Final project: executive summary for network design project essay sample

Technology, Computer

CphoeniX Inc.’s Network DesignOctober 25, 2009Executive SummaryCphoeniX INC is a small organization that specializes in aircraft maintenance. The company’s headquarters are based in Illinois; and they have facilities located in four other states as well. Each facility or office then consist primarily of four departments; maintenance, accounting, receiving, and shipping. Due to the breakdown of each department, and the multiple facilities, constant sharing of data, programs and various applications will need to be accessible over a Local Area Network (LAN); as well as over a Wide Area Network (WAN), and via remote access. The goals of the network, both LAN and WAN, are to allow for a secure yet easily expandable network, that allows real-time data transfer.

When planning the LAN for CphoeniX INC, there were multiple considerations to take into account; the main concerns being the integrity and accessibility of the data over the network; as well as the ease of expanding the network. Along with these concerns, it has also been decided that each department needs to be able to share peripherals devices; such as scanners, copiers and printers. For this reasoning, the LAN in each of the facilities will use a star topology for its setup. CphoeniX Inc.’s star topology LAN will consist of Cat 5 e and 100Base-T cables. These cables will provide the necessary support for the network design allowing for speed and integrity. As well, this network layout will also allow for network expansion and management; and help support the future goals of the company.

As for the WAN that is to be used to connect the facilities to one another, there are a few key factors that need to be considered; the requirements of

the WAN. These requirements include: being able to allow each facility to be able to connect, or rather be connected to the WAN to allow the accountants at headquarters access to all financial data. The WAN must allow for approximately 40 users at any given time on the WAN; that use the WAN for approximately an hour at a time. And due to constant accessing of the data, a synchronous connection needs to be established between each facility's LAN. So based on factors such as these, it has been decided that a SDSL connection would be optimal for CphoeniX Inc.'s WAN.

Like with any company, CphoeniX Inc.'s data is sensitive, and needs to stay secured. So when accessing the data off site, security measures need to be put into place to allow for the viewing of this sensitive data. For this reasoning, a VPN will be used to access the network remotely. VPN remote access connections use authenticated links to ensure that only authorized clients are able to connect to the organization's LAN. These authenticated links provided by VPNs will allow CphoeniX Inc. the ability to connect to its branch offices over a public network while maintaining secure communications.

In conclusion, it is believed that by implementing the following network specifications, CphoeniX Inc. will be able to continue its network's growth, and continue to allow the accessibility required to allow production to continue under various circumstances. However, the growth and security of the network is, and will continue to be constrained by the financial backing that the network is allotted.

Cabling SpecificationsWhen building the CphoeniX Inc.’s network physically, the cabling contractor will need to comply to the checklist provided below:•Category 5E Cable used to connect all devices to central hub portsoUses Rj45 connectorsoCategory 5E cable segments do not exceed 100 meter in length•100Base-T cable used to connect all hubs to the MFDoUses Rj45 connectors100Base-T cable segments do not exceed 100 meter in lengthLocal Area Network (LAN) TopologiesCphoeniX INC is an organization that specializes in aircraft maintenance. The company’s headquarters are based in Illinois; and they have facilities located in four other states as well. Each facility or office then consist primarily of four departments; maintenance, accounting, receiving, and shipping. Each department is then broken down in to specialty groups to allow for a more thorough work production. Due to the breakdown of each department, constant sharing of data, programs and various applications will be needed over a Local Area Network (LAN). When planning the LAN for CphoeniX INC, there are multiple considerations to take into account; the main concerns being the integrity and accessibility of the data over the network as well as the ease of expanding the network.

With each department broken into specialty groups, data needs to not only be shared, but more importantly saved in accessible locations for each department that needs access to the data. For instance, certain accounting positions will require access to all data concerning shipping and receiving to maintain up-to-date financial records. However, the shipping and receiving departments do not require access to the accounting department’s data.

One such way to accomplish this is through the use of a central storage unit, or server that is specifically for data and file sharing amongst all four departments. Along with specified data accessibility over the network, CphoeniX INC also requires daily backups of all data pertaining to each department, and that all finical data is to be saved indefinitely to a secure location.

