SECURING YOUR NETWORK – MAJOR THREATS AND HOW TO AVOID THEM

Risk Assessment

You take your life in your hands every time you cross the street. For most people though, this a negligible risk when compared, for example, to bungee jumping! The risks your *network* faces are also highly dependent on context. Factors such as the size of your network, the nature of your work, the type of network you have, and the number of people using your systems will dictate your security policy. Try to use the following guide to assess the level of risk your organisation is exposed to (and remember, even low risk environments need to protect their systems!).

Low Risk Environments

Low risk environments include networks that are unlikely to be deliberately targeted because of the organisations' low public profile. They include very small workplaces where it is easy to *monitor* computer use and/or where there is a small and trusted staff who work closely together and are central to the organisation hence less likely to want to destabilise it. Internal network security is not so important because they don't need to secure or hide files from each other.

Medium Risk Environments

Medium risk environments are typically larger organisations where it is difficult for management or network administrators to know what people are doing with their PCs. The organisation may make PC's available to volunteers or trainees as well as staff that are not central to the organisation. If the organisation runs a peer-to-peer network, they may be doing so without fully understanding the risks as they expect and need some files to be private. Although there may be a server in place the organisation may not be sure it is being secured correctly.

High Risk Environments

In high risk environments, the organisation is regularly or – by virtue of the work it does – continually exposed to predictable risks and threats. Irrespective of their size, these organisations may work with financially or politically sensitive data or have users that have a tendency to be antagonistic. They are organisations that allow tenants, students, drop-in users, trainees and other organisations to use or share networking equipment, PCs or Servers that belong to them.

Risk Area 1: Password Security

Many people think of passwords as just another hoop to jump through - something you have to remember to do but has no real intrinsic value. Yet in many cases, passwords may be the ONLY defence against the hacker and deserve to be taken seriously no matter how low the risk is. If you operate a peer-to-peer network, a single

password to gain access to a PC may unlock all of the shared documents on your network as well as your personal files. Make sure it is not widely known and certainly not displayed anywhere near the computer. In a server environment, network administrators centrally control passwords including enforcing minimum length, complexity and frequency of changing passwords. For more information see the Knowledgebase article on Choosing and using secure passwords

Risk Area 2: Exploited Users

One of the best ways to bypass security is to trick the user into providing information direct to the hacker. In order to mitigate this type of risk, network administrators need to be certain that all of their users are aware of phenomena such as phishing and do not give information out by responding to hoax emails or telephone calls. Similarly, incorporating confidentiality into company handbooks and Human Resources/Employment Policies is a must.

The inexperienced user can also create havoc on a network by visiting high risk websites such as those concerned with shopping, MP3's, smileys, gambling, dating, chat rooms, pornography, free *software*, peer-to-peer file sharing etc. At first this may seem trivial but can expose the network to far more serious risks. The 'cure' for these risks, is to have regularly updated anti-virus software installed and scanning on all machines as well as specialist anti-spyware / pop-up blocking tools where needed. On the preventative side, you will need to ensure that all updates for the operating systems and *web browser* software are downloaded and installed.
If you operate public access PCs, you should consider options for governing the websites that users can access. Web content can be controlled on a network either through an advanced *firewall* or through a proxy server. Both systems regulate all requests for web pages and allow administrators to decide whether access to a particular website or type of website is permissible or not. This will usually involve some form of subscription-based service that actively monitors and categorises web pages.

Risk Area 3: Viruses

Unlike spyware, popups and trojans, viruses target users indiscriminately. Low risk environments are particularly prone to viruses as those using computer systems often don't need to think about security with the same levity users in as higher risk environments. Nevertheless, regularly updated and valid virus protection should be considered essential for every PC (especially Windows PCs). Installation is however different from installing on a single PC and you should seek professional help where needed. More information on this in the Knowledgebase article *Dealing with viruses*.
If you are looking after a network, look for specialised virus protection than can be centrally managed and monitored. In this way, you can ensure that updates and scans are not being cancelled and can keep track of threats – and even remove them - without disrupting users. 'Network' versions of Anti-Virus software such as AVG Network Edition or Symantec Corporate Edition cost around £8-£15 per PC.

Risk Area 4: Internet Based Hacking

Automated – and therefore random - 'probing' of computers connected to the internet is a fact of modern life. Even those running a low risk environment will need a basic router with some firewall capabilities to ensure that

these probes do not yield results. Such routers cost from £40 to £150 and may even come as part of your *broadband* package.
Clearly, the higher the risk, the more sophisticated the firewall needs to be. Whilst a £150 *router* will usually suffice for a medium risk environment, if you run a high risk environment you may need to consider one with more advanced features that can fend off sustained and deliberate attacks. Before you buy, be sure you understand what these firewalls do – they are unlikely to prevent viruses or spyware for example! Oh, and don't forget to change the default password on the router too – the manual will tell you how.
For more on internet security risks see the knowledgebase article How secure is the internet.

Risk Area 5: Hacking from Within

It is much easier to hack into a network when you are physically joined to it.*Wireless* networks then are perhaps the greatest risk since the hacker can easily be concealed. Equally though, do not neglect the physical security of your systems – there are countless examples where networks are compromised by cleaners, night porters and service engineers who just plug in to a spare network point or turn on one of the PCs.
In order to be secure, networked devices MUST use have a strong password and WIFI must use the *WPA* (Wireless Protected Access) security system. In buildings where multiple organisations share the same network cabling, they should be separated by means of VLANs to prevent users from one organisation directly accessing the network resources of another. VLAN capabilities are supported in network switching gear costing as little as £150.

Risk Area 6: Misuse of PC's

The last category of risk applies to the higher risk environments where unknown or un trusted users have access to PCs. Although it may not be immediately obvious, the mere fact of logging into a PC may grant them sufficient privileges to stop it from functioning properly. Malicious users could uninstall printers, change system settings, delete crucial files or install software that puts equipment and data at risk.

Preventing this kind of risk is all about 'locking down' the PCs such that those users are barred from these types of activity. No matter what *operating system*or environment you use, there are many forms of restricted account that can be applied to a given computer. If this is an area you are concerned about, seek support from a network specialist supplier.

Conclusion: Network Security Checklist

Network security is a serious business. If you are a network administrator you do need to ensure that you have considered all of the risks. The following checklist highlights the major areas you need to pay attention to.

1. **Users**: do they know about the causes of spyware, popups and Trojans? Do they understand basic principles of security such as suspicious emails and password security?
2. **Secure passwords**: Not just for all PC's or users, but also on routers and WIFI points too.
3. **Policies**: Do we have policies on acceptable use of IT systems, confidentiality and use of passwords?

4. **Anti-virus/spyware etc**: Do we have regularly updated (centrally managed) anti-virus, anti-trojan and anti-spyware software. Are scans run regularly?
5. **Updates**: Do we update our PC's and servers with the latest security patches?
6. **Misuse of Systems**: Do we know and understand how our files and PC's are protected from malicious use? Are networks sharing the same network cabling seperated by means of a VLAN?
7. **Monitoring & Control**: Given the risks we face, do we need to do more to regulate access to the *internet*, shared files, or shared PC's?

Source : http://www.ictknowledgebase.org.uk/securingnetwork