FACTORS INFLUENCING USE OF VIRTUAL PRIVATE NETWORKS OVER TRADITIONAL WIDE AREA NETWORKS BY DECISION-MAKING TECHNOLOGY MANAGERS

by

Danielle L. Babb

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

March 2004

© Danielle Babb, 2004

FACTORS INFLUENCING USE OF VIRTUAL PRIVATE NETWORKS OVER TRADITIONAL WIDE AREA NETWORKS BY DECISION-MAKING TECHNOLOGY MANAGERS

by

Danielle L. Babb

has been approved

March 2004

APPROVED:

JIM MIRABELLA, D.B.A.., Faculty Mentor and Chair

JOHN HANNON, D.B.A., Committee Member

NORBERTO CRUZ, Ed.D., Committee Member

EDWARD SUJDAK, D.B.A., Committee Member

BARBARA-LEIGH TONELLI, Committee Member

ACCEPTED AND SIGNED:

_____

JIM MIRABELLA, D.B.A

_____

Shelley R. Robbins, Ph.D.
Executive Director, School of Business

Abstract

The research presented in this dissertation offers an understanding of the reasons technology managers choose to recommend or not recommend particular technologies, specifically Virtual Private Networks, to their organizations. The impact of perception related to security, reliability, cost savings and need are evaluated to understand the impact they have on decision-making. The study is based on a survey to a population of Information Technology professionals with the results showing clearly that all four issues correlate with a recommendation to recommend or not recommend the technology. The research clearly shows that security, reliability and cost-benefit are reasons technology professionals choose a solution and these topics will continue to be of utmost importance to executives, managers and vendors of equipment.

Dedication

This dissertation is dedicated to Dr. Glen Blix. While he isn't here to see the real impact he has had on my life, he has had a deep influence in the choices I have made, the education I choose to have, and the person I strive to be. I deeply respect and admire his pursuit of truth and knowledge, and his relationships with friends, colleagues and loved ones. He was a friend and a teacher, a cornerstone in my decision to pursue my dream. The ways in which he blessed others with his love will never be forgotten.

I would like to thank my loving and supportive family for their encouragement and support of my ongoing academic pursuits. Their goal-focused advice and love has helped through the most trying of times.

I would also like to thank my grandfather, who supported my bachelors and masters work and encouraged me to continue until I reached this goal.

I would like to thank my dear friend Arlene Blix for her undivided support, love and encouragement to see this through despite her own struggles.

I would like to thank Mike Hinchee for his words of encouragement, celebration of milestones, and reminding me that each little step was a success not to be forgotten.

Finally, my thanks and sincere appreciation to Dr. Jim Mirabella, the finest teacher and mentor I could have asked for. While having never met face-to-face through most of the doctoral process, Dr. Mirabella provided tremendous encouragement, strategic thinking, goal focus, and sincere friendship throughout my program. He redefines mentor, and I am truly fortunate to have developed a lifelong friend and colleague. My hope is that one-day I will be able to honor him by giving back to another the level of friendship, trustworthiness and guidance he gave to me.

Acknowledgements

I would like to acknowledge the effort and advice provided by my committee members: Dr. John Hannon, Dr. Norberto Cruz, Dr. Edward Sujdak, and Ms. Barbara-Leigh Tonelli.

Dr. Hannon has provided insight into additional areas for study and issues for concern throughout the doctoral process.

Dr. Cruz has provided his thoughts and comments on the research.

Dr. Sujdak provided tremendously valuable comments and insight into areas of study and scholarly writing.

Ms. Tonelli has provided support as a friend and has been a fantastic writing editor. I am grateful to all of you.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Introduction to the Problem

As wide area networks become increasingly common to connect disparate offices or remote users to corporate networks, many companies are relying on the use of Virtual Private Networks (VPNs) to establish these connections. The popularity of this technology has led to concerns with regard to security and reliability, often leaving the recommendation and purchase of such a system to the Technology Manger or Director responsible for the department implementing network infrastructure. Trade magazines often differ in their survey of managers and their perceptions of Virtual Private Networks, leaving little in the way of data to aid management in making a solid technology choice for their organization.

Background of the Study

Wide Area Networks in their traditional sense are often costly because Internet Service Providers charge for both distance and bandwidth; making organizations with sites far away or with many sites spend a lot of money for data communications costs. With traditional Wide Area Networks, remote users are often connected with dialup modems that open security holes and cause speed issues, or with Remote Access Services that can be difficult to configure, offer numerous security holes, and require a high degree of technical support.

Virtual Private Networks have changed the way companies can offer Wide Area Networking services. Virtual Private Networks create virtually private tunnels over public communication channels; primarily the Internet. These networks can also be configured to run over dedicated frame relay or point-to-point connections, though the study will focus specifically

on use of Virtual Private Networks over the Internet. This type of network offers stable, simple and fast ways for remote users to connect to the core network and offer companies an opportunity to save significant communications dollars while maintaining connectivity standards.

Virtual Private Networks inherently come with their own risks. When they use public lines, they require different types of security than dedicated lines do. Virtual Private Networks inherently open up security holes that would not otherwise be an issue on corporate networks . Virtual Private Networks have changed the way many businesses configure and connect their backbones with hopes of offering a competitive advantage and minimizing security risks.

Statement of the Problem

Often, managers and executives are left guessing what technology will be used in the future and whether or not professionals consider a communications method secure and reliable. This leads to poor decision making and costly mistakes. This study focuses on the factors that influence managers to recommend Virtual Private Networks over traditional Wide Area Networks. The study gauges the level of security concern Information Technology Managers have regarding the use of Virtual Private Networks, and the reasons that they ultimately recommend or do not recommend to use them. There is literature currently available on the use of Virtual Private Networks technically; how they are configured, secured and provisioned. There are also case studies available discussing the ways in which organizations use these networks to provide competitive advantages. Both are reviewed during the literature review. The researcher has conducted primary research to determine factors that influence a manager's decision to use Virtual Private Networks in their organizations.

Purpose of the Study

The purpose of the study is to identify particular management perceptions on the use of Virtual Private Networks to enable managers to make better decisions. In particular, it will help them determine whether the technology is becoming widely adopted and if security and reliability aspects of the system are generally acceptable to technology management professionals.

Rationale

Determining whether technology is appropriate is often a guessing game, based on word of mouth, vendor and consultant recommendations, and trade magazine reviews. This study will help executives and managers make better-informed decisions by evaluating the criteria listed in the hypothesis section in relation to Virtual Private Networks to help gauge technology managements perceptions of the technology. Perception often makes or breaks a technology and can provide real-life clues into the usefulness of a new method or device.

Hypotheses

Hypothesis 1: An information technology manager's decision to recommend Virtual Private Networks is independent of his/her perception of its security.

Hypothesis 2: An information technology manager's decision to recommend Virtual Private Networks is independent of his/her desire to save money in communications costs.

Hypothesis 3: An information technology manager's decision to recommend Virtual Private Networks is independent of his/her perceived need for wide area networking.

Hypothesis 4: An information technology manager's decision to recommend Virtual Private Networks is independent of his/her perception of its reliability.

Significance of the Study

This study will significantly contribute to the data in the field of Information Technology and Networking. It will help determine business reasons managers may recommend this particular remote access technology, and whether or not they are concerned about security. It will help to present ideas to understand why managers may recommend one technology over another and will offer other organizations considering the use of Virtual Private Networks some areas for consideration. In the future, business and technology managers will be interested in this data when contemplating the choice to move to Virtual Private Network technologies. It will create new knowledge in the field of Information Technology and bring into view the perceptions of professionals.

Definition of Terms

Definitions are from whatis.com, an online technical resource.

> *Encryption* – "Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.". (http://www.whatis.com)

> *Local Area Network* – "A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building) Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network)." (WhatIs Definition, 2003)

> *Virtual Private Network* – "A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.". (WhatIs Definition, 2003)

> *Wide Area Network* – "A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication

> structure from a local area network (LAN) A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks.". (WhatIs Definition, 2003)

Assumptions and Limitations

The survey is limited specifically to technology professionals in a management role. Management role will be defined by the individual's title in the organization. The study is limited only to Virtual Private Networks as a means of remote access and does not include traditional Wide Area Networks, except to draw comparisons and contrast responses in the survey. It is assumed that the sample of Southern California IT managers is representative of IT Managers as a population regarding their concerns over wide area networking. The research assumes the respondents answered honestly because there is no fear of reprisal and all answers will be kept confidential with e-mail addresses deleted. The survey asks for no specific project failure information, further increasing the opportunity for honest answers. The researcher has assumed that every organization will have had a need at one point for wide area networking for either remote users or branches.

Nature of the Study

The study will be conducted using a quantitative methodology, surveying Information Technology professional managers or executives.

CHAPTER 2. LITERATURE REVIEW

Introduction

The literature review provides a comprehensive framework for understanding the criticalness of studying Virtual Private Networks and their use in industry. The section begins by exploring computer networks and the use of Wide and Local area networking in business. It moves through the types of Wide Area Networks (WANs) used, and the costs, risks and benefits of the technology. The review moves through the efforts of cost reduction and business enhancement, as well as common issues associated with any wide area network, including quality of service, line issues, compression, risks, remote offices and downtime. An example of how a WAN can be used to boost competitive advantage will be given, as well as a comparison of WAN technology to Virtual Private Network technology. The effort moves forward through the types of VPNs available, issues for consideration including performance, security, reliability, quality of service and service level agreements, and will take into consideration common business issues such as convergence and the management and organizational implications of VPN technology. The literature review concludes with a summary of the benefits of VPNs and expected business changes as a result of using the technology.

The literature review is designed to provide an understanding of the importance of these complicated networks in today's business, and reinforce the need for further study based on the assumptions and risks made in implementation.

Computer Networks

Computer networks are defined as a "series of points or nodes interconnected by communication paths." (WhatIs Definition, 2003). Networks can connect other networks together or contain sub-networks within themselves. Networks are commonplace in businesses and allow transactions or communications to take place among computer users (Search Domino Definitions, 2003).

Networks in general provide a way for users to share files that is faster and more convenient than carrying around diskettes or CDs. Networks provide electronic mail capability and allow users to share printers with others. They also keep employees from having to go to a different computer where information is stored to look up information, using client-server applications to retrieve that information. Networks provide much more streamlined backup scenarios instead of having to back up each individual PC because data is stored in a central location (Jungle Software, 2003)

Local and Wide Area Networks

Computer networks can be divided into two main categories: Local Area Network (LAN) and Wide Area Network (WAN). Other types of networks can be established as well though they are less common, such as metropolitan area networks (MANs) and global area networks (GANs). LANs are the least complicated and are contained to one location. A LAN is a group of computers and devices that share common communications lines and share the resources on the same network. A LAN can serve as few as two users or as many as thousands. Generally speaking, it is easy to think of a LAN as the entire network or set of communications within a

single building. Technically speaking, a local area network is a network contained within a router, a network that is local and contained within a given subnet. A LAN is not needed to obtain access to the Internet or other computers on a different network. LANs are often used to share databases, files and printers in an organization (Johnson, 2003)

Technical Definitions – Local Area Network

A local area network is a network contained within a router; a network that is local and contained within a given subnet. A local area network, or LAN, is not needed to obtain access to the Internet or other computers on a different network. LANs are often used to share databases, files and printers in an organization (Spohn, 2002)

There are several ways that a LAN can be configured, or topologies that can be used. There are three main types of network topologies. They are the bus topology, the ring topology and the star topology. The bus topology connects all devices through a bus, or backbone. They are relatively inexpensive and fairly easy to install (WebOpedia, 2003)

The ring topology connects all devices through a closed loop in which each device is directly connected to two other devices, one on either side of it. They are fairly expensive and difficult to install. They offered high bandwidth capabilities in the early 1990s when compared to many of the bus or star topologies. They have the disadvantage of taking down an entire network when one node has an issue because of the way they are physically connected (WebOpedia, 2003)

The star topology connects all devices to a central hub. Hub is used in this sense not necessarily literally, as switches have taken the place of traditional “hubs”. Still this is a concentric model in which a hub location is used to connect multiple devices. They are relatively

easy to install and manage, but bottlenecks can occur where data converges. This is the most popular and common type of network used today. One additional advantage is that a single individual PC or node does not affect the entire network in the event of a workstation or PC outage. The network maintains its reliability as long as the infrastructure it is built on remains stable (Green, 2001)

Technical Definitions – Wide Area Network

A Wide Area Network, or WAN, provides the means to interconnect several corporate offices over disparate geographic regions allowing data to be shared seamlessly between all sites. (www.whatis.com). This is a key enabling technology for today's expanding business markets, allowing all personnel to interact in a cost-effective way while providing optimal collaboration and data consistency.

A network becomes wide-area when it connects geographically dispersed networks. A WAN may be privately owned or rented. Meyer (1998) said that a WAN is a computer network that directly connects computers separated by long distances--more than a mile and as much as half the globe. WANs require special media, which are provided by telephone companies and other firms that specialize in this service. WANs also require special hardware (p. 102). In the traditional Wide Area Networking model, the corporate enterprise, made up of a central data site and several smaller remote sites, employ dedicated "leased lines" between each remote site and the central site. Multiple LANs can be connected together using devices such as bridges, routers or gateways that enable them to share data. A WAN is two or more LANs connected together. A leased line is a point-to-point line with a beginning and an end; both networks trusted by each other. This provides a highly secure network but often is more expensive than lines to the

Internet. Leased line technology, such as T1 and Frame Relay, is used to create a long distance extension of the internal network wiring. There is one leased line for each remote site and a CSU/DSU "modem" on each end of the connection. These connections are point-to-point, data can only be sent to the host or remote site (Johnson, 2003)

WAN Growth

Organizations are seeing the benefit of Wide Area Networks. Growths of WANs and Internet Access have been predicted to grow from an $88 billion business in 2003 to $109 billion in 2007 (Business Communications Review, 2003). This growth represents a 24 percent increase and is based on an interview of 240 network managers in all size organizations. The growth is driven by increased WAN use for existing users and the addition of new applications, such as multimedia and Enterprise Resource Planning applications (ERPs), global applications that often manage all resources in an organization. These applications can consume significant bandwidth on a network (Business Communications Review, 2003). Leased lines and frame relay lines still account for 94 percent of carriers' Internet service revenues.

WAN Links

A service provider, typically a long-distance telecommunications company such as AT&T, provides the link between the sites. The leased line charges are based on speed and distance. If two buildings are relatively close to one another, within a few miles for example, then the total monthly fee is very low. However, when WANs cross multiple states or countries, charges quickly add up.

Wide Area Networks generally cover a wide area; as such they usually transmit data over high-speed connections or wireless connections (WhatIs Definition, 2003). One basic WAN use

is a central office or data center with multiple sites connecting to it, as is seen most often in organizations with more than one office. WANs may or may not include remote users, regional offices, corporate offices, and so forth. "A Wide Area Network (WAN) is a group of computers or Local Area Networks (LANs), not in the same geographical location, which are connected together via a connection medium such as telephone wire." (Digitus-Associates, 2003). Digitus-Associates provides the following example: "if you have a computer in New York City which communicates directly and in real time with a computer in your office in Hong Kong, it is on a WAN." (Digitus-Associates, 2003). Table 1 depicts some of the major differences been local and wide area networks.

