

Introduction

As my business expands, I need a standard set of criteria for helping customers and myself see the best approach for managing their networks. To this end I have created a list of questions that I use to establish future goals, identify current weaknesses and make sure a core set of tasks are being carried out every day. I have developed this list of questions over time and I add to it here and there as I encounter new things. Recently I have thought it may benefit others if I share this list of questions as well as potential answers. As you read through this document, the purpose is to get you thinking about strengths and weaknesses of your network and to expose you to various solutions for solving problems you may discover as you go.

Prerequisites

The only prerequisite for this document is that you have a network of some size well any size really and you have the desire to improve, shape and mold it over time.

Network Q & A

- How many locations do we want to connect with an inter-office VPN? [Either now or down the road]

It's important to ask this question because we need to know how many end-points there are in our VPN. This will determine how many licenses we need to buy in order to create our VPN infrastructure. Implementation could be done using hardware firewalls using encrypted tunnels or you may use a product such as Himachi by 3AM Labs.

- How many servers will I be responsible for?

If you are providing network support, you need to understand immediately the number of servers you will be responsible for and the products which will be running on them. To be clear, when I say server I do not mean a Windows XP machine running Mail Enable Standard or IIS. I mean a piece of hardware that most likely has a hardware disc array of SATA, SCSI or SAS drives, one or more network cards and thanks to virtualization one or more server grade operating systems which may include Linux and/or Windows Server configurations. This is important information as these pieces of equipment can cost thousands of dollars, need special software licenses and may mandate battery backup UPS devices to guarantee uptime to the internal/external base of customers. You want to identify server appliances immediately and establish management plans early on.

- Are you running Microsoft Small Business Server?

If you are running Microsoft Small Business Server this is both good and bad. You need to be aware that several versions of this product exist and that various requirements may exist depending upon which version you have. Be aware that CALs (Client Access Licenses) are required in every case but may not be compatible across some Small Business platforms. Know up front your licensing needs and make sure you have addressed this early on. 50 CALs for a Windows 2003 Small Business

Server can cost you in excess of \$3000 - \$4000 so make sure your licensing needs are understood up front. Additionally the various products within this family may include SQL Server 2000 or 2005, Microsoft Exchange Back Office, 5.5, etc. Find out immediately if you are dealing with SBS 2000/2003/2003 R2 and be aware of the premium editions for each product family. Any oversight here can be very expensive.

- Do you host your own email and website on your own server? [Do you want to?]

You need to understand if the client hosts their own mail and Web server. In many cases a company may choose to host its email but want to host its website on a server farm somewhere else. Depending on the situation you have you will need to make some decisions about security and server isolation. Additionally backing up Exchange introduces some unique challenges. There are products which will image your entire server and there are products which will only backup your email. There are merits for each product. Be sure you understand which is best for your particular situation. Costs will almost certainly be a factor.

- What is your data backup strategy? Does it provision for a fire burning down your location?

Many customers do not understand the ramifications of a catastrophic data loss. With the wide spread use of Quickbooks, a total destruction of data may in fact mean total destruction of a company. Many companies have abandoned paper processes and dual entry accounting systems altogether. Critical customer, financial and enterprise data is stored on a disc somewhere. In the event of a catastrophe companies should have a recovery plan. Companies that don't will most likely not survive the financial burdens that such an event will place upon them.

- Is each computer on your site running on a battery backup?

This is perhaps the most overlooked aspect of any business environment. Without exception every business class workstation with the exception of laptops should be plugged into some type of battery backup solution designed to gracefully shut the machine down in the event of a power loss. When your PC suddenly shuts off in a blackout and you just lost 3 hours of data you were entering and you multiply that by 30 people in your office that was a very expensive power outage. Be smart, get UPS devices in place right away.

- Is each computer saving sensitive/critical data to a server where it's being backed up?

If users on your networks are saving critical data to their local drives then they are a liability and they are putting you at risk. There are many problems with this arrangement. Among the most dangerous are the data will most likely not get backed up. It makes it very easy for someone to steal the laptop, PC or hard drive and walk out. If data is saved to a server stored behind lock and key, then regular backups ensure redundancy and prevent your data from walking out the door. Get your data off of local drives and keep it off.

- Pick any two random people, explain to me what impact it would have if their PC crashed completely and was unrecoverable.

This is one of my favorite questions to ask. Because people think they have a handle on their data until they hit this question. Most often it's like they swallowed their tongue. If your users choke on this question then the odds are their data/recovery methods need a lot of work. You need to identify which machines on their network need a full image provided by products like Acronis True image and which of their systems can get by just by saving their files on a network share. This is a very important decision and it must be made on a case by case basis for every machine on the network.