Other specifications for CphoeniX INC's LAN include that each department is able to share peripherals devices; including scanners, copiers and printers. As well, CphoeniX INC would also like to be able to provide external access to the LAN for employees who are on the road, or simply away from the facility of any given reason. However, for security purposes, an internal and external authentication, or verification process will need to be established for each employee. And finely, CphoeniX INC's LAN will need to consider expansion capabilities to allow for any additional devices that may be required in the future.

Data sharing between each department is the most important concern for CphoeniX INC, so company will need a network topology that will allow network access to a majority of their employees even in the event of a failed network segment. Network topology refers to the layout or design of a computer network's interconnections used to connect all its microcomputers and other computer devices (Walton, 1990). When it comes to network topologies, there are three most commonly used (Hallberg, 2005); these topologies are: bus, ring, and star. However, based off of the specifications

mentioned above, the most effective topology to be used in each of the CphoeniX INC offices would be the star topology.

The star topology is a network that uses a central unit, often referred to as a hub or switch, to host a set of cables that radiate out from the hub to each node or workstation on the network (Hallberg, 2005, p. 43). According to Cisco Systems, Inc. Internetworking Technology Handbook (n. d.): A hub is a physical layer device that connects multiple user stations, each via a dedicatedcable. Electrical interconnections are established inside the hub. Hubs are used to create aphysical star network while maintaining the logical bus or ring configuration of the LAN. Insome respects, a hub functions as a multiport repeater.

(¶ 20)So instead of each station being directly connected to one another, such as in a standard bus or ring topology, a star topology allows for each device on the network to have a point to point connection with the central hub. The primary benefit to using the star topology is that it will reduce the chance of network failure since each device connected to the network is directly connected to the central hub. So “ if any single network connection goes bad (is cut or damaged in some way) only that one connection is affected” (Hallberg, 2005, p. 45).

When the star topology is applied to a bus-based network, meaning that it uses an Ethernet based connection, the central hub echoes all transmissions received from any connected node to all other nodes on the network. Therefore, all connected nodes communicate with all others by transmitting

to, and receiving from the central hub only. In the event of a failed network segment, the star topology will isolate the node that it links to the central hub; but only that node will be isolated. In such an event, all the other nodes will continue to function properly, except they will be unable to communicate with the node that has been isolated. If any node connection were to go bad, none of the other nodes will be affected. However, if the central hub were to breakdown, the entire network will be affected (TechTarget, 2006).

As well as the benefit of reducing the chance of network failure, a star topology is the easiest topology to expand upon. With the use of a hub, the star topology simply relies on the number of ports that the hub has. And if more ports are needed, another hub can be connected to the central hub to allow more devices to be added to the network by the use of a patch cable. This additional hub is known as a patch panel. Then when a new device, such as a printer or a new workstation, needs to be added; the new device simply needs to be connected to the central hub or the patch panel. However, since each node is connected to the hub with its own cable, the star topology does require the use of more cable than a standard bus or ring topology.

The LAN topology for CphoeniX INC. will be relatively simple in terms of set up. Since CphoeniX INC’s departments are within proximity to one another, the best layout for the star topology would be as follows; because it allows the system to be not only expandable, but easily accessible as well.

Each department within the CphoeniX Inc.’s offices will be connected to one another through the use of the star topology LAN; which will terminate to separate network devices located in an intermediate distribution frame closet (IDF). Each of the IDF closets on the network will then be linked to a main distribution frame closet (MDF). The MDF closet will hold a switch that is responsible for connecting to the network’s router. The advantage to using such a setup is that it can be used with multiple cabling options.

The cabling specifications that will be used in the CphoeniX Inc.’s star topology are as follows. CphoeniX Inc.’s star topology LAN will consist of Cat 5 e and 100Base-T cables. Category 5 cabling is capable of data transfer rates of 100 megabits per second, which will allow it to employ 100Base-T Ethernet; which is also known as Fast Ethernet. These cables will provide the necessary support for the network design allowing for speed and integrity. Cat 5e, and 100Base-T cables will support this topology mainly since CphoeniX Inc. has a close network layout; making these cables the best options for the company. As well, this network layout will also allow for network expansion and management; and help support the future goals of the company.