In the past, the telecommunications industry has used dedicated private links to build a Wide Area Network. In the traditional Wide Area Networking model, the corporate enterprise, made up of a central data site and several smaller remote sites, employ dedicated "leased lines" between each remote site and the central site (Cisco, 2003). A leased line is a point-to-point line with a beginning and an end; both networks trusted by each other. This provides a highly secure network but often is more expensive than lines to the Internet. Leased line technology, such as T1 and Frame Relay, are used to create a long distance extension of the internal network wiring, creating a WAN (Gray, 2003). These connections are point-to-point, data can only be sent to the host or remote site. A service provider, typically a long-distance phone company such as AT&T, provides the link between the sites. The leased line charges are based on speed and distance. If a company has two buildings relatively close to one another, within a few miles for example, then the total monthly fee is very low. However, in the event that the remote sites span states or even countries, this monthly fee for the mileage can become cost-prohibitive quickly. See the

traditional WAN diagram labeled Figure 1. There are two factors involved in lease line billing: mileage (distance) and bandwidth. The more distant and the more bandwidth available, the more expensive the line is. For instance, a 384kbps line from the East Coast to the West Coast will be more costly than a 384k line within the same region (Phifer, 2002)

Table 1

Local and Wide Area Network Comparison

	Local Area Networks (LANs)	Wide Area Networks (WANs)
Most Common:	Ethernet, Token Ring, FDDI	Leased lines, serial links, ISDN, X.25
Advantage:	Speed	Distance
Cost Center:	Dense installation (about one interface per room)	Length of long-haul lines (about one interface per 100 miles)
Current Speed:	10-100 Mbps (mostly 10 Mbps).	To 45 Mbps (mostly clustered around 1 Mbps)
Common Uses:	File sharing	E-mail and file transfer (including Web)
Common Problems:	Cable disruption by users	Cable disruption by backhoes
Conceptually:	A bunch of lines hooking users together	A bunch of lines hooking cities together

WANs and the Internet

WANs have been especially useful in the modernization of the Internet and various WAN service offerings have come mainstream as corporate provide services via the web. The Freesoft (2003) site states:

> The Internet can be thought of as a bunch of LANs interconnected by WANs. An average packet will run across a company's local Ethernet (LAN), up an ISDN or leased line or PPP link (WAN) to an Internet Service Provider. The ISP has Ethernet too (LAN), that transports the packet to the right router for delivery to a cross-country provider (WAN). The packet begins bouncing from one LAN site to another over WAN links.

WAN Benefits and Use

WANs allow organizations to connect multiple sites to a single location, share data, provide electronic mail and web access, share files, printers and communicate freely. WANs allow multiple servers to access a single database, allowing for data mining and queries. WANs help maintain consistency, keeping data in a central location for reporting, financials, economies of scale advantages, and to avoid duplication of efforts. WAN usage has been expanded to include partners, vendors, and other third-party organizations securely and rapidly (Digitus-Associates, 2003)

Electronic Data Interchange

Organizations also use WANs to take advantage of Electronic Data Interchange (EDI), noted as one of the biggest value creation processes networks currently offer (Kalanidhi, 2001). Businesses create value by "converting resources through a series of processes into goods or services" (Kalanidhi, 2001). The use of WANs helps organizations accept data from numerous locations and create useful information, thus contributing to the value chain. This technology has helped to ensure compatibility despite using different systems that are generally not able to communicate with one another. EDI is a procedure that allows companies to exchange documents, such as invoices or purchase orders, by establishing a procedure within both systems for import and export of data (Kalanidhi, 2001). This is commonly seen in manufacturing organizations. "If two companies have compatible systems, they can establish a connection through which company A sends a purchase order to company B by means of EDI--computer to computer. When company B ships the product, company B sends an invoice by EDI to company A. Company A can then pay by electronic funds transfer through its bank. The entire operation

occurs without any paper changing hands." (Meyer, 1998). Intermediary EDI organizations are used to modify incompatible code to make communication possible. This also occurs via the WAN. EDI can substantially reduce a company's costs and generally requires WAN connectivity to exist (Meyer, 1998).

Voice over Internet Protocol

Another area that is being discovered by many financial executives is the benefits of Voice over Internet Protocol (VoIP), which requires WAN connectivity of some sort to work. VoIP is using existing data lines to transmit telephone calls. While the technology is still quite "buggy", it is becoming a bit more mainstream and most major router manufacturers are now supporting this technology. The potential savings in long distance costs between branch offices and vendors/suppliers if they are on the network could be substantial. This, however, will require additional bandwidth or bandwidth segmentation (Cisco, 2003)

Enterprise Resource Planning Applications

Organizations are also using Wide Area Networks to connect all users on a single enterprise resource planning application (ERP). Whatis.com defines an ERP as "a multi-module application software that helps a manufacturer or other business manage the important parts of its business, including product planning, parts purchasing, maintaining inventories, interacting with suppliers, providing customer service, and tracking orders. ERPs can also include application modules for the finance and human resources aspects of a business." ERPs are expanding to support additional functional areas and are providing significant value to businesses wishing to integrate their functions and see management and executive reports that allow them to properly plan their business. Two of the most expensive and expansive Enterprise Resource Planning

applications are SAP and Peoplesoft/JD Edwards, often used live over WANs. As organizations invest in the integration of their data, they need users and functional areas to be using the same system. This is possible even in disparate locations by use of a WAN (Resnick, 1996)

Intranet

The implementation of WAN infrastructure has helped enable Intranet technology. An intranet is usually web-based and is a set of web pages that is internal based on some criteria, such as being an employee or being in a building on the local network. Intranets have come full swing, allowing users to request help from their Information Technology department, submit Human Resources forms, get company information and phone numbers, and find out what is happening around the organization. It has become a type of portal in many companies, even supporting links to major applications to keep users from having to remember many different icons on their desktops (Microsoft, 2002). Without the use of Wide Area Networking, this would not be possible because users in different buildings would not have access to the same network. Through the use of WAN hardware, users can be on the same network while existing in entirely different countries (Jackson, 1998).

WAN Costs

As with any technology, there are costs associated with Wide Area Networking. It is critical to note that WANs use some type of dedicated line, which is generally quite expensive and is a repeated, often variable cost. This can be a frame relay line, Virtual Private Network, point-to-point connection or another service. Users generally pay on the basis of distance and bandwidth. For instance, the further apart two locations are, generally speaking, the more expensive the line costs will be. Similarly, the more bandwidth that is requested the more

expensive the line charges will be. As the network grows, companies may find themselves facing increasingly heavy line usage charges. This has been a continued issue as applications require more and more bandwidth, and more parts of businesses are integrated requiring applications on most users' desktops (Johnson, 2003).

Data Center Consolidations

Data Center consolidations are also leading to additional bandwidth requirements, hence increasing the costs of WANs. Due to the cost of hardware and desire to increase the speed of application access, many companies are centralizing their data centers. This is requiring many users who used to share files on a local server to connect back to a data center just to save files, using WAN bandwidth and requiring a connection (Johnson, 2003). "For example, server consolidation typically results in relocating a server from across the LAN to across the WAN. That means traffic that used to be local (high-bandwidth, low-latency/delays and virtually free) is now long-distance (low-bandwidth, high-latency/delays and expensive)." (Johnson, 2003). Latency refers to the time it takes for a packet to get from the sender to the recipient (WhatIs Definitions, 2003). Users often see decreased performance and executives' higher costs as a result of these consolidation efforts.

Installation Costs

In addition to the monthly recurring costs that will continue to increase as additional bandwidth is needed and new users are added, there is the hardware cost for WANs. Installing a WAN is not an inexpensive endeavor; routers can be quite costly and require particular expertise to install and make secure. This generally requires consulting or specialists in the area, adding to the installation costs. It is critical to configure it right the first time, and many network

administrators choose to use subject matter experts to do this. The level of redundancy and failover the organization wants will dictate the cost tremendously. A highly redundant system requiring removal of single points of failure will cost significantly more than a network that "just works" but may be inaccessible in the event of equipment failure (Cisco, 2003)

Ongoing Maintenance

Ongoing maintenance is another element of the cost. While routers are generally the most stable pieces of infrastructure on the network, they require maintenance to keep updated and protect against failure. Maintenance includes service packs or patches, Operating System updates and at times physical maintenance, such as checking power sources or cleaning the equipment. This cost needs to be considered when evaluating the overall WAN costs.

Cost Reduction

There are many ways to help reduce the overall cost of a WAN. During the design and implementation stage, it is crucial to properly plan and to document requirements. WAN design requires understanding what the application overhead will be (how much traffic an application generates) and therefore the appropriate minimum amount of bandwidth required on the WAN. The design phase should analyze user requirements and document them, taking typical user needs into the overall equation. It is important not to purchase too much or too little bandwidth. Too much bandwidth will lead to costs that are difficult to justify; too little bandwidth will slow down the network and wreak havoc on applications, backup processes, maintenance and user frustration. Flexibility and scalability are key elements; purchasing WAN equipment and telecommunications lines that can be expanded as needed may be an important component of a businesses' choice (Johnson, 2003)

Network Consolidation

Another way to help reduce costs is to consolidate multiple networks. “Companies often have dedicated networks for particular traffic types (voice, video, extranets or legacy applications). One firm we worked with had more than 30 networks, including dedicated extranets, an X.25 network that handled one legacy application, and multiple voice and data nets.” (Johnson, 2003). Integrating these applications where feasible will create a common infrastructure, and cost savings are cumulative. For instance, installing VoIP may not amount to much savings alone, but if video and conference calling are included, the benefits may change substantially.

Service Level Agreements

Service Level Agreements (SLAs) play a critical role to reducing the costs of WAN-related outages. An SLA will guarantee a level of service by a provider for a given cost, and will specify the reimbursement the provider will offer in the event of downtime. This reimbursement is assumed to help reduce the costs of the impact of the downtime or degradation. Companies must hold providers accountable for their guaranteed uptime and their mean time between failures, as well as their average time to repair a problem (Infonetics, 1998).

Quality of Service

Another suggestion noted by Johnson is to use Quality of Service (QoS) and selective “oversubscription” to gain additional performance out of existing lines. On dedicated lines and with most Virtual Private Networking technologies, including frame relay, the bandwidth is already paid for as most organizations have Internet connections to connect their users to e-mail and the World Wide Web. By deploying QoS at access points, the transfer of mission-critical

applications even when the WAN is congested will be close to guaranteed (Johnson, 2003). Bulk file transfers or less critical tasks are then saved for slower times on the network.

Compression

Compression is another way to save on some costs. Compression is a way of squashing down data into smaller pieces before transmitting, and then decompressing or "unsquashing" at the recipient's side. There are numerous tools that claim up to five times faster access (Johnson, 2003)

Line Negotiations

Companies can also renegotiate their line rates. For some time, rates dropped 25 to 30 percent and companies saw a decrease in costs. While this big decline appears to be over, most providers will make changes or modify agreements if it means maintaining the business.

WAN Risks

The use of WANs poses inherent risks to businesses. With some types of connectivity, the communications link is not flexible. Upgrading to a higher level of bandwidth in these cases is a big ordeal, and can be quite costly or require a complete reconfiguration of the network. Companies should choose to avoid these expensive issues (Johnson, 2003). Companies that expect growth, a change in the applications their network supports, or an increased use by existing users should be certain that the network is scalable, or flexible to growing or changing needs.

Remote User Support

Supporting remote users can also be quite costly. Remote users generally require a higher level of support, more costly technical support phone calls, and have more difficulty with their

technology than LAN users. Equipment that they are using remotely has more moving parts, and can often complicate the process of connecting to the network (Findvpn, 2003). In some cases, remote users require dedicated Internet connectivity lines such as cable or DSL, which if locations are numerous, can increase costs significantly.

WANs and Downtime

As the business comes to rely on the integration and collaboration that the Wide Area Network has enabled, the cost of downtime increases. While there are technical ways to help reduce the opportunity for downtime, there is no such thing as 100% fault tolerance. Often companies will require redundant lines to key locations, further adding to their costs. It is important to perform a business continuity analysis that will help determine the appropriate level of risk based on costs and the cost for redundant equipment or lines to help determine the "fine line" that is right for each company. Adding redundant equipment and redundant lines means additional complexity, additional cost and more maintenance. However, the costs of experiencing downtime may be enormous to the business, especially in companies where the operations of the business rely on the technology. The average organization has 1.7 "hard" downtime outages per month, with the average duration lasting about 67 minutes (Infonetics, 1998). Service Providers are the primary cause of downtime, with router failure second (Infonetics, 1998).

Service degradations are another type of downtime; they are costly and often difficult to troubleshoot. Service degradation means a loss in performance for a given technical reason. Degradations can have an impact on response times, latency, proper file locking to reduce problems with records in databases, and response-time related employee performance issues.

(Infonetics, 1998). Companies experience approximately 4.4 degradations per month lasting on average 47 minutes per instance. Degradations are most often caused by overuse of the network. Hardware problems and service provider downtime, respectively, rank second and third.

Infonetics Research has created a formula and studied the effects of WAN downtime on businesses. The formula takes into account the total hours per year of hard downtime and service degradations. It factors in the total number of employees affected by these service issues, the average percent of employees connected to the network, and average percent of employees affected by each outage or degradation occurrence. Finally, it takes into account the weight average hourly wage per employee. The table below provides a summary of downtime and degradation costs:

Table 2

Downtime and Costs

Type of Issue	Productivity Loss	Downtime Hours Per Year	Average Hourly Wage	Loss in Dollars
Downtime	80%	23	$67.40	$2,178,000
Downtime	60%	23	$67.40	$1,634,000
Downtime	40%	23	$67.40	$1,089,000
Degradation	20%		$67.40	$932,000
Degradation	10%		$67.40	$466,000

These numbers do not take into consideration revenue loss, which is expected to be about three times greater for each scenario than the lost productivity cost (Infonetics, 1998)

Organizations can implement tools to help monitor downtime and to charge back their providers. They can also use these tools to proactively spot issues and attempt to resolve them before they become widespread outages (Jackson, 1998). Remote management services or outsourcing the WAN management piece of infrastructure may help to reduce costs and note

issues before they take hold of the network. Jackson notes, "Ignoring a WAN that is functioning properly may save management time and money in the short term, but over time it will cost in terms of service quality and expenses." (Jackson, 1998) For example, a carrier may tell a customer whose WAN is congested to add more bandwidth by leasing more lines-at high cost. "If the customer monitored traffic, they could optimize the WAN by requiring users to transmit only mission-critical data at peak times." (Jackson, 1998)

WAN Use Example

The opportunity to discuss the use of a WAN and the benefits and costs associated with it are plentiful. The researcher chooses to focus on the use of a WAN in a homebuilder that had a substantial impact on their profit and business processes despite not being a technology-centric organization. The researcher gives a background of the organization, explains the structure at the company, and offers ways in which a WAN helped improve efficiencies.

