



IT Infrastructure Essentials

by Steve Tilkens, DSA Technologies, Inc.

Whether you are inheriting an existing IT infrastructure or building a new one from the ground up, there are essential technologies and strategies that must be implemented to ensure a secure and stable environment. Through years of providing administration/implementation services of information systems/networks, I have achieved a high level of client satisfaction by implementing the following solutions/strategies.

Backup/Disaster Recovery (DR) Plan – Whether your environment consists of a single desktop with a few gigabytes of data, or a large firm with terabytes of data, a backup strategy and DR plan must be defined, implemented, and most importantly tested. While cloud backup solutions offer all of the protection with none of the hassle, traditional backup technologies such as tape are still an effective solution. The goal should not be simply to implement a data backup strategy, but a data recovery solution. DR plans can consist of a replicated site location with identical equipment on standby in the case of an emergency, or simply ordering new equipment and restoring from backups if needed. Creating a DR plan is usually started by asking management the question, “What would happen to your company tomorrow if the office burns down tonight?”

Supported Hardware/Software – Having an infrastructure that runs on old hardware that does not have a support contract with the vendor will eventually lead to restoring data from backups or making your DR plan a reality. This includes your servers, switches, routers, phones, and even printers. Not only does the physical equipment need support, but your applications do too. Having vendor support greatly reduces the amount of time spent getting things working again when they break, and believe me they will, which leads to higher productivity for the business.

Power/AC – This one, in my opinion, is pretty much a no brainer. None of the servers or network devices can run without power and they all generate heat. I will however stress the importance of a quality uninterruptible power supply (UPS). Not only does a good UPS supply battery backup power to your systems in the event of a power failure, but if it includes power conditioning features then it also supplies your equipment with a much cleaner stream of power/voltage which protects your equipment from power spikes and surges. Obviously, AC is required to keep the systems from overheating and causing damage to their internal components.

Network Monitoring – If there is one thing I have told my clients time and again it is that network monitoring is far more than just pinging network devices. While ping tests are great for ensuring that devices are responding to network traffic, they offer nothing more than a heartbeat to endpoints and only alert you after something has failed. Effective network monitoring consists of polling CPU, Memory, Network Utilization, Temperature, Windows Services, Disk Space, Power Supply Units, Fans, Event Logs, etc. Simple Network

Management Protocol (SNMP) makes much of this monitoring possible and is supported by most network devices and operating systems. A well implemented network monitoring system can alert administrators to the onset of problems before they become critical and affect business productivity for end-users.

Redundancy – A difficult reality for network administrators to face is that there is no way to avoid hardware failures – all network hardware will eventually go bad one day and stop working. Planning for this fact is the only way to avoid being caught off guard by failed hardware. Eliminating as many single points of failure in your network as possible will ensure that when a critical component fails, business will continue to run – hopefully without a significant impact to end-users. Identifying the single points of failure in your network and planning for when they do fail is critical. One thing I have discovered throughout my years of IT consulting is that no matter how much redundancy you can afford to build into your network, there will always be a single point of failure.

Firewall – Security is usually one of my clients' biggest concerns when it comes to their network infrastructure. Implementing a hardened firewall device is the quickest and most effective way to keep your network safe from the outside world. Firewalls not only block unwanted traffic but they offer other advantages as well. If the business demands that one of your applications be public facing, then it should be architected with a front-end application server in a DMZ to avoid direct access to your internal network. While dedicated SSL VPN appliances are best for remote access, many firewalls on the market today offer built-in VPN features that cater to remote end-users. A firewall is an absolute necessity for every network infrastructure no matter how large the business.

Antivirus – While firewalls are great for blocking unwanted inbound traffic, they are useless against viruses, spyware, and malware programs brought into your network inadvertently by your end-users. Antivirus products are essential in ensuring the security health of operating systems – both client and server. Whether users mistakenly visit a malicious website or they plug in an infected USB flash drive, a good antivirus program should identify and stop the threat before it causes damage. A centrally managed antivirus product clearly has its benefits but also comes with a cost. There are many free products on the market today that offer just as much protection as the paid products if centrally managed administration is not required.

IT Support – Having top of the line network/server equipment implemented in a perfect fashion is all for nothing if no one is there to support and maintain it. Ensuring that someone is keeping an eye on daily backups, security and application updates, event logs, storage space, etc. is vital to the health of any network infrastructure. Your IT support team should be comfortable with the administration and troubleshooting of servers, network, databases, applications, backup, etc. In addition to monitoring and maintaining the infrastructure, your IT team should be driving the strategic IT initiatives that enable your business to increase productivity and be more successful. An IT business plan is critical to ensure the technology is aligned with long-term company goals.

The things mentioned above are just the essentials for a network infrastructure to be successful. Obviously most companies require a lot more, such as e-mail, spam filtering,

shared storage, custom applications, cell phones, tablets, etc. Virtualization is a technology that was not discussed above but is becoming more and more standard in datacenters. Even small companies can realize the benefits of virtualization. Virtualization makes greater use of your server hardware by sharing its resources among many virtual machine operating systems which reduces the need for having so many physical servers. Another trend that is emerging is a concept known as virtual desktop infrastructure (VDI) which is made possible by virtualization. VDI greatly simplifies the administration and provisioning of desktop systems for end-users by utilizing virtual machine desktops that are consolidated in the datacenter.

By implementing the technologies and strategies above you can expect a higher level of security and reliability from your infrastructure. Please feel free to contact me if you are interested in learning more about any of the technology discussed above, or if you would like to request an IT assessment.

Steve Tilkens

DSA Technologies, Inc.

Business Vision. Technology Focus.

Maritime Office Plaza | 2372 Maritime Drive | Elk Grove, CA 95758

Office 916.567.4444 | Direct 916.753.1132 | Fax 916.567.4440

LinkedIn Profile - <http://www.linkedin.com/in/stevetilkens>