Socio-technical Impacts of Virtual Private Networks (VPN) and Telecommuting

Daniel Loewus-Deitch[1]

[1]University of California, Irvine, School of Information and Computer Science
444 Computer Science Bldg., Irvine, California 92697 USA
Email: dloewusd@ics.uci.edu

Abstract

Virtual Private Networks have become increasingly relevant in today's distributed corporate environment. Working remotely is now a viable option for many workers and it often holds many advantages for both the employees and the employers. This qualitative study is uniquely focused on the role that user practices and social processes play in the design of VPN systems. The research involved 7 in-depth, open interviews with employees from 3 different local technology companies. The subjects selected were either users of VPN technology or people directly involved in the administration and implementation of VPN solutions. The resulting data was systematically analyzed, using various techniques from Grounded Theory. This data was processed through 3 semi-overlapping stages: open coding, axial coding, and selective coding. Emergent themes were extracted and carefully categorized. This paper addresses the most important and relevant themes that were found in an attempt to provide new research directions and educated hypotheses for future studies.

Keywords

Virtual Private Networks, VPN, remote workers, Grounded Theory, Computer-Supported Collaborative Work, CSCW

Table of Contents

1. Introduction 2
   Purpose and Objective 2
   Current Debates 3
   Theoretical Frameworks 3
2. Qualitative Study of the Socio-technical Impacts of VPNs 3
   Research Methodology 3
   Research Design 4
3. Emergent Themes (Data Analysis) 5
   Contrasting VPN Implementation Policies 5
   Increasing Central Control and Security in the Home Environment 11
   Company Reliance on Home Internet Service Providers 13
4. Recommendations 13
   Security Compliance in Standard and Flexible Workplaces 13
   Integrating a VPN Client Into a Centralized Workstation System 14
   Are Consumer ISP Providers Truly Being Taken Advantage of by VPN-Enabled Companies? 14
5. Conclusions 14
6. References 15
   Virtual Private Network Technical Papers 15
   Qualitative Research Methodology 15
   General VPN Articles 15
7. Appendixes 17
   A. Interview Questions 17
   B. Coding Procedures 20
   C. Possible Quantitative Survey Tool 33

1. Introduction

Working remotely, away from the office, has become an increasingly popular trend at both large and small companies everywhere. The need to be mobile during work hours is nothing new though. Many employees from sales people to IT personnel to upper management executives must frequently travel and still have access to resources at the company. Communication channels between an individual employee and his "home base" are essential for various collaborations and up-to-the-date information. Over the years, cutting-edge technologies have played a large role in providing solutions for mobile workers. Conference calling, cell phones, dial-up networking, and most importantly, the internet, have helped increase productivity for corporations and presented them with unlimited possibilities for new growth and expansion. At the same time, these technologies have created new freedoms and flexibility for employees, leading to greater job satisfaction and allowing them to efficiently perform their required tasks in diverse, multiple environments.

One of the greatest breakthroughs in remote work technologies was the introduction of Virtual Private Networks (VPN). Taking full advantage of the increasingly available consumer high-speed, broadband internet service, VPNs provide a secure and reliable method of transferring data across a convenient internet medium. Through various protocols and authentication methods, VPNs construct an encrypted tunnel between the remote client and the company intranet. The internet has long been useful for sending electronic mail, and transferring various types of files (i.e. FTP), but because of its unsecure, anonymous, and unreliable nature, it was obviously a bad idea for a company to simply open up its network to the internet. VPN provides a much more lucrative solution, by setting up tightly-controlled entry paths into a company's intranet. Essentially, this allows companies to extend their local area networks (LANs) indefinitely, all with minimal cost and hardware infrastructure requirements. With the savings that VPN technologies can deliver, companies can now afford to provide this convenient, productive tool to anyone who has a genuine need for it. VPN certainly was a powerful technological response to a tremendous social work need, but as with any solution, it also has generated new issues of its own. It is for this very reason that VPN provides a perfect vehicle in which to study the relationship between social processes and their impacts on technology.

Purpose and Objective

The purpose of this paper is to explore the issues involved with VPN technology and telecommuting. I gathered field data from the people directly involved with this technology, both on the management and user side, in order to fully understand the processes in such an implementation. The purpose of this study was to discover key issues that still currently need to be solved, as well as potential hidden anecdotes for these emergent problems. This study is designed to generate fresh approaches and ideas for future focused research.