The company has seen tremendous growth in employees, profit and market share over the past 30 years (Reuters Financials, 2002). This is known and regarded highly within the organization as the employees look to this growth for future job potential. The company concentrates on quality rather than quantity, building in the higher end markets with home prices often in the custom home range of over $1 million. The core values of the organization include commitment to a quality product, creating pride of ownership, quality and commitment to the buyer.

The organization's corporate office is in Irvine, California. The organizational structure of the company utilizes divisions, with each region being allowed complete autonomy and ultimate decision making over the strategy and implementation of the product it builds. This is

noted in meetings and in the business tact used when working with new divisions. Each division is organized centrally, has a local controller, and sometimes a human resources department and regional president. In addition, each division also has their own set of construction personnel. In an organization with about 1200 employees, only about 100 are at the corporate office. Others are working in their respective divisions.

The company operates within a decentralized structure. According to the business plan, the divisions are allowed autonomy to run their business units and to operate their regions the way they see fit because this is in the best interest of local growth. The organization fits the definition of a decentralized structure as defined previously. Synergy and cohesiveness within a division are strong; however communication with the corporate office often falls short in some departments. For example, the divisions do their own team building; do not attend formal meetings frequently with other experts in different divisions, and are focused on the success of their respective region. Within the organization, the Information Technology group also operates in a similar manner.

The autonomy afforded the divisions has been a major selling point in the acquisition process. In all three recent cases of acquisitions on the East Coast, the division presidents or owners went to the recently acquired other offices to ask if, in fact, the divisions were truly allowed to operate on their own. This has been a make-or-break factor in every acquisition to date. There is a strong perception that the divisions are very protective of what they perceive as their turf and their areas of control, especially when new to the company.

The organization has seen most of its growth through an acquisition strategy. The company has nearly doubled in size in the last twelve months by acquisition and by responding

to increasing demand in the regions it builds in (http://finance.yahoo.comThe growth through acquisition strategy is not unique to the homebuilding sector, although the rate of growth has been phenomenal in this organization.

This structure and promise of autonomy by the executive team has created rather a unique challenge for the company. Human resources, accounting/finance efforts, and the technology department are key areas for the company. Attempts at centralization or standardization have been fraught with difficulty, both politically and practically, in some regions for some functional areas since each division is allowed full autonomy. Varied products and markets on the construction side of the business are conducive to autonomous operation, however centralization may be more effective to control costs and provide equitable opportunities for all employees. The Human Resources Department has been challenged by the need to centralize payroll and benefits, which may result in the individual divisions giving up their existing benefit plans and pay schedules for the corporate standard. Each division is given the opportunity to set regional-specific pay scales, causing interdepartmental issues throughout the organization. They are migrating to company standard benefits, which are also causing concern in the new divisions. The relationship between corporate and some of the divisions is sometimes strained due to these disparities and the changes required. Several cases can be cited involving such discrepancies and a difficulty creating organizational change in the new regions.

The technology department at the company has been greatly impacted by the growth of the company. The technology department is organized into three functional areas: JD Edwards, Application Development, and Network/Client Services. Each functional area operates autonomously with some central strategic planning as oversight.

The company employed the use of Wide Area Networking to solve many of its challenges. The disparate regions disconnected from the centralized corporate structure allowed for the divisions to run on any ERP application that they were using in the past, and required exports of financial data monthly into Excel spreadsheets that were then uploaded back into the corporate financial package. This led to discrepancies, a significant waste of time, and an inefficient process. Using a Wide Area Network, the division users were able to get right into the corporate system and report their information directly. The WAN has also allowed the divisions to all standardize on one ERP package despite having autonomous control over how their division is managed.

The WAN has allowed off-site, remote users in the construction offices to connect to the corporate backbone. This allowed them e-mail capability, and put them on the corporate Intranet with access to Human Resources data, company news and phone lists. It increased communications to the employees actually building houses. It also allowed the construction managers to interface directly with the subcontractors or e-mail pictures of issues with homes that needed management resolve. This saved considerable time and effort on the part of the employees and management.

Central reporting of progress and the ability to share files amongst employees was a huge benefit to all areas of the company. Divisions were able to collaborate and gain ideas or suggestions from others. They were able to see what product other divisions were creating and how that could change their own product. They were also suddenly capable of sharing files between functional departments within their own division, greatly improving communication.

The WAN increased communication, collaboration, and saved the company money in productivity gains. Many divisions were able to limit the hiring of new employees because they were able to take advantage of the gains technology afforded them. The organization found the right balance between redundancy and costs, and was able to maximize the use of their network while keeping costs as low as possible.

Virtual Private Networking

With technology and business requirements changing at a rapid pace and the continued need for financial savings, many Information Technology departments are being asked to explore alternatives to traditional connectivity as a method of reducing their operating costs. This question is designed to explore the advantages and disadvantages to using Virtual Private Networks to gain outside access securely into a private network in an effort to reduce costs and increase performance. Several network concepts will be explored and data provided to lead to a conclusion on the efficiencies of this technology. A Virtual Private Network is also described as a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network... The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost. (SearchNetworking Definitions, 2003)

Virtual Private Networks and WANs Compared

With the expansiveness and low cost associated with the Internet, a new breed of Wide Area Network has been developed to provide both secure connections and low cost. VPNs still use leased lines but instead of connecting directly from each of the remote sites to the central

data center, the remote sites simply connect to a local Internet access point through an Internet Service Provider, or ISP. The VPN hardware or software then creates a secure, private tunnel between the remote and host sites for secure data transmission over public lines (Cooper, 2003). This greatly reduces mileage fees associated with the leased lines as all long distance traffic is transferred over the Internet instead. Data security is maintained by using several forms of data encryption and user validation technologies end to end (Cisco, 2003).

Types of Virtual Private Networks

VPNs can be constructed using several different methods. The most common forms are software, specialized stand-alone hardware, router add-ons, or hosted by the Internet Service Provider.

Software requires a computer to be used at each end that runs the VPN software package. This method is the most flexible, however can also be quite costly due to the cost of the server hardware requirements, the Operating System, and the cost of the VPN software. An example of a software-based VPN solution would be Checkpoint's VPN-1 product for Windows NT (Checkpoint Solutions, 2003). In addition, the chance of an operating system technical issue may be greater than the chance of a hardware failure. Several network managers interviewed by the researcher expressed the fear of operating system failure as a primary concern. However, it is as stable as the operating systems used on servers for sophisticated data transfer and stability. This solution relies on both hardware and operating system software to operate.

Specialized stand-alone hardware uses a "black box" at each site which links the computers at each site together and routes the data onto the Internet to another "black box" at the central site. This method is often very cost effective and simple to maintain. The downside is that

flexibility is somewhat reduced because upgrades typically require complete replacements, although recently this solution has also become software upgradeable mitigating some of the flexibility problems. An example of a stand-alone solution is one provided by Internet-Appliance, which is simply a single box attached to the network at each site. These boxes are very small, about the size of a notebook computer, and are optimized for maximum performance due to their specific purpose. They will handle encryption algorithms, connectivity, user accounts and management, grouping of users, and often provide a graphical user interface available via the Intranet for setup. Reporting tools are often available as well, showing the utilization and making justification of additional boxes easier (Green, 2001)

Network Router add-ons are similar in function to the stand-alone hardware system, however the add-ons can only work with specific high-end routing equipment. Generally unless the routing equipment has already been deployed in the enterprise, the purchase of a router simply for VPN use is not cost-effective. If however a supported routing device is already in use, VPN services can be added to the existing hardware at a cost comparable to the stand-alone hardware system, but without the need for extra hardware boxes as the VPN services run inside the routing equipment. These solutions tend to be faster and highly reliable, though more complicated to configure. CiscoSystems, the leader in research, design and manufacturing of all networking equipment, makes a router add-on that works with the existing infrastructure. Unfortunately the cost of the router add-on for a single VPN can easily be over $20,000 (Johnson, 2003)

An Internet Service Provider hosted VPN takes the technical management out of the system. The Internet Service Provider makes changes, manages the system and has control over

the tunnel that is created. Unfortunately this also leaves organizations that use a VPN as an essential core piece of their backbone vulnerable to the common issues of outsourcing; little stake hold in the performance and reliability of the system by the consultants. If this approach is taken, it is recommended by many industry professionals that only companies with an established partnership with an outsourcing firm be contracted for this type of vulnerable work (Cisco, 2003)

Issues for Consideration

There are numerous planning and control issues that need to be considered prior to making a decision to proceed with a more traditional WAN configuration or a VPN configuration. These issues are discussed below.

Security and Performance Issues

Virtual Private Networks received bad press early on in their implementations primarily due to inherent security risks. In the recent past, changes in the way data is encrypted and better encryption techniques employed by VPN solution providers have made this issue much less of one. Once the secure tunnel is created, all packets passed are encrypted and meaningful only by the box on the receiving end. Only VPN vendors that fully support IPSec, or the Internet Protocol Security protocol, should be considered for implementation. IPSec is the established protocol of the Internet Engineering Task Force (IETF). The IETF is a collaborative, peer-reviewed standards board that helps ensure compatibility and interoperability. IPSec is a collection of security protocols that adds authentication and encryption to all Internet Protocol communications (Thayer, 1997).

Types of VPN Technology

There are three primary VPN technologies in use today: trusted VPNs, secure VPNs and hybrid VPNs. Secure and trusted VPNs are not technically dependent, but they can co-exist (Ferguson, 1998). Trusted VPNs implies that the customer trusted the VPN provider to maintain the integrity of the circuits and to use the best available business practices to keep from snooping on traffic traveling on the network (VPN Consortium, 2003).

As the popularity of the Internet grew, security became more of an issue. Trusted VPNs offer no real security, and vendors started to create protocols that would allow traffic to be encrypted "at the edge of one network or at the originating computer, moved over the Internet like any other data, then decrypted when it reached the corporate network or a receiving computer." (VPN Consortium, 2003). The encrypted traffic acts like a tunnel, and even if a person watching the network captured the data they would not be able to read it or change it. These types of networks are referred to as Secure VPNs.

Most Common Security Concerns

There are many security concerns with regard to Virtual Private Networks. "Few would dispute the importance of network security—the barrage of horror stories about viruses, defaced Web sites, and denial of service (DoS) attacks have made network vulnerability all too apparent." (Greenberg, 2001).

VPN Risks

There are two primary levels of risks associated with VPNs. There is a user level risk and a network level risk, making corporate data vulnerable. There are three specific security weaknesses that users of VPNs are exposed to: Subnet access from peer computers to shared

hard drives, listening into or capturing non-VPN traffic routed over the public Internet, and buffer overflow attacks (Gartner, 2002).

Virtual Private Networks can be deployed over a number of broadband technologies, including Asynchronous Transfer Mode (ATM. and Frame Relay. To clearly explain the risks referred to in the following sections, it is important to note that the connectivity type assumed in this paper is VPN over Internet as this is the most widely used method today for cost-savings (Tissa, 2001)

User Risks

When Windows users turn on file sharing on their local hard disks, most are unaware that the default security setting is to have full access for everyone (Gartner, 2002). A drive that is shared may be an open target for anyone connected to the same network. TechRepublic (2002) notes:

> Anyone can test this at an airport hosting a few wireless LAN users. A search of the network will reveal multiple machines with full access to the hard drive. It would be easy to capture content from the drive, to delete or change documents, or to plant viruses that will later find their way into corporate repositories.

The user is not necessarily aware that this happened, and using a password does not guarantee success. Any user attempting to share a drive may find that Windows does not allow access at all unless security is removed. To mitigate these risks, users can install personal firewalls, and become educated on drive sharing procedures and security.

If a users hard drive is secure and the VPN is in place, Wireless LAN Security is therefore generally considered “good” (Gartner, 2002). To help minimize bandwidth issues, VPNs can be configured to route only internal traffic, allowing public sites to be accessed directly over the Internet instead of by tunneling through the corporate backbone. Public traffic is then unencrypted. While in theory “this does not expose sensitive information because corporate

transactions should occur only through secured Internet protocols, in practice there are still risks." (Gartner, 2002). Public electronic mail systems generally do not use encrypted passwords, and users who have the same password for their public and corporate account can easily find their password stolen. Users who use the same password for public sites that they do at work may be at risk of having their password "sniffed", allowing hackers to record information while it is being passed across the network. The easiest way to eliminate this issue is to configure VPNs to route all traffic for public LAN use through the corporate backbone, therefore requiring additional bandwidth and incurring more costs.

The third way that users may be at risk is by buffer overflow. These attacks have become far more commonplace and can be more difficult to track down. This occurs when a process tries to store more data in a buffer (a temporary data storage area) than the buffer was intended to hold. "The extra data may contain code designed to trigger specific actions, in effect sending new instructions to the attacked computer. Even with VPN and secured storage, a machine is exposed to buffer overflow attacks from machines on the same subnet. These machines enjoy full, unobstructed access to all ports and may well find vulnerabilities in old, undocumented or new buffer overflow weaknesses." (Gartner, 2002). These types of attacks are considered the most significant security vulnerability to users, and usually expose a system externally. Personal firewalls for users will help to alleviate this issue.

Corporate Risks

Corporate risks include vulnerabilities in the security methodology used with VPNs that would enable someone from the outside or the inside without permission to access data that should not be reachable. Outside attacks or compromise of data or integrity means that someone

from outside the network gained unauthorized access into the network. Inside hacking refers to someone with access to the network, but without access to a specific set of data that becomes accessible through password compromise, security breaches or a variety of other means (Johnson, 2003).

Network Administrators must take into account the sensitivity of the data that they are securing along with the costs of the security. VPNs can put corporate data at risk because they allow a point of entry into the network. Anytime a server or piece of infrastructure is put in place that requires or allows access from untrusted sites, they become risky for the organization. (Cisco, 2003)

In addition to corporate data security compromises, regulations specify that protection and control must be on the data itself. “The public is demanding that corporations become vigilant stewards of their data and apply appropriate safeguards and processes in the event that such data is compromised.” (Schoonmaker, 2003) The California Database Security Breach Act, which took effect July 1 2003, is one example. (Schoonmaker, 2003). The Act states that any organization that electronically holds nonpublic, personal information on California residents regardless of where they are located must notify residents whenever “unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (Schoonmaker, 2003). Federal legislation is pending with the same scope. Failure to comply with these requirements will result in financial penalties and lawsuits.

Service providers began offering a new type of trusted VPN, using the Internet instead of the telephone system. These VPNs still do not offer security but they offer a way to easily create network segments.

Secure VPNs can be a part of trusted VPNs, creating a third type, the hybrid VPN. Security can take place by the customer or the provider.