Wide Area Network (WAN) DesignAs stated previously, CphoeniX Inc. has a total of five offices; with headquarters based in Illinois, and four other offices branched out in four other states. Each of these locations, are then broken down into four main departments; which are then broken down further to specialty groups. Then to share and access data throughout each group and department, each of these locations will be equipped with a star

topology LAN. However, on a daily basis, headquarters will need to be able to connect to each location to share and access data; mainly this has to do with the accounting system. To accomplish such a task, a Wide Area Network (WAN) will be used.

A WAN is used to connect groups of LANs together over a distance. WANs can be used to connect over a short distance, such as connecting offices in the same city; or to connect local offices to facilities on the other side of the world. According to Cisco (n. d.), A WAN is a data communications network that covers a relatively broad geographic areaand that often uses transmission facilities provided by common carriers, such as telephonecompanies. WAN technologies generally function at the lower three layers of the OSIreference model: the physical layer, the data link layer, and the network layer.

(para. 2)With a WAN set up, the accountants at the headquarter office will be able to connect with any of the other four offices' LANs to monitor financial data. By doing so, this will allow the accountants the ability of exchanging data with one another much more rapidly than using the mail, or any other option out there; even email in some circumstances for that matter. Rather, it would be as if the accountants were in the same office; or as if the offices were all in the same location.

To build CphoeniX Inc.'s WAN, there are a few key factors that need to be considered; the requirements of the WAN. By understanding the

requirements of the WAN, the technology to achieve them can then be more easily determined.

Requirements:•All five locations need to be able to connect, or rather be connected to the WAN to allow the accountants at headquarters access to all financial data.

•Must allow for approximately 40 users at any given time on the WAN; that use the WAN for approximately an hour at a time.

•The amount of data being transferred and shared does not usually exceed that of 10KB.

•The accounting application software that CphoeniX Inc. uses requires an encoding rate of 40 Kbps.

•Due to constant accessing of the data, a synchronous connection will need to be established between each of CphoeniX Inc.’s LANs.

Bandwidth CalculationsUnder the requirements listed, it states that the data accounting application software that is used requires an encoding rate of 40 Kbps. So to calculate the total data transfer, the following calculation is used:•First calculate the data transfer per minute.

o40 Kbps multiplied by 60 seconds per minute = 2, 400 kilobits per minute•Next the kilobits per minute need to be multiplied by the average time on the WAN.

o2, 400 kilobits per minute multiplied by 60 minutes = 144, 000 kilobits•Convert the total kilobits to kilobytes.

o144, 000 kilobits divided by 8 bits per byte = 18, 000 kilobytes•Convert the total kilobytes to megabytes.

o9, 000 kilobytes divided by 1, 024 = 17. 58 MBNow, to calculate the required WAN connection bandwidth, the following calculations are used.

•First multiply the maximum concurrent users by the encoding rate.

o40 users multiplied by 40 Kbps = 1, 600 Kbps•Now convert the maximum kilobits per second to megabits per second.

o 1, 600 Kbps divided by 1, 024 = 1. 563 MbpsWan Connection TypesWhen designing a WAN, one must consider what type of connection can be used with the available services. A WAN connection refers not only to the components being used, such as cables, switches, and routers on the physical level; but also the way in which the data is transmitted on the data link layer, and the network layer. According to Warren Heaton (2000) there are three general types of WAN connections offered by most carriers; these are:•Circuit switched connections•Dedicated connections•Packet switched or cell switched connectionsHowever, along with theses three connection types, Hallberg (2005) mentions Digital Subscriber Line (DSL).

Circuit Switched Connection” Circuit switching transmits data streams and datagrams across dedicated physical circuits. To provide asynchronous dial-in and” Integrated Services Digital Network (ISDN) “ services, the telephone

companies use circuit switching” (Heaton, 2000, para. 3). However, due to the low bandwidths that circuit-switched connections offer, theses would not be recommended for CphoeniX Inc.’s WAN.

