FREE Guide – How Can Proper Network Security Save Your Company Money?

When running a small or medium sized business one of the foremost thoughts in our minds is budget. I know, I run a small business and am very familiar with the need to balance expenses with actual revenue. It can be a serious challenge to find the right balance between the two.

Often as we at Nexus IT perform network audits for prospective clients one of the areas of most concern we find is network security. We generally find that small and medium size businesses neglect to sufficiently prioritize their network security because of a misconception that doing so would be expensive. However, we find that properly implemented and maintained security practices are generally a cost savings for any company. The issues brought about by poor network security can be far more costly than doing things right.

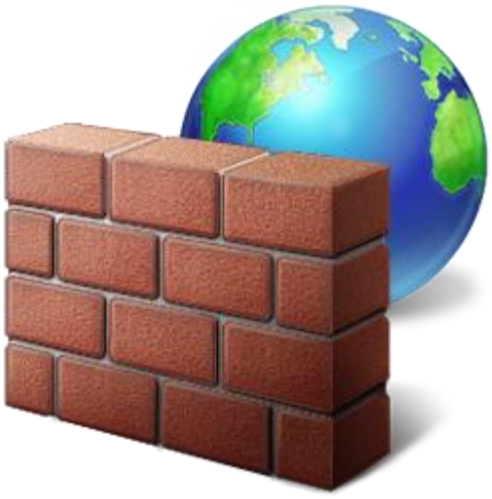
In our line of work, not a week goes by that we are not either combating against or dealing with the ramifications of poor security decisions on our client's or prospective client's behalf. There are 7 area of major concern listed below that we frequently find on new networks we are auditing and will cover in this guide.

1. Hackers
2. Acceptable Use of Technology Policies (AUP)
3. Insufficient or complete lack of AntiVirus and AntiMalware
4. Lack of installation of important software security updates/patches
5. Lack of implementation of network security policies
    1. Employee abuse or misuse of Internet and email resources
6. Wireless Security

Hackers:

There was a time when hackers primarily targeted larger organizations, government entities etc.… However it is very common for hackers now to target small and medium size businesses; knowing that their security practices are generally subpar and it is usually easy to gain access to their networks. For many of our clients we monitor the traffic on their network daily and for most of them not a month (or sometimes even a week) goes by that our monitoring tools don't pick up a hacker trying to access their network. Fortunately due to those tools and the fact that we are immediately alerted to the attack we are able to take appropriate measures to block the hacker.

So why would a hacker want to access your network? The answer is generally simple; to profit from their exploits. Hackers will gain access to your network for many different reasons (outlined below).



1. Initially they will scour your network for financial data and passwords that belong to you and your clients. With that data they can begin to use credit cards to place orders on the Internet, gain access to financial accounts and steal your or your employee's and client's identities. This is the main reason that PCI compliance regulations have come into being; to ensure the proper handling and storage of your client's credit card information. Note: If you run credit cards and are not familiar with PCI compliancy you need to be.
2. Hackers often setup shop on your computers they have hacked. They setup servers hosted on your computers where they exploit others by:
    a. Sending spam and phishing attempts to gather more financial data.
    b. Scan other networks for possible vulnerabilities.
    c. Run attacks on other networks they have found as vulnerable. Hackers generally will attempt to leave no trace of their tracks by leaving a complicated trail of their point of attack. They could be in Indonesia (just for the sake of a place to name) but be hacking a network in your town from your network. And they would likely hack your network from another network in another remote corner of the world.
    d. Setup fake services such as a rogue AntiVirus or illegal prescription delivery where they charge people for services but deliver nothing. Then they also use the credit card information obtained in the transaction to continue their personal Internet purchases.
    e. Setup pornography websites where they charge subscribers for access.
3. Hackers will usually gain access to your email and social networking accounts so they can send messages to your contacts pushing their various exploits above.
4. Hackers also install programs called key loggers on your systems. This allows them to gain access to bank accounts, email, social media accounts etc.… by recording the credentials you enter for these sites.
5. Once they gain access to your systems hackers will often riddle your systems with viruses and malware just to be destructive. Particularly if they have decided they have exploited your network to maximum potential and are pulling out of it.

So how do you protect yourself from a hacker? Here are a few suggestions to help but certainly not all the measures that should be taken.