Configuration Integrity

If the operating system is secure (disabling services that are not needed, access on all TCP and UDP ports that are not required) another area to look at is the integrity of the configuration. If an intruder modifies anything, there are ways to easily and quickly determine that. Server administration software tools such as Tripwire are useful in detecting these modifications (Greenberg, 2001)

Integrity checking "is implemented through a hash function, which produces a unique number based on data supplied to the function." (Greenberg, 2001)

The probability of getting the same hash for different data inputs is close to zero. "Tools such as Tripwire compute the hash of various key system files and securely compare the hash of the original system files with the hash of ones that may have been altered." (Greenberg, 2001). Hashes must be stored on a separate secure system or hackers can replace the original has with the one that corresponds to files they have altered. A new hash snapshot must also be created every time system configuration is changed.

Intrusion Detection

Intrusion Detection Systems (IDS) are another key element to a secure VPN and network environment. It is a real-time analysis of the interactions of a computing environment, and determines if penetrations have occurred or are likely. An IDS generally has several components: probes, servers, workstations, firewalls, and routers. Each of these components is analyzed for symptoms of a security breach.

A well-configured IDS will monitor for attack patterns, monitor system logs, and issue alerts based on violations of documented security policy. Intensive logging can consume significant resources and the cost of doing so must be weighed with the actual risk (Greenberg, 2001). Vulnerability audits will analyze system weaknesses. Vulnerability scanners may appear as intrusions by the IDS. Vulnerability analysis and intrusion detection should be focused on all component levels: the network, server, desktop and applications. IDS and vulnerability analysis tools can also be used to manage components managed by carriers and Internet Service Providers. These scans must be coordinated through these companies.

Denial of Service

Denial of service attacks take advantage of inadequate filtering. Without proper filters, routers will deliver traffic wherever a hacker wishes, regardless of the IP address of the source, the destination address, or the traffic type. Systems can be overburdened and taken down based on utilization. Filtering should not only occur at the firewall; any components that are not needed should be disabled. ISPs should establish a solid escalation path that allows technologists to quickly notify engineers to filter DoS traffic. ISPs should share their procedures in coordinating DoS attack issues. Running systems close to capacity (memory, storage, CPU, network bandwidth). maximizes threats to a DoS attack. Resource usage should be monitored within the system, looking for increases in usage and allocating spare capacity to accommodate unexpected loads.

Issues to Bring to Executives

Many industry professionals do not recommend looking to technology right away to minimize risks, but rather assessing current strategy and policies. Experts recommend

establishing a “security incident team” that responds to intrusions. The team needs to be capable and ready to perform analysis, carry out surveillance, and “bait” hackers. The team needs rights to shut down affected services, carry out recoveries from backup systems, coordinate any public relations issues, and address the vulnerability.

> Repairing instead of rebuilding a hacked system is dangerous and a nearly impossible task; you do not know exactly what the hacker did. Obviously, the replacement system should incorporate a defense against the successful attack and should be built with your organization's latest tested and approved system patches and in accordance with any configuration advisories. Clearly, backup and recovery procedures are an important part of a quality security strategy.”. (Greenberg, 2001)

Security Policies

“Contrary to popular belief, corporate sabotage is among the least likely causes of computer security breaches, according to an April 2002 survey by the Computer Security Institute. The Computer Crime and Security Survey reports that sabotage accounted for just 8 percent of system attacks in 2002.” (Southgate, 2002). According to these organizations, security breaches are more often due to errors by end users or administrators. These inadvertent mistakes are often the cause behind viruses; denial-of-service attacks, and open entryways to data that is supposed to be secure (Southgate, 2002)

“CIOs can reduce, and possibly eliminate, an organization’s risk from these errors by creating and implementing a comprehensive set of IT security policies aimed at user behavior. These policies, along with efforts to educate users about how to eliminate security weaknesses, can thwart future vulnerabilities and boost awareness about security issues throughout the

enterprise." (Southgate, 2002). There are ways to automatically create these policies based on management employee policy and desired outcomes (Fu, 2001). Determining what to cover in IT policies is a difficult part of the process. A good security policy must address end users and administrators. User policies should address how staff is permitted to make use of computer equipment and applications (Southgate, 2002). According to Southgate and TechRepublic, online resources for IT professionals, some areas to address are: data and application ownership, helping users understand what applications and data can be shared, hardware use, reinforcing existing guidelines, defining appropriate use of the internet and e-mail, reinforcing end user policy-based rules, account administration and password configurations, patch management, incident reporting practices, and emergency escalation plans.

Policies must be properly updated and monitored when changes on the servers or network are made. In addition, policies are not valuable unless they are enforced. For example, BindView's Policy Center and PentaSafe's VigilEnt Policy Center helps create policies for the enterprise and includes online quizzes to build user awareness of policies (Southgate, 2002).

Security - Industry Cases

There are numerous examples of accounts and network data being "hacked" by individuals, resulting in corporate and personal data compromise. The section below describes the cases recently noted at TD Waterhouse, Ecount, Playboy, Egghead, Creditcards.com, Western Union, CD Universe and America Online.

TD Waterhouse

In a recent case, a teenager hacked into another individual's online brokerage account to trade options (CNN, 2003). The hacker concealed his identity to remotely capture other people's

user names and passwords. He then logged into the individuals account to buy options. The Securities and Exchange Commission Internet enforcement unit has brought 424 Internet-related actions since the unit opened in 1995, involving in almost all cases stock manipulation schemes. The thief used about $47,000 from the victim's account and avoided personal options losses of about $37,000.

Ecount

Ecount is an online gift certificate service that was hacked into and had personal information belonging to customers stolen (Sandoval, 2002). The crime has yet to be solved, and the intruder offered to return the information for a fee. Hackers are rarely caught and elude capture easily because of he sophistication of their technology is generally superior to the technology of law enforcement officials. Fraud costs e-tailers about $700 million last year in lost merchandise, costing web stores approximately 5 to 8 percent of sales (Sandoval, 2002). According to a Gartner study, 5.2 percent of online shoppers have been victims of credit card fraud and 1.9 percent of identity theft, hurting the economy and business for e-tailers. There are many hacks unsolved, including six high profile cases noted below from C|Net News:

Table 3

List of recently hacked systems

Site	Incident
Playboy.com	An intruder slipped past the Web site security systems of the adult entertainment company last November and obtained the personal information of an undisclosed number of customers of the site's e-commerce store. The hacker notified customers that he or she had pilfered the information and, as proof, gave them their credit card numbers.
ECount	A hacker circumvented the Internet defenses of the Philadelphia-based company's gift certificate service and notified customers of the breach in an e-mail that included their home addresses. The

	hacker then demanded $45,000 from the company to keep him from exposing the personal information of 350,000 customers.
Egghead.com	A hacker infiltrated the e-tailer's system in December 2000. After three weeks of investigation, the company said the intruder did not obtain the personal information of its 3.7 million customers, but many banks said they spent millions of dollars to issue new credit cards in the meantime
Western Union	In September 2000, a hacker exploited an opening in the Web site of the financial services company and got away with more than 15,000 credit card numbers. Human error left "performance management files" open on the site during routine maintenance, allowing the hacker access.
CD Universe	About 350,000 credit card numbers were stolen from the online music company in January 2000, one of the first large-scale hackings of its kind. The thief, identified only as "Maxus," held the card numbers hostage and demanded a $100,000 ransom. When the company refused, the hacker posted the numbers on a Web site.
Creditcards.com	In December 2000, a hacker broke in to systems maintained by the company, which enables merchants to accept payments online, and made off with about 55,000 credit card numbers. The hacker tried to extort the company and, when executives refused to pay, exposed the numbers by posting them on the Web.

American Online was also hacked as its community leader data was circulated via e-mail (Hu, 1998). The excel file attachment sent around via e-mail contained screen names, true names, and account numbers of more than 1,300 AOL community leaders. Community leaders are members who volunteer their time as guides and chat room monitors in exchange for free membership. A hacker broke into the account of an AOL employee who oversees the leaders and sifted through the employee's 400 e-mail files, finding the attached Excel document. The hacker then mass e-mailed the list.

Decreasing Risks

There are several ways to help increase the security level of VPNs. Encryption, authentication and firewalls are the most common ways to reduce risks.

With encryption and a reasonably secure method of transmission, the other issue to consider is performance. The VPN tunnel still uses the public Internet, which is notoriously slow. Most analysts, and even VPN solution providers, do not recommend using VPNs for transmissions that require immediately responses, such as the airline industry. A potential traveler waiting at the ticket counter at an airport will most likely find a three second Internet delay for each push of a button too slow, which can often happen with VPN technology (Mohan, 1999). VPNs should be used where a possible delay will not leave a customer with a bad taste in their mouth. If a VPN is going to be used in front of customers, it is important to be sure that adequate bandwidth is purchased for the remote site to ensure that the Internet is not a bottleneck.

Encryption

Encryption is a solid way to ensure data integrity. The difficulty is that it must be encrypted regardless of how it is created or distributed. Encryption must happen "consistently across all relevant applications without affecting the way users work." (Schoonmaker, 2003). Repository or container-based encryption approaches such as Pretty Good Privacy (PGP) are not user friendly or reliable enough because the sender and receiver must take an active role in maintaining the protection. Studies have shown that if users have to enable encryption then more often than not, the initial protection is removed permanently (Schoonmaker, 2003). Full disk encryption is another method and may be useful for laptops, but once the users password is hacked thieves gain access to all of the data again. Encryption on all data is a difficult control to

apply. Encryption secures data at rest or in transit, but does not protect when it is being used in applications.

VPNs generally use IPSec as a form of encryption. IPSec policies are widely deployed in firewalls or security gateways to protect information (Fu, 2001). Encryption is the conversion of data in a way that cannot be understood by anyone or any machine that is not authorized to view it. Likewise, decryption is converting the encrypted data back into its original form so that it can be read. To decrypt messages, a decryption key is needed. This key takes apart the encryption and reads the information underneath this security layer. We see encryption as a key element in both Virtual Private Networks and wireless communications. A simple form of confidentiality can be achieved through encryption, but pure encryption is not sufficient. Another important security property is semantic security, which ensures that an eavesdropper has no information about the information, even if it sees multiple encryptions of the same data (Goldwasser, 1984)

IPSec is not necessarily secure, though many network engineers believe that is the case (Murphy, 2002). However, it is still recommended by experts as a requirement for implementing any form of VPN device (Huttunen, 2003). Often using high levels of encryption is difficult across multiple continents because the International Standards Organization (ISO) defines more than 230 countries in the world, 69 of which have import/export controls on cryptography for governmental security reasons. “In more than 58 countries, it is unclear what you can do, and in 19 countries there are external restrictions on export/usage of encryption from the US. In Myanmar in Burma there is a minimum five-year jail term for the illegal use of encryption." (Murphy, 2002). In addition, using IPSec creates issues finding carriers that can truly provide global access.

IPSec is a framework of protocols that is evolving to become a standard. It is compatible with most different VPN hardware and software solutions due to compatibilities and requirements being set by standards organizations. IPSec authentication is not user-based, but comes from the IP address or a certificate to establish the users' identity and ensure integrity. An "IPSec tunnel basically acts as the network layer protecting all the data packets that pass through, regardless of the application." (Web Host Industry Review, 2003). IPSec VPNs allow the administrator to define a list of networks and applications to which traffic can be passed. However, IPSec-compliant products provide access control over the network and transport layers only, and not many options to regulate access to the resources within these hosts (Web Host Industry Review, 2003). It is important that when encryption schemes are being analyzed, a thorough "analysis of the different paths in which an intruder can take and to precisely specify the assumptions that have been made" is crucial. Therefore, it is key that Network Administrators not just install encryption technology but be sure it covers adequately the organization's information (Needham, 2001).

"Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Forwarding (L2F) are also available, and although only a handful of firewall vendors support these security protocols, they are part of the reason why there is no current universally accepted standard." VPN vendors must determine what standard they are going to use and must adhere to standards organizations requirements if they will be compatible (Web Host Industry Review, 2003).

Authentication

Authentication is the process of determining whether something is what it says it is. Authentication is most often done through the use of login passwords. Knowing the password is

assumed to guarantee that the user is authentic. This methodology leaves much vulnerability, including theft of passwords by numerous methods, accidentally revealing passwords, or forgetting passwords. The Internet often uses a more stringent method of authenticating, called public key infrastructure (PKI). Authenticate precedes authorization, or access to a particular set of data (Pigeon & Vandendorpe, 1998)

Authentication verifies the source of the packet at both ends, and encryption codes packets so only the intended sender and receiver can view data. This helps to ensure that even if a hacker did obtain the data, it is unusable to him or her (Thayer, 1997). Encryption keys can change and be verified through software and hardware; encryption can even be set at the network card level. Wireless networks easily integrate as the wireless card receives its addressing information from a host router and then connects to the VPN through the routed Internet connection. While companies are using VPNs to share documents and electronic mail, many IT groups are still not comfortable using it to share highly confidential information as the data travels across public lines. For instance, the health care industry has all but completely disregarded VPNs as a solution for any data transmission (Schneider, 1999). For most organizations, VPNs are a safe alternative for connectivity issues.

"Authentication is the process of validating a user; are you who you say you are?" (Greenberg, 2001). There are many solutions providing authentication, from basic user name and password devices to tokes, smart cards and biometric scanners. (Tankus, 1997). Systems can authenticate based on three criteria: what you know, what you have, and what you are. "Tokens and smart cards (what you have) must be paired with passwords (what you know) or biometric technology (who you are) to produce a stronger solution. This helps prevent stolen smart cards or

tokens from being used." (Greenberg, 2001). The RSA SecurID card is a popular choice among authentication professionals as it displays a constantly changing numeric identifier on a tiny LCD Screen. The number is synchronized with server software. Users login entering a user name, password, and the unique identifier on the token. Server side software determines if the identifier is correct for that moment. This security option generally costs about $50 to $100 per user but greatly improves security.

Smart cards contain an embedded chip that is programmed to send and receive data and perform tasks. The electronics are small and can be formed into many different physical "packages". Many of these smart cards are about the size of credit cards. According to Greenberg, there are three categories of smart cards:

1. Memory-only: Capable of storing and returning information but no more. Such devices have limited use in network security and are generally relegated to applications such as phone cards, gift cards, and the like;

2. CPU-based: Capable of processing information;

3. CPU- and crypto-coprocessor–based: Typically tied to a public-key infrastructure (PKI) and sometimes called PKI-enabled smart cards. PKI is a combination of software, services, and encryption technologies that facilitate secure communications and transactions. The only way to get a card to perform private-key operations is to provide a password or biometric information. (Greenberg, 2001)

A multiple platform driver-level procedure call called PKCS #11 (public key cryptography standard 11) has been developed by the RSA Security Consortium. "PKCS #11 facilitates the use of removable devices that work with cryptography and is well suited to smart-

card devices and to cryptographic accelerators, such as those used to speed up Secure Sockets Layer (SSL) or IP Security protocol (IPSec) processing." (Greenberg, 2001). Smart cards offer benefits but require smart card readers or some mechanism by which to interface with the computer. The Aladdin eToken is one smart card that is compatible with any Universal Serial Bus (USB) based input, allowing the technology to be easily and widely deployed.