Dedicated ConnectionsNow unlike circuit switched connections, dedicated connections use point-to-point serial connections that provide a fixed or permanent connection to a remote network. The awesome thing about dedicated connections is the fact that they offer speeds up to T3, or 44. 736 Mbps, over a public carrier’s network. With fixed or permanent connections, dedicated connections allow for less overhead to be required in order to establish communication between two locations. Now since dedicated connections offer such low overhead, as well high bandwidths, they are excellent choices for companies that require WAN connections with a high bandwidth. However, of the three connections, the dedicated connections are on the usually the highest.

Packet Switched or Cell Switched ConnectionsPacket-switched or cell-switched connections, on the other hand, are point-to-point connections that allow the data to travel over a public carrier’s network. Now even though packet-switched and cell-switched connections are more costly than ISDN connections and asynchronous dial-in. Packet switched and cell switched connections are able to provide much higher bandwidths than either circuit-switching connection; and at a much lower cost than dedicated connections. Some examples of packet-switched and cell-switched networks are: Frame Relay, which is packet switched; X. 25, which is also packet switched; and Asynchronous Transfer Mode (ATM), which is cell switched.

DSLDSL is a connection type that can deliver reliable, high data transfer speeds for office-to-office connectivity. Along with DSL’s high speed capabilities, the fact that it runs over traditional twisted pair copper wire makes it available in most areas. DSL is more expensive than standard dialup; but, it is affordable for most small businesses. However, according to Hallberg (2005), there are at least six different choices to choose from when choosing a DSL connection. These include:•Asymmetric DSL (ADSL), which allows for up to 8 Mbps of data to be received and up to 1 Mbps of data to be sent.

•High-speed DSL (HDSL), this allows between 768 Kbps and 2. 048 Mbps connections between two sites.

•Rate-adaptive DSL (RADSL) allows for 600 Kbps to 12Mbps of data to be received and 128 Kbps to 1 Mbps of data to be sent.

•Symmetric DSL (SDSL) allows bidirectional rates varying from 160 Kbps to 2. 048 Mbps.

•Very-high-speed DSL (VDSL) allows up to 26 Mbps of bandwidth.

•ISDN-based DSL (IOSL) speed is about the same as ISDN, but IOSL is used for data almost exclusively, because it is an always-on connection to a single destination, as opposed to ISDN, which can be used to place calls to other ISDN connections.

(p. 86)Connection to be UsedOf the six DSL choices, the SDSL would be an excellent connectivity choice for CphoeniX Inc.’s WAN. The main reasoning

behind this is that SDSL offers the efficient data transfer speeds that meet the requirements. Now since DSLs run over existing telephone-lines, a SDSL connection will also be the most cost-effective way for CphoeniX Inc to build their WAN. As well, the SDSL also allows the WAN to be an on, or open connection always.

DSL HardwareThe use of a DSL connection over a LAN will require the installation of a DSL router provided by the ISP at each CphoeniX Inc. location. However, in order to connect multiple LANs, access routers are used. The access router is connected to each LAN's hub or switch, to serve as a gateway to the WAN. Along with an access router at each location, CphoeniX Inc will also need to establish an enterprise-wide account with an ISP. In turn, the SDSL's constant connection will then also allow for the accountants at headquarters to be able to monitor the daily financial data at each location.

ConclusionIn conclusion, the connection that will be used for CphoeniX Inc.'s WAN will be a SDSL connection. The reasoning for this choice is simply because it not only is the most cost-effective for CphoeniX Inc.; but the SDSL also offers the desired bandwidths to meet the network requirements.

Network Remote Access" Remote access is a set of technologies that transparently connects a computer, typically located in an off-site or remote location, to a network" (Microsoft, 2002, ¶ 2). Simply put, remote access refers to methods used to connect one device to another that are usually on different networks. One way to view it would be that remote access is a

computer program installed on a computer that allows one the ability to access his or her computer from another computer over the Internet, LAN, or phone connection. This access would then allow him or her to access the organization’s network on the computer as if it were the one he or she was at the location. However, to accomplish such a task, there are two different methods to choose from: Dial-Up; and Virtual Private Networks, or VPNs.

