LAN technologies, make sure that the installer understands the security implications of wireless LAN technologies and implements the appropriate controls. If this is not done, anyone with a wireless LAN device within a couple of hundred feet of your office could actually be part of your network. They would then be able to access

information, use resources such as Internet connections, access illegal inappropriate content, distribute copyright protected content etc.

8. Passwords. Make sure that the systems installed all require unique UserIDs and Passwords to access IT resources, and that these are locked out on failed login attempts. Users should be made aware of the responsibility associated with access to IT resources.
9. Disable UserIDs once staff members have moved or departed.
10. Remote Access. If remote access is necessary for users, ensure that only the appropriate people have access, and it is removed when no longer necessary. It the Internet is being used for remote access, it is critically important to ensure that strong authentication and encryption are used.
11. Do not allow external devices such as laptops of consultants or suppliers to connect to your LAN. If they must, then you should check their machine in advance for the presence of an up to date, and functioning, anti-virus product.
12. Email phishing. Never supply any confidential information to anyone via email. This is true even if the request looks like it is coming from a legitimate institution that you are familiar with. Reputable banks and other institutions will never request this information via email. If in doubt, contact the organisation via phone and request more information.
13. Make sure that you are performing regular backups of your data, on servers/desktops/laptops/PDAs etc. Periodically, take some of the backup media out of the office in case the office, with all the backups, is destroyed
14. Investigate the outsourcing of the management of SPAM and viruses in email to a specialist organisation such as TopSec Technologies (Irish) or Messagelabs (International). This will mean that you are not paying for the downloading/management of email that was unsolicited and may be damaging to your company.
15. Have an Acceptable Usage Policy in place for all employees that require access to IT resources such as the Internet. Many samples are available on the Internet and through bodies such as IBEC etc.
16. Awareness among staff of these points is probably the most important part of the process.