"Biometric authentication systems capture and store physiological data such as fingerprints, hand prints, iris or retina scans, or behavioral characteristics such as voice patterns, signature style or keystroke dynamics." (Greenberg, 2001). Users provide a sample, which is compared to the stored biometric data. They are expensive and complicated to administer, and often result in Type I errors, or false rejects, which are frustrating to legitimate users.

Firewalls

Firewalls, devices that provide a barrier between the Internet and internal networks for security purposes, are the "easiest way (to secure a network) because they require minimum management by the user and they can be integrated into the corporate firewall policy management" (Murphy, 2002). In addition, firewalls can be administered and managed remotely by the IT security staff. However, even using firewalls does not keep employees from being the victims of gateway access. This allows others on the network to use the employees' computer as access to the file shares (Davoine, 1997)

Firewalls handle most authentications of VPN users. There are also firewalls designed specifically for VPN use now, such as NetScreen, Watchguard or NetFortress. These firewalls can connect to as many LANs as needed and keys are exchanged between two units. When this occurs, the VPN is complete (Green, 2001)

Different VPNs, Different Security

Secure VPNs should always require data encryption and authentication. Some VPNs will require authentication but no encryption and there is no privacy in these networks. Network administrators need to explain to the business the risks associated by having two endpoints in a VPN tunnel, and the person(s) responsible for security must agree to the same security properties on both sides of the connection. It also must be impossible for anyone outside of the VPN to affect security properties (VPN Consortium, 2003)

Trusted VPNs are of value because the customer trusts the provider to provision and control the VPN. Therefore, it is assumed that no one outside the trust relationship can change any part of the VPN. In the case where the VPN spans more than one provider, the customer is trusting "the group of providers as if they were a single provider" (VPN Consortium, 2003). With this type of VPN, no one other than the VPN provider should be able to change, add or delete data within the VPN. Customers should also develop a maintenance plan for routing and addressing and compare the routers to plan as often as possible (VPN Consortium, 2003).

Hybrid VPNs should make sure address boundaries within the trusted VPN are clear. In a hybrid, the secure VPN may be a subset of the trusted VPN, for instance, if one department runs its own secure VPN over the corporate trusted VPN. For any address in a hybrid VPN, the VPN administrator "must be able to definitively say whether or not traffic between those two addresses is part of the secure VPN" to help minimize risks (VPN Consortium, 2003)

Policies

Network Administrators must work in conjunction with security personnel to be certain that firewall policies are inline with VPN policies. "Policies are a means of influencing

management behavior within a distributed system, without coding the behavior into the managers. Authorization policies specify what activities a manager is permitted or forbidden to do to a set of target objects and obligation policies specify what activities a manager must or must not do to a set of target objects. Conflicts can arise in the set of policies and network administrators must work through them to remove conflicts that will compromise security (Lupu & Sloman, 1997). They must also work with systems administrators to be sure that system-level passwords and security settings are applied properly.

Proactive measures will also help protect data. Organizations must ensure that they have control over data regardless of what users have it, including validating that former employees do not have access to data. CIO Magazine cites three ways in which Chief Information Officers can help protect their corporate data. They are through the use of encryption, controlling and monitoring data access, and always enforcing policies (Schoonmaker, 2003)

Controlling and monitoring access to and the use of data must extend to the data throughout its use in unencrypted formats, and provide rights based on the users role and sensitivity of the data. Users' actions should be logged and audited, including data edits, copying and pasting, printing and reading (Schoonmaker, 2003)

Policies must be enforced at all times. Business units, not Information Technology groups, should define usage policies. Information Technologists must use the policies set by the business functions and create policies that work without interrupting users (Schoonmaker, 2003)

Technologies to Reduce Risk

There are multiple technologies available both within and as third party tools to VPNs that will reduce security risks. It is important that Information Technology professionals

understand the goals of their security framework, authentication, protection of privacy and system integrity, vulnerability, intrusion detection and protection against Denial of Service (DoS) attacks that often result in excessive traffic, bringing down a network (Greenberg, 2001)

Quality of Service

One consideration when determining whether or not to use a traditional line method of connectivity of a Virtual Private Network is the scope of the network. If the network will be used for voice and data then the requirements will be different. Quality of service may be critical to networks that converge. For that reason, it seems important to have a brief discussion on the technical definitions and how they relate to Virtual Private Networking. Quality of Service, or QoS, is the idea that data transmission can be improved and guaranteed in advance. (WhatIs Definition, 2003).

Class of Service

Class of service, generally noted as CoS, is a way of managing traffic by similar classification. With this type of quality guarantee, each type of data is treated as a class and will prioritize based on a set priority set by organizations on routers, and classification. It does not guarantee a transmission rate (WhatIs Definition, 2003).

Service Level Agreement

Generally, a Service Level Agreement (SLA) is reached between the provider and the user. This is the agreed upon service level that users will receive. In the data communications field, it is the service level that the subscriber will receive from the provider. The terms are measurable and organizations should match realized service quality with guarantees. The SLA will dictate what bandwidth guarantees and priority traffic will receive. Determining this

requirement is fundamental to determining whether or not a Virtual Private Network will save the organization money. If it does not meet QoS requirements then it is not useful to the company.

QoS, CoS and SLA all need to be worked into plan requirements whether a traditional network or a Virtual Private Network is being created. Quality of Service is a key element to building on any network. Without a QoS agreement, the operations team has no fundamental data upon which to build network services. CoS is often handled in-house on routers by infrastructure personnel. A key use for this would be packet prioritization based on fundamental applications that the business relies on. For instance, SABRE (proprietary application) traffic might be prioritized for a travel agency instead of HTTP (Internet) traffic (Green, 2001)

When handling capacity plans and determining future needs and scalability requirements, network planning teams should also note the available bandwidth by the service that they are using. For instance, if DSL will only handle a maximum upload speed of 300kbps but the users, based on forecasting, will need 2 mbps, then a change in service should be included in the plan. Since different services all provide varying speeds and quality of service guarantees, these need to be predetermined and providers should be carefully selected to ensure these service level agreements. To do so requires careful planning, forecasting, and benchmarking to measure success.

Convergence

Before undertaking a wide Virtual Private Network project, companies need to consider the issue of convergence and whether or not they will attempt to undertake this in their structure.

Convergence also deserves discussion because choosing to converge will alter an organizations plan for Virtual Private Networks. .

Convergence is the mixing of video, voice and data networks onto one network, "line" or "pipe." (Green, 2001). There are concerns with converged networks that are very real; most of which pertain to quality and whether or not cost savings are actually seen in these networks. Quality generally suffers if networks are not implemented properly, potentially leading to issues with data transfer as well (Green, 2001).

There are serious disadvantages to the converged network. There are however a few business models in which it may be advantageous. In some cases it can enhance the customer service component to the end user. For example, web-enabled call centers that do not require a toll charge but still allow users to receive premiere support is one key advantage. Obviously this would not be an advantage in most industries. A potential cost savings may be seen if data and voice are traveling over the same line rather than having to pay for separate lines; in addition toll charges for long distance calls may be eliminated. Voice over IP is a good example of such networks, data and voices sharing the same lines. In some organizations this may be enough to justify the project and the reduced quality of voice.

Whether or not network convergence takes place should be defined and well understood prior to determining any network operating or strategic plan, especially whether or not traditional WAN lines or VPN connectivity will be used in the business. Network convergence will change the underpinning of the network, the backbone and architecture. Proper resources must be devoted to such a project, which will reduce availability of staff for other projects. Proper resource planning and documentation will help to ensure a solid technology plan.

Considering VPN Technology

Virtual Private Networks have become increasingly important in enterprises that require multiple office connectivity and desire a reduction in their overall costs of doing business. They have the potential to greatly reduce costs associated with Wide Area Networking and to change the face of networks permanently. They are capable of getting data from point A to point B quicker and less expensive than previous technologies. According to Information Week, using a local Internet service provider dial-up line saves an estimated 60-80% over toll-free remote access server lines (Mohan, 1998). Cisco Systems estimates that an organization with 1000 dial-up users and 3000 users on an 800 number, with an average number of hours online of only 5 per week per user, will save anywhere from $376,000 per month to $481,000 per month. The savings depends on whether a hardware, software, or router solution is chosen. In addition, there is an estimated 20-40% savings over dedicated leased lines due to the elimination of long distance communication charges required for traditional Wide Area Networks (Mohan, 1998). Adding users to the Virtual Private Network is also very simple requiring little time, while adding users to a direct dial-up solution can take months (Schneider, 1999).

Management and Organizational Implications of VPN Model

Virtual Private Networks may be used to provide an organization with many competitive advantages. Moving to VPN architecture may create additional centralization and the ability to manage users and connections around the world from a single site. The management utilities available with a VPN allow for network managers to make changes centrally without the need to touch desktops. It may be used to connect remote offices or branch offices to the central office to maintain database consistency. It is also being explored as a means for third parties, such as

consumers, partners and suppliers, to connect directly to the organization for updates, accurate product information, ordering and billing and a variety of other online tasks. It may also be considered as a remote access solution for employees who travel or are off-site often and require access to the central site. For instance, if a traveling salesperson needs to connect and is in New York, the individual can simply connect to the local Internet Service Provider in that state free of long distance phone charges, and using the VPN software on a laptop, access the central office seamlessly and securely. The increasing security and extensive cost savings make VPNs an essential ingredient to a successful, low-cost network (Johnson, 2003)

WAN and VPN Equipment Differences

WANs and VPNs use different equipment. Wide Area Networks require traditional routers and some sort of wide area connection that connects two or more sites together directly. This can be frame relay, ATM, point-to-point, or many other types of connections. The lines are centralized at one spot and connect to the infrastructure hardware.

Virtual Private Networks connect using VPN devices. These can be hardware or software devices that are placed at both sides of the connection. Sometimes the connection is established using software on the users' PC and hardware on the VPN box at the host. There are entire software-to-software solutions, however they are generally less efficient and may not be as secure (Cisco, 2003)

Wireless Networks

Wireless networks increase the risk of security breaches. Many executives believe that applications provide protection for passwords transmitted over the network. However, most passwords are sent either unencrypted or weakly protected. A hacker can set the LAN interface

into “promiscuous mode” (sniffing mode) and read passwords and anything else unencrypted (Greenberg, 2001). Vulnerability scanners and intrusion detection systems can help check for these weaknesses. However it is difficult to control every interface on the network.

Most Internet applications such as File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), or Simple Network Management Protocol (SNMP) commonly used when surfing the web or transferring files offer little or no password protection. A secondary form of security such as Secure Socket Layer (SSL) or IPSec must be used. SNMP is used to configure routers and servers and get statistical information from them but offers little password protection. The servers and routers should be configured to accept SNMP queries from the IP address of the network management server only, limiting the exposure or risk of an unauthorized person gaining access.

When creating web pages using SSL and HTTP (referred to as HTTPS), a common programming “error often exposes passwords. HTTP basic authentication is the most common method of authenticating web site visitors, but alone it provides inadequate password protection.” (Greenberg 2001). When using SSL to secure a page for which HTTP basic authentication is configured, the administrator must be sure to gather the password after activating SSL in the HTML code, not before. Otherwise, passwords will be sent in plain text and not through the protected SSL session. (Greenberg, 2001).

Another interesting point when choosing network hardware to secure the VPN is that both SSH and SSL are strictly two-party, point-to-point protocols and do not work with a third system, such as a firewall. “To SSH and SSL, the firewall is something to tunnel through, not to

interact with." (Greenberg, 2001). IPSec is designed to accommodate more than two other devices.

IPSec Authentication works by establishing security associations (SAs) between two devices on methods for secure communication. A single IPSec SA can exist between two endpoints, with firewalls establishing their own encryption and authentication SAs to apply corporate firewall policies. "The encryption of a connection is broken at the firewall, allowing it to inspect the session's contents. The contents can then be re-encrypted for transmission to the destination. In this way, two endpoints can securely authenticate themselves, but intermediate firewalls can also inspect contents of the session and perform their own authentications." (Greenberg, 2001)

VPN Benefits

There are several benefits to using Virtual Private Networks. There is inherent reliability in use of the Internet that transfers to VPNs. Low equipment mean time between failure is another benefit, as is the wide selection of vendors available. Authentication and encryption technology advances have also aided in adding benefit to the system.

Reliability

WANs and VPNs are both quite reliable. The inherent reliability advantage that the VPN has is its use of the Internet, which in its early form (ARPANet) was built for redundancy by the government during the Cold War. This model has continued, ensuring continuity of service for commercial applications and e-commerce. The very nature of the Internet provides automatic redundancy and failover by infinite routes, whereas WAN connections require separate lines be run for redundancy. In both cases, equipment failure could lead to downtime however.

Selection of Vendors

When VPN technology was new, companies had to manage them in-house. They had to purchase their own equipment, install Internet connectivity separately, and connect the two sites. There are numerous major communications providers now offering complete services. The communications provider, instead of simply offering the Internet Protocol connection, offers the service that provides the secure tunnel across the Internet to both sides of the connection. Under the right circumstances or where there is limited in-house expertise, outsourcing can be a huge advantage to businesses.

VPN technology has also advanced to provide better encryption, more reliable service and more users per device than ever before (Cisco, 2002). Competition increasing and VPN standardization in many companies has increased the opportunity for better equipment at less expensive prices. Boxes take less physical room than in the past, and provide better service and reliability.

Cost versus Cost Savings

The potential cost savings for companies using Virtual Private Networks in place of traditional Wide Area Networks is significant. As noted earlier, this is especially true when remote clients or hosts are in international territory. Using a VPN for remote access, a company with 350 users and 31 hours of connection time per user per month can save $525,000 annually, according to Infonetics analysists (Schneider, 1999). This is about a 70% savings over traditional dial-up access numbers. "The ability to have users dial in through the Internet from places other than a branch office has inspired CIOs to consider VPN technology as a platform for connecting to partners and suppliers. ‘Imagine trying to connect 10,000 third parties,’ says Dan Merriman,

vice president at Giga Information Group Inc. in Cambridge, Mass. ‘That would be a nightmare with frame relay or private lines. With the Internet, all you do is ship out your IP address and you are off and running.’" (Schneider, 1999). As mentioned earlier, to save $481,000 per month would require an initial investment of $40,000 with monthly costs of $95,000 compared to the dial-up costs monthly of $576,000. This is based on dial up users paying between $20 and $50 per month, a relatively low rate. There is a one-month payback period using a VPN over traditional Wide Area Network connectivity methods.