The following analysis is based exclusively on interview data collected from three different companies and seven different subjects. Tailored questions were asked, depending on whether the subject was on the management or user side. Although, it quickly became clear that the IT management subjects were also avid users of VPN themselves, and therefore were able to provide valuable data in user experience as well. The following research questions guide the path and scope of this study:

- How is VPN currently being implemented in various companies? What protocols, authentication methods, and other components are being used?
- What are the company policies regarding telecommuting and VPN use?
- Who is using this technology, and to what extent?

- What are the users and IT managers experiences with this emerging VPN technology?
- What are the prevalent issues that affect security, cost, and usability?
- Is VPN technology truly increasing productivity and usage advantages for companies and their remote employees?
- What further solutions might be developed from resources that are already available to the company?

Current Debates

From the literature, it is clear that the most widely used VPN protocol, PPTP (Point-to-Point Tunneling), is also considered to be the most significant security risk. This Microsoft protocol simply does not provide strong enough encryption or authentication methods, which leaves companies vulnerable to various attacks. Many companies are now transitioning away from PPTP towards a more powerful solution. Some are looking at using Microsoft's new incarnation, L2TP, while many more are ditching Microsoft's integrated OS solutions altogether, and instead looking at independent clients that utilize the non-proprietary IPSec protocol. Another large area of concern, for those in charge of security, is the VPN user's home environment. IT personnel do not have a great deal of control over remote clients, like they do on their own company computers which are centrally controlled and behind numerous industrial-strength firewalls. This has left many companies scrambling to maintain security and protection on their networks, while at the same time extending these networks into virtual unknown territory. Other debates range over who should be allowed VPN access, the effects of telecommuting on corporate cultures, and the viability of CSCW collaborative applications over VPN.

Theoretical Frameworks

In the search for survey resources, I quickly discovered that most studies out there focus on the effect of technology on its users and their reactions. They look at how well people adapt to these technologies, how often they use them, and how various work processes much be modified to fit into the new technology's design model. I decided it would be interesting and potentially more useful to reverse the focus of this relationship and look at the effects of users and social processes on technology design. I wanted to look at what sort of catalysts spark changes in the implementation and what possible technology solution ideas may be inherently hidden in the social processes and user experiences. Could it be that the company already has certain tools that it is not taking full advantage of?

2. Qualitative Study of the Socio-technical Impacts of VPNs

Research Methodology

As mentioned earlier, the goal of this study is to look both at current corporate VPN solutions and at user practices to discover relationships and patterns. The hope is that such relationships will lead to a better focus of research and eventually provide realistic solutions to various telecommuting challenges, which are prevalent in these companies. I felt the best way to uncover these issues was to go out in the field and get first hand accounts of the processes involved in implementing and using VPN technology.

This study utilizes the grounded theory approach (Strauss & Corbin, 1998), which is a qualitative research method, designed to generate theory from interpretations of raw field data. Following the grounded theory template, I begin the study with no preconceived

theories. I started merely with the general research questions that I mentioned in the introduction. These questions guided the design of my interview questionnaires, which can be found in Appendix A.

I used grounded theory because it allows researchers to generate theory that is deeply grounded in the data. This makes my conjectures more likely to reflect reality and it provides me with useful, solution-oriented hypotheses to later test in standard quantitative studies.

My fieldwork generated over 50 pages of typed interview transcripts. These interviews were conducted at the companies, using the *long interview* method (McCracken, 1988). This method consists of asking probing questions to initiate open discussion that I hope will provide me with answers to my research questions. With this method, one must be careful not to question in a suggestive manner, because this may result in contaminated data.

All the data was analyzed using systematic procedures from grounded theory. These procedures provide standardization and rigor to our analysis. The analysis was done in three semi-overlapping stages: open coding, axial coding, and selective coding. Examples of these first two stages can be found in Appendix B. In open coding, one first searches for segments in the data that appear to provide some answers to our research questions. These segments are then broken down into discrete parts, examined, and compared. You search for similarities and differences and eventually organize these parts into various categories. In axial coding, one begins to link these categories to each other. You identify main and sub categories, and organize everything respectively. In the final stage, selective coding, one develops a central theme which ties together all of our categories. While producing this "storyline" or "plot," you continue to modify the categories and their contents to strengthen the relationships between them. The ultimate goal is to formulate accurate explanations of phenomena, based solely on the data, so that you can have enough understanding to generate relevant and plausible theory.