- Do you want employees to be able to access their work PC from anywhere that has an INTERNET connection? Do you want this for everyone?

This is a new and popular option for many businesses. They had no idea this was even an option and thanks to a product called LogMeIn it's a very simple thing to do and much easier to use than any other technology in the same product family. LogMeIn is top tier and this ability to remotely log in greatly expands the possibilities for many businesses. Making them aware of this option could make you out to be a super star.

- How many laptops exist? Does each laptop user also have a desktop and do they want to synch data?

This question is important for networks that are not running Small Business Server and the answer may or may not provide justification for bumping a network up to Small Business Server. Are there other much less expensive means of doing this? Yes there easily are but none of them are as "set it and forget it because it just works" as what is offered by Small Business Server.

- Who is currently ♦hosting♦ your website and email?

A very important question to ask as there may be limitations imposed by a companies ISP on whether or not they can run *any* public servers on their networks. This includes mail and Web. You need to know up front if the ISP allows servers and what type of bandwidth cap limits exist in the network plan your client has.

- Who is your domain registered with (GoDaddy, Network Solutions, etc.)?

Most clients have no idea what the answer to this question is and nothing will get you panicked more than when your clients domain name registration expires affecting their email and website. You would really like to go renew the domain but have no idea at all where to go or how much it's going to cost. Get this information up front and try to convince your clients to register their domains in 5 year blocks at the minimum.

- Who is your INTERNET service provider and what INTERNET package do you have (512Kb Upload / 1.5 Mb Download) etc.?

This question is similar to who their ISP is. ISPs will impose restrictions on bandwidth, server hosting and other technologies. Some ISPs won't even issue static IPs making it much harder (not impossible) but harder to run email and Web servers.

You want to know exactly the service package your client has and you also need to know what their choices are when it comes to their INTERNET service. Don't hesitate to encourage them to upgrade to a better plan. I've been thanked many times for doing this and I speak openly and honestly to each of my clients about their ISP services and offerings.

- How many computers/laptops/servers do you plan to add this year?

A very important question in many ways. This is a critical question and the answer must be accurate. You may license software that you can only get once a year cheaply. If you need more licenses outside the licensing window, your costs may double or triple. This information will help your client to know if they need to renew their office lease at a current location or plan on finding a new place to operate from. You can also negotiate pricing in advance with certain companies where you can get firm pricing throughout the year on systems as long as you commit to buying X number of systems or more. This piece of knowledge can make or break just about any IT budget. Insist on a firm number from all your clients.

- How many employees or locations do you plan to add this year?

This question is just as important as the one right before it. Some software is licensed per person or per machine. Know your licensing models. If your client plans on adding locations or equipment you need to make sure they allocate funds for all aspects of this growth. It's amazing how adding even one person can have a company writing checks in excess of \$5000 in U.S. currency. It's your job to help clients dodge this bullet and manage costs as much as possible.

- Who is my primary contact for IT related issues including support needs and expenses?

Identify up front who the decision maker is and do not get wrapped up in power struggles. Once the decision maker is identified you need to establish that no work is performed or purchases made without the decision makers signature indicating their approval... PERIOD!!!

- Has your network ever been hacked by spyware, malware or virus? Have any of your current machines had an infection?

Before I take over work on any network I ask this question. If a machine has been compromised it could mean hours of work to clean the entire organization. Get this information up front and find out what type of impact it had on the network and make sure you know what methods were used to correct the problem and how thorough those methods were. Your time and your money may hang on this information.

- Have you ever had a problem with pornography or INTERNET abuse in your office(s)?

If the answer to this question is yes, then you may have problems in the form of the question above this one and not even know it. Most of the very severe spyware and malware originates from pornographic sites. Knowledge is power in this case, make

sure you know before you commit to a support agreement. Always exclude this type of work from your agreements. I charge by the hour to clean a clients network of any trouble caused by INTERNET abuse. I have a zero tolerance policy on this and I won't budge.

- In the last 2 years what are the names, usernames of employees that have left your company?

A no-brainer here. This is just good house-keeping. You don't want orphan usernames and passwords hanging out on your domains. It could have very serious ramifications. Clean it up immediately when you come across it.

- For employees that have left, were all their related IT accounts disabled/deactivated?

In the same spirit as the question above, it makes sure you understand what access each employee has to what resources. Pursue each user account with prejudice and lock it down. You are responsible and you will be liable for any oversight on your part. Don't take chances.

