ADVANCED OFFICE SYSTEMS

296 East Main Street
Branford, CT 06405

IT Discovery / Assessment Report
Conducted on: DATE (MM/DD/YYY) HERE
On-site Discovery By: AOS ENGINEER NAME
Assessment Document By: AOS ENGINEER NAME

For:
CLIENT NAME HERE
CLIENT ADDRESS HERE

1. Current IT Setup and Configuration

a. Network Infrastructure

i. Internet Connection: 90/30 Comcast Cable Internet
ii. Firewalls/Routers: (2) Cisco ASA 2510, (1) SonicWall SRA 1200 SSL-VPN, (1) SonicWall NSA 240
iii. Switches: (2) Dell PowerConnect 2724 24-port 10/100, (3) HP ProCurve 2610-48 48 port 10/100/1000, (1) HP ProCurve 2610-24 24 port 10/100/1000, (1) Netgear ProSafe FS105 5-port 10/100.
iv. Wireless Access Points: (5) NetGear G54/N150 Wireless Router
v. Remote Locations: 4 Remote Locations

b. Server / Workstation Configuration

i. Dell PowerEdge 2800 – “SERVER NAME X”

- Warranty Expiration: 6/7/2013
- 2.8GHz Intel Xeon CPU
- 4GB RAM
- Windows Server 2003 R2 Standard
- C: Volume: 68GB total, 31GB used
- 4 Network Interfaces
- Server Roles: DC for CLUBHOUSE domain

ii. Dell PowerEdge SC430 – “SERVER NAME X”

- Warranty Expiration: 3/9/2009
- (2) 3.20Ghz Intel Pentium D CPU
- 3GB
- (2) 160GB 7.2K SATA Drives in RAID 1
- Windows Server 2003 R2 Standard
- C: Volume: 12GB Total, 8.18GB Used. D: Volume: 137GB Total, 106.3GB used
- 2 Network Interfaces
- Server Roles: DHCP, DNS, SQL, File Replication
- Applications: Crystal Reports, PeachTree Quantum, Pervasive PSQL

iii. Dell PowerEdge R710 – “SERVER NAME X”

- Warranty Expiration: 10/23/2014
- 2.4GHz Intel Xeon E5530 CPU
- 4GB RAM
- (4) 300GB 10K SAS Drives in RAID 5
- Windows Server 2008 Standard
- C: Volume: 40GB Total, 32.44GB Used. D: Volume: 793.58 Total, 496.08 Used. E: Volume: 3GB Total, 1GB Used. G: Volume: .05GB Total, .05GB Free
- 4 Network Interfaces
- Server Roles: Domain Controller, DHCP, DNS, FSMO Holder, File Replication
- Applications: SQL, SAGE, Volunteer Accounting, PeachTree Quantum 2010, HRIS, ABIL Accounting Software

iv. Dell PowerEdge 2900 – “SERVER NAME X”

- Warranty Expiration: 3/8/2015
- 2.33GHz Intel Xeon E5410 CPU
- 12GB RAM
- (3) 250GB 7.2K SATA drives in RAID 5
- Windows Server 2008 R2 Standard
- C: Volume: 50GB Total, 37GB used. D: Volume: 414GB total, 233GB used
- 4 Network Interfaces
- Server Roles: DNS, IIS.
- Applications: Exchange Server 2010

v. Dell PowerEdge R710 – “SERVER NAME X”

- Warranty Expiration: 10/23/2014
- 2.4GHz Intel Xeon E5530 CPU
- 16GB RAM
- (6) 146GB 15K SAS drives in RAID 5
- Windows Server 2008 R2 Standard
- C: Volume: 80GB Total, 56GB used. D: Volume: 598GB total, 3GB used
- 4 Network Interfaces
- Server Roles: Remote Desktop Services, DNS, IIS
- Applications: PeachTree Quantum, Crystal Reports

vi. Dell PowerEdge 2900 – “SERVER NAME X”

- Warranty Expiration: 6/25/2015
- 2.00GHz Intel Xeon E5405 CPU
- 8GB RAM
- (4) 146GB 15K SAS drives in RAID 10
- Windows Server 2008 R2 Standard
- C: Volume: 272GB Total, 118GB used
- 2 Network Interfaces

- Server Roles: IIS
- Applications: SAGE, Primary SQL Server, SpiceWorks, Old EHR Application

vii. Dell PowerEdge 2900 – "SERVER NAME X"

- Warranty Expiration: 6/25/2014
- 2.00GHz Intel Xeon E5405 CPU
- 8GB RAM
- (4) 146GB 15K SAS drives in RAID 10
- Windows Server 2008 R2 Standard
- C: Volume: 272GB Total, 120GB used. E: Volume: 149GB total, 122GB used
- 2 Network Interfaces
- Server Roles: IIS
- Applications: Secondary SQL Server, Mail Archive Server

viii. Dell PowerEdge R200 – "SERVER NAME X"