“ With dial-up remote access, a remote access client uses the telecommunications infrastructure to create a temporary physical or virtual circuit to a port on a remote access server, which is typically attached to a corporate network” (Microsoft, 2003, para. 2). However, to make this connection the dial-up method requires the use of two modems. The client uses one modem, which is connected to his or her computer, to connect to a telephone-line to dial into an ISP’s node. Once connected, he or she can then establish a modem-to-modem link with the remote server’s modem in the other location. This modem-to-modem link then allows for a secure connection through an authentication or authorization process involving LAN and operating system protocols.

VPNs, on the other hand, “ provide a more active form of security by either encrypting or encapsulating data for transmission through an unsecured network” (Cisco, n. d., para. 2) through the use of protocols installed on both the remote access client’s device, and the organization’s remote access server. So when using the VPN method, a VPN client would be able to use any IP network to create a virtual point-to-point connection with a remote access server at the other location (Microsoft, 2002). One way to look at it

would be that a VPN is an encrypted communications network tunneled through another network that is assigned to a specific network through protocols that are put into place.

Now, while even though both methods provide a secure connection over an unsecure network; the manner in that this security is reached is completely different. A VPN does not require explicit security features such as authentication or authorization; as with a dial-up remote access. Instead VPNs use a set of tunneling protocols to establish a secured tunneled network that is encrypted. Because of this, it has been decided that CphoeniX Inc. will implement a VPN to allow for private connections over the Internet to its network.

VPN Remote AccessNow as stated previously, the CphoeniX Inc. network will use a VPN to establish remote access to the network. However, a closer look at the VPN remote access it needed. VPN connections can be used in two different manners. The first is to use VPN technology to form WAN connections between two networks that have access to the Internet; this is known as a WAN VPN connection. As well, VPNs can be used to form remote access connections that enable remote access clients the ability to access an organization’s LAN via the Internet. The main difference between a WAN VPN connection and a VPN remote access connection is that a WAN VPN connects two networks together, rather than a remote client and a LAN. A remote access connection is usually formed when needed and uses less expensive hardware on the remote side (Hallberg, 2006), such as CphoeniX Inc.’s SDSL modem. The makeup of a VPN remote access connection consists

of the remote access client, the organization’s remote access server, and a shared or public network; which is typically the Internet.

However, the manner in which the VPN is established can be varied by the choices of hardware and software that will be used. As such, the following factors were considered when deciding on the remote access solution to be used:•Cost factors•Network hardware and connections•Performance factorsCost FactorsCost plays one of the most important roles in determining anything on a company’s network. As such, this is no different with the network remote access; and according to Hallberg (2006), “ VPN connections cost much less than dedicated connections” (p. 135). As well, the protocols that are used to establish the security offered by VPNs come standard on Windows based servers; which also make it more cost efficient than other options.

Network Hardware and ConnectionsAll CphoeniX Inc.’s offices use Windows 2000 and higher based operating systems (OS) on their servers and work station computers. So because of this, the use of the use of the VPN remote access is that much more appealing since all Windows 2000 and higher based OSs can be used to establish this remote connection through the use of various protocols.

Performance FactorsVPN remote access connections use authenticated links to ensure that only authorized clients are able to connect to the organization’s LAN. These authenticated links provided by VPNs will allow CphoeniX Inc. the ability to connect to its branch offices over a public

network while maintaining secure communications. As well, VPNs “ use encryption to ensure that data that travels over the Internet can’t be intercepted and used by others” (Microsoft, n. d., ¶ 4). However, this extra security is only available due to the remote access protocols (RAP) that are put in place.

Network ProtocolsAccording to Hallberg (2006), network protocols are “ rules that data communications over a network follow to complete various network transactions” (p. 92); and as stated previously, a VPN requires a set of tunneling protocols that allow a remote client computer to establish a secured connection with the organization’s remote access server. As such, the three most commonly used VPN tunneling protocols are: Point-to-Point Tunneling Protocol (PPTP); Layer Two Tunneling Protocol (L2TP); and Internet Protocol Security (IPSec) (Hallberg, 2006). However, according to Microsoft TechNet website, the L2TP and IPSec go hand-in-hand.