1. The number one tool is to install an adequate hardware firewall for your network.
2. Install software firewalls for your mobile workforce and laptops.
3. Use VPN connections for any remote access to your network resources wherever possible.
4. Don't open ports on your network unless absolutely necessary. Use non-standard port numbers if possible.
5. Use complex passwords for your network devices, servers, workstations, user accounts etc.… Using simple passwords make it very easy for a hacker to quickly gain access.

Being the victim of a hack can be very expensive; generally costing thousands of dollars and countless hours to reverse the damage caused. Sometimes the damage is irreversible and systems or a network have to be completely rebuilt to repair extensive damages. Under most circumstances it is more expensive to deal with the ramifications of a hacking incident than it is to implement and monitor proper protection to avoid it.

Acceptable Use of Technology Policies (AUP):

IN TODAYS WEB CENTRIC WORLD IMPLEMENTING AN AUP FOR YOUR ORGANIZATION IS ABSOLUTELY NECESSARY.

An Acceptable Use Policy (AUP) is a written agreement all parties on a computer network promise to adhere to for the common good. An AUP defines the intended uses of the network including unacceptable uses and the consequences for non-compliance. You will most commonly see an AUP when registering on community Web sites or when working on a corporate network. We find that most small and medium sized businesses pay little to no attention to what the users on their network do with the technology at their fingertips. The reality is that they need to as so many network security issues arise from the misuse or abuse of this technology.

Why Acceptable Use Policies Are Important? A good Acceptable Use Policy will cover provisions for network etiquette, mention limits on the use of network resources, and clearly indicate of the level of privacy a member on the network should expect. The best AUPs incorporate "what if" scenarios that illustrate the usefulness of the policy in real-world terms.

The importance of AUPs is fairly well known to organizations like schools or libraries that offer Internet as well as internal (intranet) access. These policies are geared towards protecting the safety of young people against inappropriate language, pornography, and other questionable influences. Within corporations, the scope expands to include other factors such as guarding business interests and protecting the network from security threats.

Nexus IT has created a **FREE** resource to enable your organization to simply modify and implement a well-written AUP immediately to protect your technology assets and infrastructure. Simply go to the link below to request your template.
http://www.nexusitc.net/acceptable-use-of-technology-template/

AntiVirus and AntiMalware:

We are often surprised when we perform computer network audits that most companies either have no AntiVirus/AntiMalware protection or what they have is old and out of date.

Viruses and Malware are so ever present in today's world. Even with up to date, effective AntiVirus and AntiMalware there is no 100% guarantee that you won't get infected with a virus if you are not careful with Internet and email usage. However, without AntiVirus or out of date AntiVirus/AntiMalware protection you are much more vulnerable to being infected.

Most infections have become so damaging that they cost hundreds of dollars and many hours to fix. It is common that the effects of an infection are so extensive that it is necessary to format a computer or server and rebuild it from scratch.

Network aware infections are becoming more and more common. Once these have installed themselves on a computer on your network they spread to your entire network; infecting all computers and servers. Some will erase or hide all of the critical shared data on your network. With these types of infections a 3 to 4 hour disinfection on a single computer turns into 3 to 4 hours for every computer on your network; often costing into the thousands of dollars.

It is absolutely imperative to run an effective up to date AntiVirus/AntiMalware. As it is not feasible for most small and medium size businesses to manually ensure that all of their systems are adequately protected Nexus IT offers a scanning/updating/monitoring service that allows us to certify your protection is always up to date, your systems are always scanned for infections and we are alerted if any issues are found. Often if your systems are infected and the infection is detected early and dealt with quickly we are able to safeguard that the infection doesn't worsen on the infected machine and doesn't spread within your network. This type of scanning, updating and monitoring is essential to ensure your network security.

Security Patches:

While it is unfortunate, most software is released to the public with bugs and security loopholes. This includes operating systems, office suites, line of business software, CRMs, browsers, and plug-ins (i.e. Reader, Flash, Java, etc…). While the bugs are annoying the security loopholes are the primary

concern. Hackers and malware authors utilize these loopholes to exploit your systems, infect them and gain access to your personal data and your systems. Microsoft releases operating system and Office updates weekly due to these types of issues.

It is imperative for businesses to keep these applications up to date to remain safe from security threats. Because this is so necessary and because staying on top of this for most businesses is a daunting task; as part of our Basic Managed IT Services package Nexus IT patches all of your computers and servers on a weekly basis for you. We do the legwork, making sure that newly released security patches and bug fixes are applied across your entire network.