This incredible cost savings is evident when analyzing a case study within a large organization, the dilemma that faced Twentieth Century Fox Film Corporation. They needed to get 31 international sites onto their main network by the end of the year 2000. Dedicated leased lines to these locations were unaffordable, even with a very large technology budget. Instead, they decided to connect the sites to corporate headquarters with 128Kbps-dedicated connections to UUNet's Internet backbone, using Novell Inc.'s Border Manager VPN product (Schneider, 1999). The London, Mexico and Tokyo offices were up in 1999, and 18 more sites were scheduled for deployment in the last half of the year. "Employees are using the network to access e-mail, the Internet and customer, sales and other business data from Fox's servers in Los Angeles." (Schneider, 1999). In the Tokyo office alone, Fox is paying $350 a month in charges to a local Internet Service Provider, much less than the $7,000 to $9,000 a leased line would cost, says Nader Karimi, Fox's executive director for client computing services (Schneider, 1999). Karimi predicts the company "will save at least $600,000 a year in e-mail transmission and file sharing costs from the first 21 sites—even after spending $6,000 to $8,000 to install new equipment at each site.” (Schneider, 1999) Karimi's staff will also be able to monitor the network

from Los Angeles, which will help the company maintain its goal of 99.9 percent uptime. (Schneider, 1999)

CHAPTER 3. METHODOLOGY

The purpose of the study was to evaluate Information Technology manager's perceptions of the security and reliability of Virtual Private Networks, and to identify the relationship of their perceptions with their willingness to recommend them. The conceptual framework for the study was specifically a survey instrument sent to a pool of information technology management professionals.

Sample Design

The theoretical population was all Information Technology Professionals in a management role. The study population were technology managers and executives in Southern California including Los Angeles, Orange and San Diego counties. It was assumed that technology professionals in Southern California are no different in their perceptions than all other technology professionals in the United States. The sampling frame contains more than 1,000 technology professionals and represents small, medium and large-sized businesses. Each of the over 1,000 technology professionals in the sampling frame were sent the survey, thus minimizing sampling error.

The study did not require that a manager support a particular number of users, but only that he/she was familiar with the use and implementation of Virtual Private Networks. The researcher provided the sample based on surveys sent via electronic mail and taken on the web to a mailing list of professionals in the Southern California area. The mailing list was made up of professionals in technology management in various sized companies and industries that choose to network with one another for future employment, technological advice and vendor discussions. The mailing list was free to all participants and did not require purchase for access.

No individual-specific information was on the mailing list except that which each person chooses to publish in individual posts. The survey was sent to the entire mailing list with a cover letter and the web-based link in the text. The entire sample were asked to complete the survey and submit it by web interface to the researcher.

Research Hypotheses

Hypothesis HO1 (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perception of its security.

Hypothesis HA1 (alternate): An Information Technology manager's decision to recommend Virtual Private Networks is dependent on his / her perception of its security.

Hypothesis HO2 (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her desire to save money in communications costs.

Hypothesis HA2 (alternate): An Information Technology manager's decision to recommend Virtual Private Networks is dependent on his / her desire to save money in communications costs.

Hypothesis HO3 (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perceived need for wide area networking.

Hypothesis HA3 (alternate): An Information Technology manager's decision to recommend Virtual Private Networks is dependent on his / her perceived need for wide area networking.

Hypothesis HO4 (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perception of its reliability.

Hypothesis HA4 (alternate): An Information Technology manager's decision to recommend Virtual Private Networks is dependent on his / her perception of its reliability.

Instrument

The data for this study were gathered using a questionnaire, which is located in the Appendix.

Survey Design

The first section of the survey was designed to evaluate the manager's perception of Virtual Private Networks as it relates to security. The second section refers to the respondent's perception of Virtual Private Networks as it relates to the cost versus benefit. The third section refers to the need for Wide Area Networking. The fourth section gains a perspective of the respondent's view of reliability of the technology. The fifth section gains an understanding of the respondent's general attitude toward Virtual Private Networks. The last section identifies demographics and asks open-ended questions with regard to the individual's perceptions of the technology. A five-point Likert scale was be used for sections one through five, and the survey takes approximately eight minutes to complete.

Validity and Reliability

Validity was measured through the use of pretest validity assessments. Peer reviews assisted in assessing whether the researcher has accurately stated the questions from a technical perspective. Internal validity is not considered critical to data analysis for exploratory studies of this nature because its primary purpose is not to establish causality (Yin, 1994). In addition, the study maintains content validity as the questions on the survey represent a defined domain of content or logical validity (Messick, 1998). To provide evidence of content-validity, Yun & Ulrich (2002). suggest defining the domain of interest, selecting a panel of judges, having the

judges evaluate the instrument based on specific criteria, and summarizing the information. This method was used in the researcher's study through pre-testing with a panel of Information Technology experts. In addition, face validity was performed by two sets of colleagues and peers who were focused on clarity and contextual interpretation.

Reliability was measured to ensure repeatability through the use of the Cronbach Alpha in SPSS. Reliability was found to be relatively high, with a Cronbach Alpha of .74.

Variables

The dependent variable is the manager's decision to recommend Virtual Private Networks to their organization; this variable is measured by the response to question 15.

The independent variables are as follows:

Security is the perceived level of concern and/or comfort the manager has with Virtual Private Networks. This variable is measured by response to question one in the survey.

Cost-Benefit is the manager's perceived level of benefit versus cost for the communications technology. This variable is measured by response to question six in the survey.

Need for Wide Area Networking is the manager's perceived need for corporate connectivity to remote users and distant offices. This variable is measured by response to questions nine and ten in the survey. Question nine measures need for remote sites, while question ten measures the need for remote users to connect to the corporate backbone.

Reliability is the manager's perception of the reliability of the technology. This variable is measured by response to question 12 in the survey.

Data Collection

Data were collected by a survey questionnaire administered by the researcher. The survey site address was distributed by e-mail and the survey was administered on the web. The web site

address was sent via electronic mail to the group of network managers and executives representing the areas of Los Angeles, Orange and San Diego Counties of California. Each subject was given written instructions for the survey and was asked to submit the survey to the researcher.

As with any written survey, there is always the potential for the bias of non-response; offering copies of the results to all respondents should have minimized this. Additionally, respondents may have been concerned with risks associated with replying to a survey that relates to their jobs, given the current workplace environments. To alleviate this concern, the researcher included a statement that assured confidentiality to each respondent and would not include identifying data about the respondent or the company on any survey.

Data Analysis

Each of the four hypotheses were tested using the Chi Square Test of Independence. The significance level was set at 0.05.

Summary

This chapter contains the methods used to conduct a survey and evaluate the perceptions of managers with regard to their decision to recommend Virtual Private Networks to their organizations. The study was conducted with a web-based survey and the results were measured using the Chi Square Test of Independence. The following chapter presents the results of the study.

CHAPTER 4. DATA COLLECTION AND ANALYSIS

This chapter presents findings as a result of the study. The purpose of the study was to identify particular management perceptions on the use of Virtual Private Networks to enable managers to make better decisions. In particular, it will help them determine whether the technology is becoming widely adopted and if security and reliability aspects of the system are generally acceptable to technology management professionals.

Results

There were 53 respondents to the survey, which represents over five percent of the population tested. Expected response rate for a web-based e-mail survey was expected to be low, especially when sent to workplace e-mails; this is due in part to employees changing jobs, to invalid e-mail addresses and to blocking access to messages with links or attachments. It doesn't appear that the responses represented extreme views, which is the typical result from the nonresponse bias, and there is no reason to suspect a fear of reprisal impacting response bias. It is assumed that the results are representative of the population as the list members include professionals from various companies with varying size and industry.

Hypothesis One

Hypothesis One stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perception of its security. This hypothesis was evaluated by comparing responses to question one and question 15 on the survey. Question one is “I feel that Virtual Private Networks Are Secure”; question 15 is “I would feel comfortable recommending Virtual Private Networks in my Organization Rather than Using Traditional Wide Area Networks.” Since a *strongly agree* is the only response that equates to a

fully committed recommendation, the responses were coded into two possible categories: *strongly agree* (coded as 1) and *less than strongly agree* (coded as 2).

Table 4

Crosstabulation for Hypothesis One

Count

		VPNs are Secure		
		1.00	2.00	Total
I Would Recommend VPNs to My Organization	1.00	15	2	17
	2.00	4	32	36
Total		19	34	53

Table 5

Chi Square Tests for Hypothesis One

	Value	Df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	29.866(b)	1	.000		
Continuity Correction(a)	26.606	1	.000		
Likelihood Ratio	31.739	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	29.302	1	.000		
N of Valid Cases	53				

a Computed only for a 2x2 table

b 0 cells (.0%). have expected count less than 5. The minimum expected count is 6.09.

Since the p-value is .0000 which is less than 0.05, the null hypothesis was rejected. As a result, it can be concluded that an Information Technology Manager's decision to recommend Virtual Private Networks is dependent on his/her perception of its security.

Hypothesis Two

Hypothesis Two stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her desire to save money in communications costs. This hypothesis was evaluated by comparing responses to question six and question 15 on the survey. Question six is "Virtual Private Networks provide a good value for their costs;" question 15 is "I would feel comfortable recommending Virtual Private Networks in my Organization Rather than Using Traditional Wide Area Networks." Since a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* (coded as 1) and *less than strongly agree* (coded as 2).

Table 6

Crosstabulation for Hypothesis Two

		VPNs Are A Good Value (Cost/Benefit)		
		1.00	2.00	Total
I Would Recommend VPNs to My Organization	1.00	14	3	17
	2.00	2	34	36
Total		16	37	53

Table 7

Chi Square Tests for Hypothesis Two

	Value	df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	32.315(b)	1	.000		
Continuity Correction(a)	28.773	1	.000		
Likelihood Ratio	33.628	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	31.705	1	.000		
N of Valid Cases	53				

a Computed only for a 2x2 table
b 0 cells (.0%). have expected count less than 5. The minimum expected count is 5.13.

Since the p-value is .0000 which is less than 0.05, the null hypothesis was rejected. As a result, it can be concluded that an Information Technology Manager's decision to recommend Virtual Private Networks is dependent on his/her perception of the technology's value.

Hypothesis Three

Hypothesis Three stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perceived need for wide area networking. This hypothesis was evaluated by comparing responses to question ten with question 15 on the survey. Question ten is "My organization needs the ability to connect remote users to the corporate backbone"; question 15 is "I would feel comfortable recommending Virtual Private Networks in my Organization Rather than Using Traditional Wide Area Networks." Since a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* (coded as 1) and *less than strongly agree* (coded as 2).

Table 8

Crosstabulation for Hypothesis Three

		My Organization Needs the Ability to Connect Remote Users		
		1.00	2.00	Total
I Would Recommend VPNs to My Organization	1.00	14	3	17
	2.00	5	31	36
Total		19	34	53

Table 9

Chi Square Tests for Hypothesis Three

	Value	df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	23.535(b)	1	.000		
Continuity Correction(a)	20.652	1	.000		
Likelihood Ratio	24.314	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	23.091	1	.000		
N of Valid Cases	53				

a Computed only for a 2x2 table
b 0 cells (.0%). have expected count less than 5. The minimum expected count is 6.09.

Since the p-value is .0000 which is less than 0.05, the null hypothesis was rejected for both remote users and remote sites. As a result, it can be concluded that an Information Technology Manager's decision to recommend Virtual Private Networks is dependent on his/her perceived need for remote user and remote site access.

Hypothesis Four

Hypothesis Four stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perception of its reliability. This hypothesis was evaluated by comparing responses to question 12 and question 15 on the survey. Question 12 is "Virtual Private Networks are inherently reliable"; question 15 is "I would feel comfortable recommending Virtual Private Networks in my Organization Rather than Using Traditional Wide Area Networks." Since a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* (coded as 1) and *less than strongly agree* (coded as 2).

Table 10

Crosstabulation for Hypothesis Four

		VPNs Are Reliable		
		1.00	2.00	Total
I Would Recommend VPNs to My Organization	1.00	14	3	17
	2.00	4	32	36
Total		18	35	53

Table 11

Chi Square Tests for Hypothesis Four

	Value	df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	26.131(b)	1	.000		
Continuity Correction(a)	23.051	1	.000		
Likelihood Ratio	26.963	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	25.638	1	.000		
N of Valid Cases	53				

a Computed only for a 2x2 table

b 0 cells (.0%). have expected count less than 5. The minimum expected count is 5.77.

Since the p-value is .0000, which is less than 0.05, the null hypothesis was rejected. As a result, it can be concluded that an Information Technology Manager's decision to recommend Virtual Private Networks is dependent on his/her perceived reliability of the technology.

The survey included questions that were gathered for further research. The basis for the study was to determine what factors influence manager's decisions to recommend or not recommend technology regardless of their company size or their previous experience. The suggestions for further research section in Chapter 5address the possibility of reexamining the data to determine if demographics change the results of the survey.

Representation of Population

According to the California Labor Market data provided by the California Employment Development Department (http://www.edd.ca.gov), approximately 63% of businesses in California have fewer than 200 employees, 15% have 200 to 500 employees, and 22% have over 500 employees. A Chi Square Goodness of Fit test reveals no significant difference between the distribution of company sizes in the sample versus the population; refer to table 12 and figure 1.

Table 12

Size of Company

Number of users

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 to 199	23	43.4	46.9	46.9
	200 to 500	7	13.2	14.3	61.2
	500 to 2000	17	32.1	34.7	95.9
	Other	2	3.8	4.1	100.0
	Total	49	92.5	100.0	
Missing	99.00	4	7.5		
Total		53	100.0		

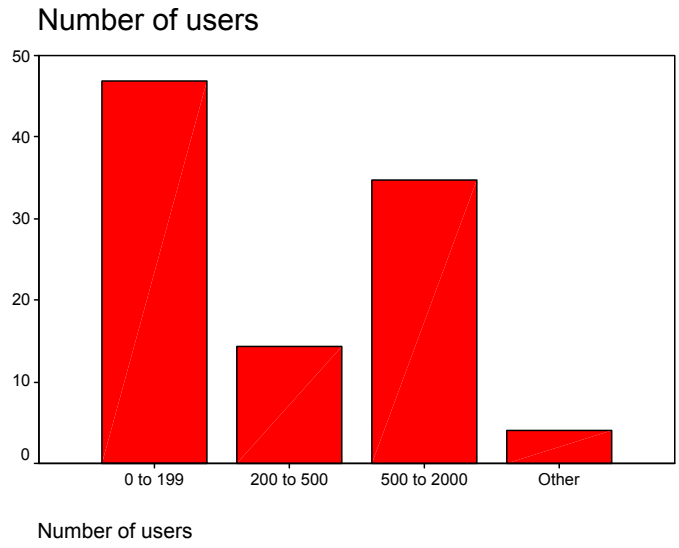


Figure 1

Size of Company (Chart)

Crosstabulation analysis on the number of users the manager supports and their willingness to recommend the technology provided results indicating that those supporting smaller companies were less likely to recommend the technology than those supporting larger companies. Refer to table 13 for the crosstabulation analysis.