- Do you feel like someone or some person would be motivated to break in and steal your intellectual property or ideas?

Most companies are very surprised by this question and its answer. If the answer is yes, then make sure all IT/IP is behind lock and key. All servers and sensitive drives, devices and data should be kept behind a closed and locked cabinet or office door.

- Do you feel like an employee might be persuaded to copy your data and sell it to a competitor?

If this is possible establish rules on your networks regarding USB drives, cameras and phones. Make sure people understand they can be fined or terminated for bringing them onto the premises.

- What are your feelings towards having an employee or visitor ♦walk-off♦ with a hard drive or a computer?

Is your work environment casual enough where employees can take their work home? Make sure you are not at jeopardy of losing sensitive data. Make sure you have good security measures in place when your technology leaves the premises.

- How often are passwords changed in your office and do you feel like you have a good security policy in place?

Do you have password length, complexity and expiration limits in place? Do you need them? Make sure you are doing as much as you need to in order to protect your data. If screen savers need to lock workstations after 1 minute of inactivity, then you need to change it from the default of 15 minutes. Think about these things and act on them.

- Do you want everyone to have access to all your data or do you want to control access on a per-user/per-group basis?

How sensitive is your data? Do you need user, group and role based security? Should you establish regular audits of user permissions? Do you want to have optimistic (Default allow) or pessimistic (Default deny) security in place? Make your decisions based upon what's at risk.

- Will you be having interns work with you or outside agencies that need user accounts?

A great question and a huge liability in any environment. With HIPAA and medical student interns this is a biggie. Don't mess around. If your environment needs to adjust to these situations, have strict security policies and procedures in place ahead of time. Make sure logging, sniffing and monitoring is configured and tested before your first intern arrives. Products like 1st Security Agent can save your company. Make sure you buy the right tools for your security job.

- Are you operating a wireless network or do you plan on operating one in the next year?

Do not for any reason use wireless networks unless there is a business reason to do so. If there is, invest in very expensive wireless equipment that has threat measures and counter-measures built in. Your wireless network should be aggressive towards intruders and make sure you understand the risks involved with a wireless network.

- With regards to wireless, do you want it secured and isolated off of your local network shared by the desktops?

If you must use wireless networks, then isolate them. Keep them on separate subnets from your regular network and require strong encryption VPN clients to negotiate access. Make sure your access point can detect rogue access points and wireless sniffing technologies and shut them down.

- What sort of anti-virus are you using on site?

If it's by Norton or Symantec then you might as well save your money and just hand out copies of your data on CD to total strangers. Do your research and select a good anti-virus product that meets your needs. Understand that anti-virus must take place at the INTERNET gateway or firewall, the email server and the users desktop. Fail to enforce anti-virus in any one of these areas and you assume all risks.

- Are you using the same anti-virus on laptops?

You should make sure you have a multi-threat anti-virus, spyware and malware client on your laptops. This might mean using a combination product like ZoneAlarm or multiple products such as Webroot Spysweeper and AVG. Laptops face a totally different set of risks than desktops. Your desktops may be sitting behind thousand dollar firewalls that detect and eliminate 99% of security threats. Your user out in the Ameritel Inn may not be behind any firewall and his laptop just got hosed because you didn't have a good multi-threat client installed and running.

- Are people allowed to bring their own computers/laptops to work?

No! End of story.

- Does anyone receive their email on a cell phone?

Make sure you understand who, where and why. If that person leaves the company make sure you take the appropriate steps to disable this feature immediately. This could be a security risk and you need to make that decision on a case by case basis.

- Have you thought about a yearly budget for IT related hardware/software/service expenses?

You absolutely must have an IT budget and goals. Establish yearly cycles for product replacement. Ideally hardware should be replaced every 3 to 4 years and software should be evaluated and updated every 1 to 2 years. Make sure your budgets allow for this. It's your data that is at risk so make good choices here.

- What is your replacement plan for old equipment? (Replace every 2/3/4/5 years? or Replace as it fails?)

If you choose to replace equipment as it fails your data is at a much higher risk. Make sure your backup strategy takes this into account and always make sure backups are verified and that you run fire-drills twice a year where you attempt full-fledged restores to make sure your backup process is effective and your restore process is understood. Front to back awareness will make your life easier and save you money.

- Do you use any special or in-house 3rd party software not bundled by Microsoft?

Make sure you have proper support agreements in place. Make sure you understand hardware and operating system compatibility. Make sure you understand licensing costs and how hardware will affect those costs. Some products have a per-processor cost. It pays to know these things up front.