PPTP is a Microsoft designed protocol that is capable of handling IP, IPX, NetBEUI, and AppleTalk packets. According to the Microsoft TechNet webpage, the PTPP is an extension of the Point-to-Point Protocol (PPP). The PPP is a protocol that is responsible for utilizing point-to-point connections to transport multiprotocol datagrams. What the PTPP does is it encapsulates PPP frames into IP datagrams over an IP-based internetwork; whether it is an unsecured or secured network. To accomplish this, the PPTP utilizes the Microsoft Point-to-Point Encryption (MPPE) to encrypt the PPP frames with a 40-128 bit encryption. “ PPTP takes advantage of the underlying PPP

encryption and encapsulating a previously encrypted PPP frame” (Microsoft, 2002, ¶ 24).

Simply put, the PTPP “ leverages the authentication, compression, and encryption mechanisms of PPP. PPTP is automatically installed with the TCP/IP protocol” (Microsoft, 2002, ¶ 22), which makes it applicable to the CphoeniX Inc.’s network. The benefits of using PPTP is that PPTP offers compatibility with various clients, including older versions such asWindows95, Windows98, Windows NT 4. 0, Windows ME, and Windows 2000; as well as newer versions including Windows XP and Windows Vista (Microsoft, 2002).

The L2TP, as suggested by its name, operates at layer two of the OSI Model; at this layer, the protocol is capable of handling all layer three protocols. L2TP is a protocol that is an Internet Engineering Task Force (IETF) standard tunneling protocol. However, unlike the PPTP, which uses MPPE to encrypt PPP frames, the “ L2TP relies on IPSec for encryption services” (Microsoft, 2002, ¶ 26) to encrypt data with a 56-128 bit encryption (Microsoft, 2002). IPSec, unlike L2TP or PPTP, operates at layer three of the OSI model; and it is limited to handling specifically IP trafficking. However, according to PC Magazine (UK) (1998), IPSec is “ a lot less vulnerable to typical playback and spoofing attacks” (¶ 5).

This combination of the L2TP and the IPSec is known as “ L2TP/IPSec” (Microsoft, 2002, ¶ 26); and is generally the most secure. The way that the L2TP/IPSec works is by using the L2TP and IPSec both for encapsulation.

Once the PPP frame is encapsulated with the L2TP, it is then encapsulated again by an “ IPSec Encapsulating Security Payload (ESP) header and trailer, an IPSec Authentication trailer that provides message integrity and authentication, and a final IP header” (Microsoft, 2002, ¶ 28). Simply put, an encapsulated PPP frame, or “ L2TP message is encrypted with IPSec encryption mechanisms by using encryption keys generated from the IPSec authentication process” (Microsoft, 2002, ¶ 28). This higher security and standard implication on Windows 2000 sever based OS makes the L2TP/IPSec the right kind of VPN protocols that are needed to be used on CphoeniX Inc.’s network for remote access.

Network Business ApplicationsBusiness applications that are supported by the VPN remote access solution can be determined by the network administrator; however, some of the most commonly used applications include communication, inventory, database access, financial data, internet, and human resources. As well as these applications, this remote access solution is also capable of supporting Voice Over IP, client/server applications, and e-mail; which in turn make the use of the VPN solution that much more appealing to CphoeniX Inc.’s network.

The advantages and disadvantages of using such a remote access solution as the VPN are listed below.

AdvantagesThe advantages of a using the VPN remote access as a solution are:•The internet can be used to transport data•The cost of using a VPN is much cheaper than using a dedicated connection•There is no private

connection required between the client and the serverDisadvantagesThe disadvantages of using the VPN remote access for a solution are:•Performance can be impacted due to necessary data tunneling protocols•The client and server must both support the same tunneling protocols•Packets are transmitted over the internet, so there are security risks.

Backup and Disaster RecoveryA disaster recovery (DR) plan is a plan designed to explain " both the hardware and software required to run critical business applications and the associated processes to transition smoothly in the event of a natural or human−caused disaster"(Cisco, 2007, ¶ 1). As such, the following will discuss the backup strategies and elements that have been put into place for each of CphoeniX Inc.'s facilities if such an event were to take place.