Table 13

Number of Users and Recommendation Crosstabulation

			I would recommend VPNs		Total
			1.00	2.00	
Number of users	0 to 199	Count	3	14	17
		% within Number of users	17.6%	82.4%	100.0%
	200 to 500	Count	4	1	5
		% within Number of users	80.0%	20.0%	100.0%
	500 to 2000	Count	7	7	14
		% within Number of users	50.0%	50.0%	100.0%
	Other	Count	2		2
		% within Number of users	100.0%		100.0%
Total		Count	16	22	38
		% within Number of users	42.1%	57.9%	100.0%

From the researcher's experience, the distribution of titles in the sample are representative of the population. Companies generally have fewer Vice Presidents and CIOs than IT Directors and Managers. 40.7% of the respondents hold the title of IT Manager, IT Director, VP of IT, or Chief Information Officer. Fifty One percent claimed to hold a title of “other than listed”. These may include other managers, including consulting management, Chief Technology Officer’s, Chief Security Officer’s, and network architect managers. Table 14 and figure 2 depict the responses to the variable title.

Table 14

Title

My title is

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IT Manager	8	15.1	16.3	16.3
	IT Director	8	15.1	16.3	32.7
	VP of IT	1	1.9	2.0	34.7
	CIO	3	5.7	6.1	40.8
	Other	25	47.2	51.0	91.8
	NonIT	4	7.5	8.2	100.0
	Total	49	92.5	100.0	
Missing	99.00	4	7.5		
Total		53	100.0		

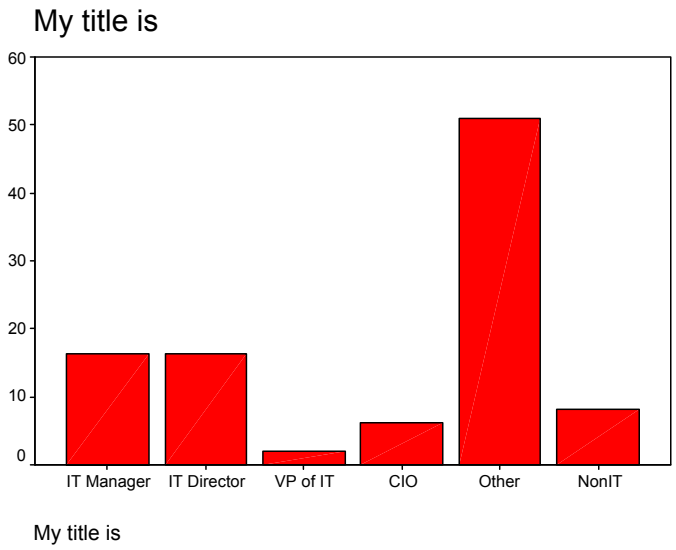


Figure 2

Title (Chart)

An analysis using cross-tabulation by title and recommendation show that seven out of eight IT directors strongly agreed to recommend VPNs, but no other title had a majority in the *strongly agree* category. Table 15 displays the results of this analysis.

Table 15

Title and Recommendation Crosstabulation

			I would recommend VPNs		
			1.00	2.00	Total
My title is	IT Manager	Count	2	3	5
		% within My title is	40.0%	60.0%	100.0%
	IT Director	Count	7	1	8
		% within My title is	87.5%	12.5%	100.0%
	VP of IT	Count	1		1
		% within My title is	100.0%		100.0%
	CIO	Count		3	3
		% within My title is		100.0%	100.0%
	Other	Count	6	12	18
		% within My title is	33.3%	66.7%	100.0%
	NonIT	Count		3	3
		% within My title is		100.0%	100.0%
Total		Count	16	22	38
		% within My title is	42.1%	57.9%	100.0%

The individuals responding to the survey were divided with regard to their experience implementing Virtual Private Networks. Approximately 46% of the respondents had experience implementing the solution. Approximately 43% did not have experience with the technology. Approximately 8% were in the process of implementing. Refer to table 16 and figure 3 for the analysis.

Table 16

Experience

I have used VPNs to connect corporate offices

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	23	43.4	46.9	46.9
	No	22	41.5	44.9	91.8
	In process	4	7.5	8.2	100.0
	Total	49	92.5	100.0	
Missing	99.00	4	7.5		
Total		53	100.0		

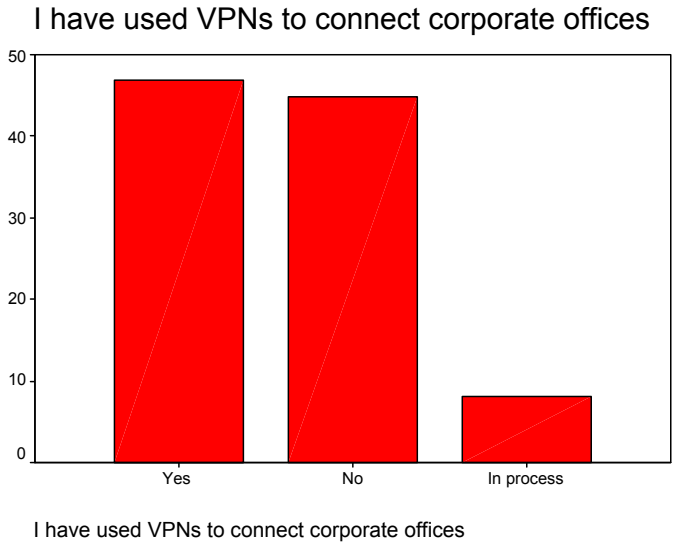


Figure 3

Experience (Chart)

CHAPTER 5. RESULTS, CONCLUSIONS, AND RECOMMENDATIONS

This chapter will explore results, conclusions and recommendations for further study on Virtual Private Networks and related topics. The research questions studied focus on the relationship between perceptions of Virtual Private Networks and managers' decisions to recommend their use. Specifically, the topics of cost-benefit, security, reliability and need were measured as independent variables on the decision to recommend the technology. Questions investigated in this study were: (a). Is an Information Technology manager's decision to recommend Virtual Private Networks independent of his / her perception of its security? (b). Is an Information Technology manager's decision to recommend Virtual Private Networks independent of his / her desire to save money in communications costs? (c). Is an Information Technology manager's decision to recommend Virtual Private Networks independent of his / her perceived need for wide area networking? (d). Is an Information Technology manager's decision to recommend Virtual Private Networks independent of his / her perception of its reliability?

The study focused on contributing factors to managers' choice to recommend technologies. The study will help decision makers determine what components of Virtual Private Networks are still of concern to other professionals, and may provide vendors with data to help them determine what is important to their customer base. Most importantly, it will help decision makers develop the right solutions for their organizations.

Perceptions of technology, its reliability and use in organizations, and in today's marketplace the security of the product are paramount to a decision to use it in a business. Information Technology professionals and executives are doing what they can to maximize their

returns; this is becoming increasingly so in Information Technology where cost-benefit analyses are becoming a part of a manager's everyday terminology. In the technology booms, companies were often adopting technology and finding out after implementation whether it was of value. Those days are gone, and managers are required to do the same analysis other business sectors were forced to do for years. For that reason, the study of technology and its factors for decision-making are increasingly important. Often in the technology field, the benefits and costs of solutions can be difficult to define strictly with numbers, leaving intangible benefits and the perceptions of technologies in industry holding more weight than in the past. It can be difficult to quantify the real dollar benefit of, say, an Operating System upgrade. However, it can be identified with intangible benefit analysis, such as reduced support costs and increased reliability. This study helped to focus on the intangibles that help determine whether an IT professional will choose to use Virtual Private Network technology.

Hypotheses

Hypothesis One

Hypothesis One stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perception of its security. The Chi Square Test of Independence resulted in the researcher rejecting the null hypothesis and concluding that the decision to recommend is dependent on the perception of security.

Hypothesis Two

Hypothesis Two stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her desire to save money in communications costs. The Chi Square Test of Independence resulted in the researcher rejecting

the null hypothesis and concluding that the decision to recommend is dependent on the desire to save money.

Hypothesis Three

Hypothesis Three stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perceived need for wide area networking. The Chi Square Test of Independence resulted in the researcher rejecting the null hypothesis and concluding that the decision to recommend is dependent on the perceived need for wide area networking.

Hypothesis Four

Hypothesis Four stated (null): An Information Technology manager's decision to recommend Virtual Private Networks is independent of his / her perception of its reliability. The Chi Square Test of Independence resulted in the researcher rejecting the null hypothesis and concluding that the decision to recommend is dependent on the perception of reliability.

All of the factors contributed to a manager's willingness to suggest the use of VPNs in their organizations.

Design

The research population for this study consisted of IT Management Professionals in all size businesses with a wide range of experience and user base. The first section of the survey was designed to evaluate the manager's perception of Virtual Private Networks as they relate to security. The second section referred to the respondent's perception of Virtual Private Networks as they relate to their cost versus benefit. The third section referred to the need for Wide Area Networking. The fourth section provided a perspective of the respondent's view of reliability of

the technology. The fifth section provided an understanding of the respondent's general attitude toward Virtual Private Networks. The last section identified demographics and asked open-ended questions with regard to the individual's perceptions of the technology for further research. A five-point Likert scale was used for sections one through five.

IT Professionals were asked to participate voluntarily in the study by following a web-link in e-mail. Alternatively, respondents could both download a copy of the survey in a multi-word-processor format from the web and e-mail it to the researcher, or they could use the file attached to the e-mail for convenience and send that to the researcher. 95% of the respondents chose to take the survey over the web and the results were anonymously collected and sent to the researcher for manual entry into SPSS. Results submitted by the 5% e-mailing the survey were also manually inputted into SPSS for analysis.

Conclusions

The results of the Chi Square tests performed supported four of the four hypotheses. The results also made intuitive sense, as security and reliability are have become increasingly important topics in Information Technology literature.

These findings help to understand the factors surrounding the willingness of managers to recommend the technology. It shows that there are multiple reasons an individual may or may not recommend a solution, and both vendors and managers should be aware that technologies often require many benefits to be adopted. This implies that organizations require reliability, cost savings and security before solutions touching their core network from the outside will be recommended, a key into the future of technology growth and decision making for IT executives. Additional testing may be done to determine the impact that the size of the organization and

previous experience with the technology may have on the individual's willingness to recommend the solution. Companies with the number of users ranging from 200 or more recommended Virtual Private Networks far more often than those supporting less than 200 users. This may indicate that only bigger companies can afford the technology or have the expertise to make a decision as to whether or not it will provide solid return on the investment. Additionally, smaller companies may not have the in-house technical expertise or the budget to implement the technology, or may not have a need because they have fewer users than those running bigger organizations.

Title may also impact the manager's comfort, authority and desire to recommend or not recommend a technology based on the four criteria in the study. As indicated in the results section of this paper, management level staff with an IT Director title was the only groups to strongly recommend Virtual Private Networks a majority of the time. The study indicates that many factors play a role in decision-making; further study could indicate which factor plays more of a role than others.

It can be concluded that technology managers evaluate technology based on many criteria, and that before funding projects executives are requiring substantial research and information related to the benefit of the solution, the cost and its return, the security of solutions and the reliability when technology is so critical to companies.

The survey provided respondents with a chance to further explain their selections and to explain any of their concerns, suggestions or general information about the technology. Several managers that appeared to work in the healthcare industry responded to the survey, indicating that they were using the Virtual Private Network in their company to provide physicians with

after-hours access to patient information stored online, indicating the ability of the technology to make a solid contribution to quality of service for customers. There were four comments indicating that the Virtual Private Networks implemented already were stable and very reliable, an important part of the business. Based on the information provided by respondents, companies are using this technology to accommodate traveling employees and are using it to connect remote users frequently. Five respondents mentioned this as a core benefit to the solution. Respondents felt compelled to mention their solution of choice when they had positive comments about the technology, consistently mentioning Shiva's LANRover product. Seven respondents noted that to be successful, the solution must be integrated with Intrusion Detect Systems, Anti-Virus solutions, Spam Control, Access Logging, Security and Encryption. Six respondents mentioned that Virtual Private Networks are "the wave of the future" and that traditional methods, such as frame relay, "are dead". Five respondents commented that the solution must be properly implemented to minimize installation problems and inconsistencies.

Common threads among respondents indicate that implementation method is a key element to both choosing and installing a Virtual Private Network. Another common theme was the use of security and encryption to maintain access control and prevent breaches in security. Respondents also felt that Virtual Private Networks would be the clear mechanism for allowing remote site and user access into a corporate backbone, and that the networks were providing significant value to their organizations. With this information, it is easy to conclude that Wide Area Networks using traditional connectivity means are being replaced with this newer, secure, encrypted, reliable and cost-effective solution.

Suggestions for Further Research

There are several fascinating topics that can come from this study. A similar study may be done that changes the approach of the survey to increase response rate. Given the relatively low response rate that comes with web-based surveys, it might prove insightful to conduct live surveys at professional conferences with IT managers. While the results will probably be similar overall, the open-ended comments may add valuable insight since the attendees would be from different companies and there would be no reason to suspect bias. Additional research may be done on the existing data set to find the impact company size and prior use of the technology has on decision-making. It may be revised to fit other technologies or solutions as a whole, or may be revisited to understand the most significant predictor of the willingness of management to recommend the solution.

Security is an important topic with continually increasing virus threats and breaches keeping Information Technology professionals up at night. A researcher may choose to explore the individual components of security, such as the encryption and authentication methods used and which type of each is considered safest. Also related to security, facts on security compromises of various technologies would be an interesting topic of study. The study of security breaches in Virtual Private Networks as they relate to banking and healthcare (both places where privacy is critical) may provide insight into what works, what does not, what consumers can count on, and what provides the best cost-benefit for organizations.

Researchers may choose to study the true reliability of hardware and software as a single working component; finding what companies can really count on as opposed to just manufacturers' mean-time-between-failure (MTBF) statistics. Researchers may explore whether

MTBF is really an accurate measure of what businesses see in hardware and software failure, and might explore what combination of the two is most reliable. This suggests a study in partner testing, such as software developers testing their software on a particular hardware platform, may also uncover interesting results.

There are several topics related to cost-benefit of Information Technology that an economic-minded researcher may wish to explore. Do companies post-test their cost-benefit assumptions and do a gap analysis? Are variances widely tolerated in Information Technology? How can IT professionals make their recommendations and financial analysis most accurate? How important are the Chief Financial Officer's opinions of technology or do IT professionals ultimately have the final say in most organizations? Research may also be done to find out how smaller companies compare in their IT spending to independent variables, such as the number of users or their profitability.

Finally, researchers may wish to explore the use of traditional Wide Area Networks and the options to centralization. In technology, we often see a migration to centralization, decentralization, and back again. Uncovering the true value of each in a financial model may help IT professional's stay with one model for a while.

REFERENCES

Angoff, W. H. (1988). Validity: An evolving concept. In H. Wainer & H. I. Braun (Eds.), *Test validity*. Hillsdale, NJ: Lawrence Erlbaum.