Network Security Policies:

All too often security risks, viruses, and malware enter a network due to unapproved activity from employees.

Activities such as chatting, social networking, unapproved Internet browsing, installation of personal software, illegal downloading, file sharing, etc… are very often the cause of issues and infections on networks.

For a company to protect itself in today's digital age it is necessary to implement policies and rules in regards to the use of its technology. A network administrator can implement security policies across a network that prevents employees from performing unapproved activities and accessing unapproved data on the network. Not only does this help keep employees on task and more productive but it also prevents many of the most common security risks.

A properly built network with properly implemented security policies can save your company time and money.

Content and spam filtering will also help to curtail internal and external sources of security threats and assist with employee productivity.

Another common practice we see in businesses is for employees to share their passwords to computers, software and other network resources. Proper security protocol is for each employee to utilize and not divulge their own complex passwords. Adhering to this type of practice will minimize an organizations exposure to security threats and ensure employees only access approved network data and resources.

Failure to implement and monitor these types of policies and solutions is likely to lead to costly repairs on your network caused by security threats, virus and malware. As the old adage states “an ounce of prevention is worth a pound of cure”.

Wireless Security:

When auditing new small and medium business networks we often find concerning lack of proper security as it relates to wireless networking. We often find that businesses have either implemented wireless networks with no password or outdated password encryption. It is also common practice for business to give out their wireless password to guests. All of these practices are serious security threats.

Allowing guests to use your wireless network or not using any encryption invites others to browse around your network, often giving them access to sensitive financial and personnel data. Your neighbors or guests may thank you for the free Internet access but their Internet activities can severely cripple your Internet speeds and expose you to security threats. As mentioned above there are many network aware viruses. Unauthorized parties accessing your wireless network can inadvertently spread viruses and malware across your network.

A properly implemented wireless network uses up to date encryption technologies. If it is necessary for you to provide wireless Internet access to your guests this network should also be properly encrypted and should be implemented as a completely separate network separated from your network through a firewall or proper network segmentation practices. When possible it is advisable to provide a separate Internet connection for your guest access that utilizes separate network hardware that is in no way connected to your network.

Conclusion:

Unfortunately there is no 100% sure-fire, bulletproof equation that will keep you safe from all possible security threats. However, fortunately, implementing the above network security practices and protocols will go a long way to guarantee security for your company, prevent lost time and money due to security threats and in the end save your organization money.

Of course there are costs to properly implement and monitor adequate network hardware, protocols and policies. However, failure to do so in most cases will be more costly in the end and could create serious security issues and often consequences for your organization.

Generally for most small and medium sized businesses without the proper knowledge and experience it is intimidating to properly implement and monitor appropriate network security.

For this reason at Nexus IT we make it our responsibility to safeguard your network. We offer cost effective security solutions and services that fit small and medium size business budgets.

We are so confident in our abilities and your satisfaction that we are willing to let prospective clients put us to the test at no charge to you!

FREE Network Security and Performance Audit:

We would like to offer you a **FREE Network Security and Performance Audit ($999 value).** During this health check we will perform a comprehensive audit of your entire network to look for potential problems, security loopholes, spyware, and other hidden problems that will cause the computers on your network to run slow, act funny, crash, and lose data.

We will:

- Review your system backups to make sure they are working properly and CAN be restored quickly in the event of a disaster.
- Scan for hidden spyware, malware, and viruses that MOST anti-virus tools and software can't detect or won't remove
- Check for security updates and patches to validate that your network really IS secure.
- Review your firewall and wireless security settings.
- Check the integrity of your server and workstations hardware (Side Note: Did you know that hardware failure is one of the leading causes of data loss that CAN be detected early and avoided with proper monitoring?).
- Audit your virus definitions and protection.
- Conduct a visual inspection of your server room and cabling to make sure your network is PHYSICALLY safe and set up properly.
- Check your overall system performance, space and settings to see if your network is running as fast as it could be.
- Test your Internet speed to ensure it is adequate for your needs and meets the speed you are paying for.
- Check for outdated unreliable and slow equipment that is hindering your network performance of causing issues.
- Ensure you phone system and other IT systems are meeting your needs and operating properly.
- Generate a report detailing our findings and recommendations for long-term health, reliability and security of your network.

To participate in this free offer simply call us at 435 487 9099, email us at info@nexusitc.net or provide us your contact information at the following link on our website http://www.nexusitc.net/itaudit/