BackupWith all five offices sending and saving data to the network constantly, data backups need to be done on a daily basis. Each of CphoeniX Inc.'s locations will have its own backup servers with a least a terabyte (TB) of capacity to save data specifically related to the facility it resides in; that get switched out when full. The purpose of this is to allow for easy access of lost data on site. Along with each facility backing up all data on a server located on the premises, each facility will make daily backups on the backup servers located at CphoeniX Inc.'s headquarters. This will allow for all material to be kept safe in case of a disaster at a specific facility. But to ensure the safety and access of the data in case of a disaster at

headquarters, an outside vendor will also be used to backup and develop better DR plans.

There are a variety of vendors out there that offer different strategies and solutions to backup and recover a company’s network data. Traditional DR solutions can be complex and costly; and hardly ever meet the criteria needed to protect the various applications being used on a company’s network. As well, when testing these different solutions, it can become quite tedious; and because of this, the documentations of the plan are hard to keep up-to-date. So after researching the different vendors out there, it has been decided to use VMware for a DR plan and data backup and recovery.

VMwareVMware vSphere allows the security administrator the ability to recover any data to any machine he or she desires; whether the machine is directly connected via cables, or the machine is hooked up via remote access. The way that VMware accomplishes this, is by allowing the user to virtualize the network’s production severs. Even if the user has not “ virtualized all production servers, virtualize target servers for your data recovery to allow greater simplicity, reliability, and cost savings” (VMware, 2009, ¶ 1). The key factors of the VMware disaster recovery strategies are to help networks: recover from disasters quickly; ensure reliable disaster recovery; reduce the cost of disaster recovery; and to automate disaster recovery.

To help recover from any disaster quickly, VMware uses 40 questions about the backup and recovery, high availability and disaster recovery setup and

plans that are in use. Then using the answers given, VMware's DR Assessment will suggest different ways to help improve the backup, recovery and availability of the network's critical applications (VMware, 2009). As well, VMware virtualization allows the administrator to store all hardware configuration, firmware, operating system install, and application installation data to be stored in just a few files on disk. Then by protecting these files using whatever backup or replication software the entire system becomes protected. " These files can then be recovered to any hardware without requiring any changes because virtual machines are hardware-independent" (VMware, 2009, ¶ 4).

To ensure the reliability of the DR plan, VMware suggests testing the system. Unlike traditional recovery plans, which are often difficult to test, difficult to keep up-to-date, and depend on exact execution of complex, manual processes. VMware's virtualized environment, testing becomes much simpler because the user is able to " execute non-disruptive tests using existing resources. Hardware independence eliminates the complexity of maintaining the recovery site by eliminating failures due to hardware differences" (VMware, 2009, ¶ 5).

With using VMware vSphere, the security administrator is able to provide a quick and reliable recovery without requiring identical hardware. With hardware independence, the administrator is capable of repurposing existing servers for DR, rather than needing to purchase duplicate servers " for rapid recovery. Server consolidation also lets you slash the cost of server

infrastructure needed both for production and disaster recovery” (VMware, 2009, ¶ 6).

The use of VMware’s virtualization allows the administrator to turn “ physical servers into data and recovery procedures into software” (VMware, 2009, ¶ 7); this then makes testing the DR plan to ensure the highest levels of reliability and availability of CphoeniX Inc.’s entire IT infrastructure that much easier. This then allows for rapid and cost-effective execution of the DR plans.

Along with backing up data, other elements have been put into place to prepare for disasters. Since most disasters cause some form of power outage of some kind, each computer that is connected to the network will have its own emergency battery pack. The battery pack will give the user of the computer the extra time they may need to save any unfinished work. As well, all servers, routers, modems, and other network hardware will also have their own emergency battery packs to allow the data time to be saved.

So with each facility using a daily backup procedure to on the ground servers, and the headquarters’ backup servers, all data can be easily retrieved in the event of a disaster. However, in the event of a disaster occurring at headquarters, all data will be able to be retrieved from the VMware server. As well, the service of offering DR plans specifically designed for CphoeniX Inc.’s needs make VMware that much more beneficial. In the end, the use of the VMware will allow for rapid and cost-effective execution of the decided upon DR plans.

For more information on how the VMware virtualization works, and benefits the network, please refer to the Using VMware® ESX Server System and VMware Virtual Infrastructure for Backup, Restoration, and Disaster Recovery (2005) manual; located at http://www. vmware. com/pdf/esx_backup_wp. pdf.