Avolio, Frederick. (2003). Firewalls and Virtual Private Networks. Sprint. Retrieved May 3, 2003, from http://www.spirit.com/CSI/Papers/fw+vpns.html.

Bocij, P., Chaffey, D., Greasley, A., & Hickie, S. (1999). *Business Information Systems*, Financial Times Pitman Publishing.

Business Communications Review. (2003). 33/6, 1-4.

CNN. (2003). Teen hacked TD Waterhouse Account. Retrieved October 9, 2003, from http://www.cnn.com.

Cisco Systems. (2003). White Paper on Security. Retrieved May 15, 2003, from http://www.cisco.com .

Cooper, D. R., & Schindler, P.S. (2003). *Business research methods.* Boston, MA: McGraw-Hill Irwin.

Corporate Technology Information Services, Inc. (1997). *Corporate Technology Directory 1997*. Rev. 12.3. Wellesley Hills, MA.

Cronbach, L. J. (1971). Test validation. In R. L. Thorndike (Ed.). *Educational Measurement (2nd Ed.).* Washington, D. C.: American Council on Education.

Dash, J. (2000). Health Care Industry Looks at Security Risks. [Electronic Version]. *Computer World, Aug. 14 2000.* Retrieved September 20, 2003, from http://www.computerworld.com.

Davoine, F., & Li, H., & Forchheimer, R. (1997). Video compression and person authentication in Audio- and Video-based Biometric Person Authentication, J. Bigun, G. Chollet, and G. Borgefors, eds., Springer, Berlin, pp. 353-360, 1997.

Ferguson, P., & Huston, G. (1998). What is a VPN?, *The Internet Protocol Journal*, 1, 1-2.

Freesoft.Org. (2003). *An Internet Encyclopedia: LANs and WANs*. Retrieved October 3, 2003, from http://www.freesoft.org/CIE/Topics/13.htm

Fu, Z., Wu, F., Huang, H., Loh, K., Gong, F. Baldine, I., et al. (2001). IPSec/VPN Security Policy: Correctness, Conflict Detection, and Resolution Policy 2001, *LNCS, 3956.*

Fu, Z., & Wu, S. (2001). Automatic Generation of IPSec/VPN Security Policies In an Intra-Domain Environment, *LNCS.*

Gartner Group. (2002). Securing Public WLANs: VPNs will not solve everything. Retrieved September 2, 2002, from http://www.gartner.com.

Gilbert, D., Aparicio, M., Atkinson, B., Brad, S., Ciccarino, J., Grosof, B., & et al. (1996). The Role of Intelligent Agents in the Information Infrastructure. Technical Report, IBM Corporation, Research Triangle Park, NC.

Green, J.H (2001). *The Irwin Handbook of Telecommunications Management.* New York: McGraw Hill.

Greenberg, E., & McLaughlin, C. (2001). Eliminate Security Risks: *PC Magazine*. Retrieved October 30, 2003, from http://www.pcmagazine.com.

Hu, J. (1998). AOL volunteer list hacked. C|Net News. Retrieved October 2, 2003 from http://www.msn.com.

Hussman, H., Mamias, G., Venieris, I., Prehofer, C., & Salsano, S. (2000). Implementing Integrated and Differentiated Services for the Internet with ATM Networks: A Practical Approach. *IEEE Journal.*

Huttunen, A. (2003). UDP Encapsulation of IPsec Packets. Retrieved January 10, 2004 from http://www.microsoft.com.

International Standards Organization Technical Information. (2003). Retrieved October 1, 2003, from http://www.iso.org.

International Telecommunications Union. (2002). Retrieved October 1, 2003, from http://www.itu.int/home/.

Internet Engineering Task Force (IETF). (2003). Retrieved October 1, 2003, from http://www.ietf.org/.

Institute for Electrical and Electronic Engineers. (2003). Retrieved October 1, 2003, from http://www.ieee.org/portal/index.jsp.

Internetweek. (2003). Retrieved May 17, 2003, from http://www.internetwk.com/VPN/default.html.

Jackson, L. (1998). Watch Your WAN. *Network World*. Retrieved December 22, 2003 from http://www.networkworld.com.

Jungle Computers. (2003). Retrieved October 4, 2003, from http://Jungle-computers.co.uk.

Johnson, J. (2003). In search of elusive telco cost savings. *Network World.* Retrieved December 20, 2003 from http://www.networkworld.com.

Lacity, M., & Jansen, M. A,. (1994). Understanding qualitative data: A framework of text analysis methods. *Journal of Management Information System*, 11, 137-160.

Kalanidhi, S. (2001). Value Creation in a Network: The Role of Pricing and Revenue Optimization and Enterprise Profit Optimization. *Information Systems Frontiers* 3:4, p. 465-470.

Khalil, I., & Braun, T. (2002). Edge Provisioning and fairness in vpn-diffserv networks. *Journal of Network and Systems Management*, 10(1), 11-38

Legard, David. Study on VPN, firewall. *IT World.* Retrieved May 3, 2003, from http://www.itworld.com/Sec/2211/021120vpnfirewallsales/.

Lupu, E., & Sloman, M. (1997). Conflict analysis for management policies 1997. *Proceedings of the 5th IFIP/IEEE International Symposium on Integrated Network Management IM'97*, San Diego, CA.

McKenna, S., Gong, S., Wurtz, R., Tanner, J., & Banin, D. (1997). Tracking facial feature points with gabor wavelets and shape models. In *Proceedings of the First International Conference on Audio- and Video-based Biometric Person Authentication Crans*, Montana & Switzerland, 12-14 March 1997.

Messick, S. (1998). Test validity: A matter of consequence! [Electronic version]. *Social Indicators Research,* 45, 35-44.

Meyer, M., & Que, R. (1998). Computers Today and Tomorrow. Retrieved September 30, 2003, from http://www.mis.boun.edu.tr/ulus/ibs511/notlar/lans.htm.

Microsoft. (2003). Retrieved April 23, 2003 from http://www.microsoft.com.

Mohan, S. (1999) Tunnel Visions. *CIO Journal*. 6, 1-5.

Moss, P. A. (1994). Can there be validity without reliability? *Educational Researcher*, 23, 5-12.

Murphy, I. (2002). Planning is the Key to Successful VPNs: *VNUNet.* Retrieved October 5, 2003 from http://www.vnunet.org.

Narin, F., & Hamilton, K., & Olivastro, D. (1997). The Increasing Linkage Between U.S. Technology and Public Science. *Research Policy,* 26: 317-30.

Needham, R., & Schroeder, M. (2001). Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12): 993-999.

Phifer, L. (2002). Virtual Private Networks. *Internet Journal. 6, 22-40.*

Pigeon, S., & Vandendorpe, L. (1998). Multiple experts for robust face authentication. *SPIE Optical security and counterfeit deterrence II*, 3314, 166-177.

Resnick, M. (1996). Beyond the centralized mindset. *Journal of the Learning Sciences, 5*(1)., 1-22.

Reuters. (2003). Retrieved February 11, 2003, from http://www.reuters.com.

Salamone, S. (1998). Products Promise To Boost VPN Services. *Information Week, 5/98.*

Sandoval, G. (2002). War on Cybercrime – We're losing. C|Net News. Retrieved on May 14, 2003, from http://www.cnet.com.

Schneider, P. (1999). The Bargain Hunter's Guide to Global Networking. *CIO Journal*. 7, 22-31.

Schoonmaker, J. (2003). Three steps CIOs should take to protect corporate data. Retrieved September 23, 2003, from http://www.cio.com.

SearchDomino. (2003). Retrieved October 5, 2003 from http://www.searchdomino.com.

Senevirathne, T., Sikdar, S., & Premmaraju, N. (2001). Ethernet Over IP - A Layer 2 VPN Solution using Generic Routing Encapsulation (GRE). *Internet Journal.* 7/01, 70-88.

Sha, G. & Micali. S. (1984). Probabilistic encryption. *Journal of Computer Security*, 28, 270-299.

Shiva. (2003). Virtual private networks white paper. Retrieved April 23, 2003, from http://www.intel.com.

Southgate, D. (2002). User policies are good first step in minimizing security risks. *CIO.* 10/16 1-2.

Spohn, D.L., Brown, T., & Grau, S. (2002). *Data network design*. New York: McGraw Hill.

Sun Microsystems. (1999). White Paper. Retrieved April 30, 2003, from http://www.sunmicrosystems.com.

Suneby, P. (1999) Indus River Networks. Retrieved August 20, 2003 from http://www.msn.com.

Tankus, A., Yeshurun, H., & Intrator, N. (1997). Face detection by direct convexity estimation. In Proceedings of the First Intl. Conference on Audio- and Video-based Biometric Person Authentication, Springer, Crans-Montana, Switzerland, March 1997.

Tech Republic. (2003). Tech Republic Information Network. Retrieved October 30, 2003 from http://www.techrepublic.com.

Technology Review. (2003). *Journal of Technology Review*. Retrieved May 30, 2003, from http://www.capella.edu.

Thayer, R. (1997). Bulletproof IP. *Sable Technology*. 11/21, 1-10.

The Advantages of a VPN. (2003) Retrieved October 6, 2003, from http://findvpn.com/articles/benefits.php.

University of Montana. (2003). Retrieved October 1, 2003, from the Internet at http://www.hct.umontana.edu.

Veciana, G., Park, S., & Sang, A., & Weber, S. (2002). Routing and provisioning VPNs based on hose traffic models and/or constraints. University of Texas at Austin. 1-25.

VPN Consortium. (2003). VPN technologies: definitions and requirements: what about VPN security? Retrieved November 10, 2003, from http://www.informationweek.com.

Wide Area Networks. (2003). Digitus-Associates. Retrieved October 3, 2003 from http://www.digitus-associates.com/wan.html.

WAN Downtime and SLAs. (1998). Infonetics Research, San Jose: CA.

Web Host Industry Review, Inc. (2003). What is a Virtual Private Network? Retrieved February 1, 2004 from http://www.informationweek.com.

WebOpedia. (2003). Retrieved November 11, 2003, from http://www.webopedia.com.

Whatis.com (2003). Retrieved November 11, 2003, from http://www.whatis.com.

Xenakis, C., Gazis, E., & Merakos, L. (2002). Secure VPN Deployment in GPRS Mobile Network. *European Wireless*,1-15.

Yahoo Finance. (2002). Retrieved December 20, 2003 from http://finance.yahoo.com

Yin, R. (1994). Case study research. *Design Methods*. Thousand Oaks: Sage Publications.

Yun, J., and Ulrich, D.A. (2002). Estimating measurement validity: A tutorial [Electronic version]. *Adapted Physical Activity Quarterly*, 19, 32-47.

APPENDIX

This Virtual Private Network survey is designed to evaluate the perception of Virtual Private Networks among technology managers. Please make your views known by taking the time to complete this questionnaire.

While the questionnaire is anonymous, the demographic information is important to differentiate the views among managers. Completed surveys will be treated confidentially with results being reported only in summary.

Please indicate the most appropriate response for each question.

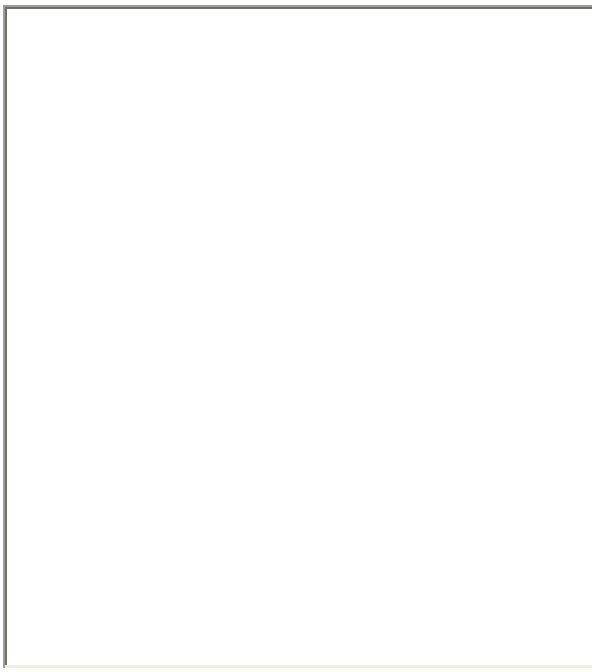
Security	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
1. I feel that Virtual Private Networks are secure.	☐	☐	☐	☐	☐
2. I am/would be concerned with the type of authentication Virtual Private Networks use when implementing them in my organization.	☐	☐	☐	☐	☐
3. I am/would be concerned with the encryption capabilities when implementing Virtual Private Networks at my organization.	☐	☐	☐	☐	☐
4. I am willing to use Virtual Private Networks to transfer sensitive information at my organization.	☐	☐	☐	☐	☐
5. Virtual Private Networks weren't secure three years ago.	☐	☐	☐	☐	☐
Cost-Benefit	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

6. Virtual Private Networks provide a good value for their costs.	☐	☐	☐	☐	☐
7. The cost of maintenance is lower with Virtual Private Networks than with traditional Wide Area Networking methods.	☐	☐	☐	☐	☐
8. I would consider Virtual Private Networks a considerable cost savings over traditional Wide Area Networks in my organization.	☐	☐	☐	☐	☐
Need for Wide Area Networking	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
9. My organization needs the ability to connect remote sites to the corporate backbone.	☐	☐	☐	☐	☐
10. My organization needs the ability to connect remote users to the corporate backbone.	☐	☐	☐	☐	☐
11. Wide Area Networks provide a significant benefit to my organization.	☐	☐	☐	☐	☐
Reliability	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
12. Virtual Private Networks are inherently reliable.	☐	☐	☐	☐	☐
13. The Internet is reliable enough to transfer time-sensitive data within my organization.	☐	☐	☐	☐	☐
14. Virtual Private Network hardware is	☐	☐	☐	☐	☐

reliable.					
General Information	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
15. I would feel comfortable recommending Virtual Private Networks in my organization rather than using traditional Wide Area Networks.	☐	☐	☐	☐	☐
16. I feel that Virtual Private Networks use proven technology.	☐	☐	☐	☐	☐

17. My experience implementing Virtual Private Networks or Wide Area Networks and their use in my organization has been:

20. My additional comments on benefits or concerns with Virtual Private Networks are:



21. My organization supports:

- ☐ 0 to 199 users
- ☐ 200 to 500 users
- ☐ 500 to 2000 users
- ☐ Other

22. I have implemented Virtual Private Network technology for remote user connectivity:

- ☐ Yes
- ☐ No
- ☐ In process

23. I have implemented Virtual Private Network technology for corporate office connectivity:

- ☐ Yes
- ☐ No
- ☐ In process

24. My Title is:

- ☐ IT Manager
- ☐ IT Director
- ☐ VP of IT
- ☐ CTO
- ☐ CIO
- ☐ Other IT _____
- ☐ Not IT