- Warranty Expiration: 6/24/2014
- 2.00GHz Intel Xeon E5405 CPU
- 8GB RAM
- (4) 146GB 15K SAS drives in RAID 10
- Windows Serer 2008 R2 Standard
- C: Volume: 272GB Total, 38GB used.
- 2 Network Interfaces
- Server Roles: IIS
- Applications: SQL Witness Server, PeachTree Quantum, ABIL Accounting Software

ix. HP ProLiant MicroServer – "SERVER NAME X"

- Warranty Expiration: 1/25/2014
- AMD Turion II Neo N40L Dual-Core CPU
- 8GB RAM
- Windows Server 2012 Standard
- C: 97GB Total, 31GB used
- 2 Network Interfaces
- Server Roles: RODC, DNS, DHCP
- Located at EARN site

x. Outlook 2010 Connecting to Exchange 2010 on premises.

xi. Around 110 Workstations – Most workstations are running Windows 7

c. Backup Configuration

i. Software: EVault Cloud-based backup solution

ii. Hardware: None

d. Software

i. Their primary application is "CareLogic EHR".

ii. Antivirus: VIPRE Managed Antivirus

2. Analysis and Recommendations for Improvement

a. Network Infrastructure

i. Firewall Upgrade and Consolidation (Main Location):

CLIENT currently has a SonicWall NSA 240 as well as two Cisco ASA firewalls. Having multiple firewalls over-complicates the network setup. Modern-day firewalls have the ability to act as a firewall and router for multiple network subnets, so there's no need to have a separate firewall for each physical or virtual network. The SonicWall NSA 240 is going End of Life on 5/1/15 and no support will be provided for this device after that date. My recommendation is to purchase a new current generation SonicWall appliance. We will configure the device to act as a single Firewall and Router solution for both the "Public" and "Corporate" networks. This will allow us to decommission the two Cisco ASA devices as well as the NSA 240 consolidating three firewalls down to one. We will also work with CLIENT to configure the new SonicWall's web content filtering to make sure their clients do not access restricted websites.

ii. Network Switch Upgrade and Network Isolation:

There are two Dell PowerConnect 10/100 switches in place. 100MB switches bottleneck network performance between the workstations and the servers. I recommend upgrading these to a Managed 48-port HP ProCurve Gigabit switch. This will make it so that all switches in the environment are managed switches and are not bottlenecking network performance. Once this is in place, we can validate that network security is meeting the appropriate standards. We will go through and confirm that the Public and Corporate networks are either on separate physical switches or isolated by separate virtual networks (VLANS) always adhering to the customer's specific security requirements.

iii. Remote Firewalls and VPN Tunnels:

Network connectivity to the remote locations is severely lacking. With the exception of the EARN location, remote sites are not connecting back to the main site. This connectivity would allow centralized management of all of the sites and allow the remote sites to tap into server resources at the main location. My recommendation is to install smaller SonicWall firewalls in each of the remote locations. This would increase the network security at each remote site as well as allow us to create a VPN Tunnel between the main site and each remote site. These tunnels will bridge the remote networks into the network at the main location.

iv. Wireless Access Points:

During our network assessment, we noticed that wireless coverage was very poor. The Netgear access points that are currently in place were designed more for home use rather than corporate use. The quantity and quality of these access points are insufficent to service the number of clients using them. I recommend upgrading to our Ruckus Wireless solution. The solution includes enterprise class access points and a Zone Director access point manager. One of our wireless experts will come on-site with tools to map out exactly where wireless access points need to be placed in order to have the best coverage. The Zone Director allows us to manage all of the access points in your organization from one central location. We will have the ability to set up separate wireless network for "public" and "corporate" use, always keeping security in mind.

v. SonicWall Global Management System (SGMS Agreement):

SGMS is a SonicWall managed services agreement that allows AOS to monitor and maintain your SonicWall firewalls. SGMS includes features such as automatic firmware updates, configuration backups, extended manufacturer warranty, and next business day hardware replacement

b. Server Configuration

i. Server Virtualization and Consolidation:

CLIENT has 8 physical servers at their main location. Their two newest servers are 4 years old and the other 6 servers are between 6 and 8 years old. Many of these production servers have expired manufacturer warranties. It is extremely important to move away from all of the aging hardware. If a hardware failure were to occur on an out-of-warranty server, it could require expensive replacement parts and would also bring down the organization while these parts are getting ordered and replaced. Two of the servers are running Windows Server 2003 which is going End of Life in 2015. Running an unsupported OS is a major security risk because Microsoft will no longer be providing security patches. We also believe that some of their servers are performing roles or functions that are no longer needed or have already been migrated to other servers. It would be a good idea to decommission servers where necessary. We would like to take a comprehensive approach to resolving these major server issues. Here are the steps that we recommend to get your server environment into a healthy state:

- Purchase a new Dell PowerEdge server to act as a Hyper-V Virtualization Host server. This server would be powerful enough to run all 8 of the current servers inside of it and still have plenty of room for growth.
- Convert the 6 servers that are running Windows Server 2008 or higher into virtual machines and run them on the new server. Determine if some of these servers can be decommissioned immediately. If a server is hosting a few roles or applications, migrate these roles and applications to another server so that we can consolidate the total number of servers down to a smaller number.