Network SecurityAlong with the threat of losing data in the event of a disaster, security threats are just as important to plan against. According to cgisecurity. com (2008), the top nine security threats are: malicious insiders, malware, exploited vulnerabilities, social engineering, careless employees, reduced budgets, remote workers, unstable third party providers, and downloaded software including open source & p2p files.

With threats such as these, CphoeniX Inc. has implemented the following network security elements. A fairly strong firewall; strong antivirus software and internet security software; all authentications need to use strong passwords that get changed on a bi-weekly basis; all wireless connections will use robust passwords to connect; there is physical security in place such as cameras; an optional network analyzer will be used to monitor the network; and CphoeniX Inc.’s security administrator will be in charge of monitoring the network for errors constantly.

To ensure the protection of CphoeniX Inc.’s WAN, and each office’s LANs, Fortinet® FortiGate® appliances will be used. According to Fortinet’s Solutions for Small to Medium Business (SMB/ROBO) (n. d.), “ Fortinet® FortiGate® appliances integrate all the essential security services needed to

protect a business in an affordable package, including antivirus, firewall, VPN, intrusion prevention, Web filtering, antispam, antispyware, and traffic shaping” (¶ 1).

References

A., Robert (December 29, 2008) Top 9 Network Security Threats in 2009. Retrieved October 17, 2009, from: http://www. cgisecurity. com/2008/12/top-9-network-security-threats-in-2009. htmlCisco Systems, Inc. (July 12, 2007.) Disaster Recovery: Best Practices White Paper. RetrievedOctober 17, 2009, from: http://www. cisco. com/warp/public/63/disrec. pdfCisco Systems, Inc. (July 12, 2007.) Disaster Recovery: Best Practices White Paper. RetrievedOctober 17,
2009, from: http://www. cisco. com/warp/public/63/disrec. pdfCisco Systems, Inc. (n. d.) Internetworking Technology Handbook. Retrieved September 05, 2009, from http://www. cisco. com/en/US/docs/internetworking/technology/handbook/ito_doc. htmlCisco Systems, Inc. (n. d.) Internetworking Technology Handbook. Retrieved September 19, 2009, from http://www. cisco. com/en/US/docs/internetworking/technology/handbook/Intro-to-WAN. htmlCisco Systems, Inc. (n. d.) Internetworking Technology Handbook. Retrieved September 25, 2009, fromhttp://www. cisco. com/en/US/docs/internetworking/technology/handbook/VPN. htmlFortinet (n. d.) Solutions for Small to Medium Business (SMB/ROBO). Retrieved October 17, 2009, from: http://www. fortinet. com/solutions/soho. htmlHallberg, B. (2005). Networking: A Beginner’s Guide. 4th ed. New York:

McGraw-Hill/OsborneHeaton, Warren (2000, August 16) What’s the best WAN connection type for you?. RetrievedSeptember 19, 2009, from TechRepublic: http://articles. techrepublic. com. com/5100-10878_11-5033247. htmlMicrosoft Corporation (2002, March 16) Microsoft Remote Access Introduction and Overview.

Retrieved September 25, 2009, from Microsoft TechNet: http://technet. microsoft. com/en-us/library/bb742490. aspxMicrosoft Corporation (2002, June 16) Administrator’s Guide to Microsoft L2TP/IPSec VPNClient. Retrieved October 03, 2009, from Microsoft TechNet: http://technet. microsoft. com/en-us/library/bb742553. aspxMicrosoft Corporation (2003, March 16) Dial-up Remote Access Technical Reference.

Retrieved October 03, 2009, from Microsoft TechNet: http://technet. microsoft. com/en-us/library/cc780183%28WS. 10%29. aspxMicrosoft Corporation (2006, October 30) How to Install and Configure a Virtual PrivateNetwork Server in Windows 2000. Retrieved September 25, 2009, from Microsoft Helpand Support: http://support. microsoft. com/kb/308208″New standards for remote access.” PC Magazine (UK) (Oct 1998): 227(1). GeneralOneFile. Gale. Apollo Library-Univ of Phoenix. Retrieved October 03, 2009, fromhttp://find. galegroup. com/itx/start. do? prodId= ITOFTechTarget.