- If your entire network were to come crashing down how long could you survive without it? (1/2/3/.. days? A month?)

Use the answer to this question to determine how much money you put into your backup process. The higher your required uptime availability, the more money should be spent on your backup processes. Don't go cheap. It's your data. You may cease to exist or burn bridges with valuable customers without it.

- Do you want to maintain a low-end, low-performance server that could be swapped in during a major failure?

This may be a good idea. Keep a dog-eared server in the mix and use him if the world ends tomorrow. Having gimpy, the 4 year old server as a stand-by could be the difference between profit and loss. Make this decision on a business by business, and in some cases a department by department basis. Never assume that your

Kajillion Dollar server will run forever. That's about when it will crash throwing you in front of the high speed train.

- How much is your data worth? Develop a number and keep it in mind as we discuss current systems and improvements.

If your data is worth more than your mother then make sure you have good processes, procedures and equipment protecting it. If you cut corners, you are taking big risks and you may be liable for fines, penalties and imprisonment from Uncle Sam if you screw up. Know your responsibilities and make sure you have your contingency well laid out and a good reaction plan in place.

So now you have your client's responses but what do you do? How do you quantify all of this and put it into something usable? Just as important is how do you establish a rate for charges and establish priorities for improving the network in all spaces? These are great questions and you really must sit back and look over the data you have received. Try to categorize responses into what I call "network space". Any time I refer to "email" or "storage" I'm referring to a "space" within the existing or planned network. By creating a notion of spaces, you can establish layers for your network that will help you to establish tasks and rank them by cost and priority. You should always be aware of every aspect of your network space and get used to thinking of the various spaces you can divide your network into. Spaces will save you time, multiply your efforts and result in a proper and well thought out plan for managing your infrastructure now and into the future.

Now that we've established spaces and discussed the idea of creating spaces and dividing the answers to these questions into individual spaces, let's talk about what we do with this information and how we prioritize it. In a perfect world your client or manager will say, "Fix it all and spare no expense." but that never happens and for good reason. No company would survive if that kind of shoot from the hip philosophy prevailed when it came to spending. So what matters most? You have a client that has limited resources and needs to implement changes over time. How do you determine what should be done first and what should have first dibs on the available budgets? This is easier than you might think. You just need to step back and get some perspective. Above all the data is the most important aspect of any network whether that data is email, databases, documents, etc... data is king. Your first priority is to protect the data in two ways. Those two ways are security and redundancy. If you have a weak network perimeter that is open to various attacks then you need to resolve that immediately. If you have no backup/recovery plan and no resources to implement one, then get it done and do it today.

Once we have protected the data at the perimeter and at the disc level we can begin to prioritize other tasks on a departmental, individual or company strategy. From the data we have collected, let's try and define some spaces. In no particular order we have:

- Perimeter Security Hardware
- Server Hardware "Bare Metal"
- Server Software "Tools"
- Logical Network Segmentation "Email / Web / Data"

- Disaster Planning ♦ Storage / Recovery
- Power Protection Schemes ♦ UPS / Surge / Cleansing
- Data Management Methodology ♦ Accessibility / Security / Organization
- System State Management ♦ Disk Imaging Vs. File Selection
- Remote Accessibility ♦ Outlook Web Access (OWA) / VPN / Remote Desktop
- Data Replication ♦ Desktop-to-Laptop / Server-to-Server
- ISP Provision ♦ Bandwidth Maximums / Public Servers / FAP Limitations
- Domain Management & Registration
- Projected Growth ♦ Systems / Servers / Infrastructure / Staff
- Key Decision Makers ♦ CFOs / CEOs / VP-IT
- Acceptable Use Policies & Provisions
- Turnover Management Systems
- Physical Access Control ♦ Security Systems / Locks / Cabinets
- Security Policy & Procedure
- Connectivity ♦ Wired / Wireless / VPN / SSL
- Data Threat Sentry ♦ Anti-Virus / Anti-Spyware
- Portable Data Assistants ♦ PDA / Laptops / Cell Phones

Start to rank what your priorities are. Each individual department or business entity has a basic understanding for where money needs to be spent in the short-term. What is lacking is a vision for how to manage current assets to prevent them from becoming liabilities and how to plan for and predict future needs to grow and scale with changing business models. If you haven't surrounded yourself with people who can comfortably help you establish this then you may need to consider staffing changes or hiring a consultant. This stuff comes naturally for some and others really have to work at it. So start by breaking all this information up into large problems that can easily be broken up into smaller sub-problems that can be easily solved with minimum time and money.