- Migrate any Roles and Applications off of the two servers running Windows Server 2003 so that these servers can be decommissioned and shut down.

Virtualizing their servers will allow us to shut down all of their outdated server hardware and get them running on a machine that is under warranty. Moving to a virtual environment will give them a performance boost as well as the freedom to adjust server specifications (CPU, RAM, Hard Drive) as needed. It also adds future-proofing as we can spin-up new virtual servers on the fly should the need arise. While it may be disconcerting having one physical server be responsible for many different virtual servers, we believe this concern is mitigated by having a strong backup and disaster recovery system in place. See the Backup Solution section for more details.

ii. Office 365 – Hosted Exchange:

CLIENT currently has an on-premises Exchange 2010 server. John Lynch mentioned interest in migrating to Microsoft's cloud-hosted Exchange, part of the Office 365 suite. Office 365 provides businesses and organizations with full Microsoft Exchange connectivity and features without having to run an on-site Exchange server. This means that if your building is offline, mail continues to flow in and you can still receive it on your mobile devices. You also get the ability to create shared distribution groups, calendars, and contacts just as you would with an on-premises Exchange server. Active Directory passwords also sync with Office 365, so users will have one password for the computer login as well as their email login. Using Office 365 puts the hefty hardware requirements and liability of running an Exchange server onto Microsoft rather than having to worry about it yourself.

iii. Network Server Agreement (Managed Servers):

NSA is a managed services agreement that allows AOS to monitor and maintain your servers. NSA includes features and services such as server hardware monitoring, security patching, and user account administration. It also includes remote problem resolution and on-site response for critical server problems that stop business functions.

c. Backup Configuration

i. Backup Solution:

CLIENT is currently using EVault Cloud Backup for their backup solution. This is being managed by their current IT provider. EVault is an imaged-based cloud-only backup solution. This means that an entire image of each server is backed up and saved directly to the cloud. Cloud-based backups are good because the data is instantly saved off-site for disaster recovery purposes. The problem with this is that there is are no local (on-site) copies of the backup data. If an entire server needed to be restored from backup, the process would take hours or even days. The entire image of the server would either have to be downloaded from the cloud or shipped over on an external hard drive. A good backup solution should not only back up servers, it should also offer business continuity

AOS offers a backup solution that solves all of these problems. Our backup solution is a hardware appliance that takes hourly snapshots of your servers. These snapshots are image based, so restoring a server from bare metal is quick and painless. These snapshots sync to a secure datacenter in the cloud, but are also retained on the on-site hardware appliance. This "hybrid backup" solution allows you to get the speed and reliability of on-site backups as well as the redundancy and availability of cloud backups. This device also has the ability to instantly create a virtual copy of your backed up servers in the event of a hardware or software issue with your primary server. If one of your servers has a hardware or software issue, we can spin up a virtual copy of the server on the backup appliance and get you back in business within minutes. Additionally, you also get the ability to boot your servers up virtually in the cloud datacenter. In the event of a disaster or extended power outage, we can power up your machines in the cloud and allow your users to gain access to them so the business can continue to function even if the building is out of commission. AOS can manage the backup operations and resolve any issues that come may come up.

d. Software

i. Antivirus Software:

CLIENT is currently using a managed version of Vipre Antivirus. The software is being managed by their current IT vendor. Should CLIENT decide to do business with AOS, they would need to migrate away from Vipre. AOS offers a similar cloud-based AV solution called Symantec.Cloud. This antivirus software offers fast and effective protection from viruses and malware. The management server is cloud hosted which allows for centralized management of all of their AV protected machines. This makes it easy for us to set up security policies at a global level and apply them to all protected machines. It also makes it so virus definition updates get pushed from the cloud rather than relying on an in-house server

3. Priority

Here is the order in which I believe CLIENT'S issues should be prioritized:

i. Server Virtualization / Consolidation:
It is critical to move away from the current aging hardware and unsupported operating systems as soon as possible.

ii. Backup Solution:
Protecting against data loss and downtime is extremely important. This phase compliments the Server Virtualization phase.

iii. Firewall Upgrade:
Security is a big concern and having an End of Life firewall in-place isn't going to cut it. Cleaning up and consolidating the networking equipment will also help with the manageability of their network setup.

iv. Switch Upgrade:
This compliments the Firewall Upgrade phase. Making sure the two networks are separated is a security necessity.

v. Remote Firewalls:
Getting the remote locations to connect to the main site will enable central IT management.

vi. Wireless Access Points
Ruckus Wireless will improve the reliability, performance, and security of the wireless setup.

vii. Office 365 – hosted Exchange
Hosted Exchange will make it so email is no longer dependent on any of the local servers being online.