Research Design

All analysis in this study was based on in-depth interviews conducted at local technology companies, although I also gathered a few facts from informational websites inside the corporate networks. Two of these companies were large international corporations (QC and UNS), and one was a small Internet start-up (CSN). Only the two large companies currently had a VPN solution in place. The small company was still in the process of planning its VPN implementation. There were seven interviews. Five were employees involved in IT and network management, and two were frequent telecommuters, who used the VPN technology to connect to work on a regular basis. One set of questions was used for the IT managers, and one set of questions was used for the VPN users. The former focused on more technical aspects of the company's VPN implementation, while the latter focused on the employee's experiences using the technology every day. The purpose of the next section of our paper is to focus on the key themes that have emerged in our analysis of this field data.

3. Emergent Themes (Data Analysis)

Contrasting VPN Implementation Policies

This category involves various aspects and points of view that affect VPN implementation. It includes some contrasting philosophies about levels of standardization, broadness of support, authentication solutions, and who should be granted VPN accounts.

- **Flexible vs. Standardized Approach**

When comparing the two large companies, a fundamental contrast emerged that governs the way each company planned and implemented their VPN solutions. QC maintained that flexibility among software, operating systems, and connection methods was important to consider when providing telecommuting services to their employees.
JF says, at the beginning,

> "Any technology or application that empowers the employees is going to be very important on our list of things to support…The company tries to be as flexible as possible."

UNS, on the other hand, has a different approach. They feel that their employees should conform to certain standards, because this is more cost-effective and manageable for the company. Furthermore, this company likes to do things in its own personalized, specific way.
DT alludes to this company mindset,

> "…it will all stay in-house. Being a development type company, they keep a lot of the stuff in-house. What UNS does is they do partnerships and mess with the code to create our own product."

These general philosophies hold with varying degree across different aspects of implementation. Such aspects are described below.

Pros and cons of these two differing approaches:

QC clearly shows its commitment to varying platforms and environments in its provision of multiple protocols and methods for VPN. Although they hope to eventually phase it out, PPTP accounts are still granted in certain cases where the OS or various software applications are not compatible with the Cisco VPN client that is generally used.
JF states,

> "We're fairly agnostic about what we pursue, as long as it gives us the flexibility for different OS's amongst different VPN users. "

This type of policy obviously makes it easy for any user, regardless of their home system setup, to connect to the company, but it also has the potential to cause headaches for IT staff, trying to manage multiple types of remote access to the company. Furthermore, these multiple options have created an insecure environment, because some of the options "do not support an acceptable level of encryption or authentication" (internal VPN website). It is true that a system is only as strong as its weakest link. Once the company feels it can provide one solution that will adequately work on most systems, they will narrow everything down to a single IPSec based method. Still it is clear that their ultimate priorities remain in scalability.

As stated earlier, UNS likes to use partnered applications that allow them access to the code, so that they may configure and tailor it to their own specific needs. They prefer to provide one solution to all telecommuting employees, with the apparent belief that users interested in working remotely will be willing to make the necessary modifications on their system so that they can comply with company standards. Such an arrangement works well from an IT standpoint, but it does take away some choice and freedom away from the user:

> "For instance, if someone calls me and says 'I just loaded XP on my machine and now I'm having all these problems,' well, I'm going to have to say sorry, but we can't help you…Corporate tests all that and fixes it before making it an official (supported) standard for the company."(DT)

OS and software support is a tough issue to address as well, when considering standardization possibilities. It is compounded when people don't keep their system updated with the latest service packs and security patches. UNS only supports Microsoft OS's ('98 and higher), but they strongly recommend Windows 2000. They also give strict mandates on firewall and anti-virus software. These security applications are provided directly by the company to all remote users:

> "We also have what we call standard desktop software, a list of software we use at UNS. The reason they do that is so that they can control the way problems are handled. They can control security. For instance, our standard here at UNS right now is Windows 2000 (Service Pack 2), Office Suite 2000 (Service Pack 2), and Norton Anti-Virus 7.51, which is the corporate edition that we use here…Now that we've partnered with Symantec, they provide us with anti-virus and firewall software which is mandatory for people working from home."(DT)

There are certainly good reasons for these requirements. A technically proficient user shares his sentiments about using VPN on older Windows systems, stating,

> "Window 2000 is a good product. Window 98 is not stable. If you want a stable product and a faster connection, you should go with Windows 2000 Professional."

QC takes a very lenient stance on OS and software choices. They work hard to accommodate for all major operating systems and, although they strongly recommend anti-virus and firewall protection, they don't expect a user to use one particular standard. McAfee anti-virus and BlackIce firewall are available for download on the company intranet, but others can be used, if a user so desires. According to JF, "There's a very large Unix community here at QC." Apple computers are also scattered across certain departments. The company recognizes this diversity, and chooses to do everything in its power to accommodate for this technological variance. After "extensive trials", QC chose a VPN client from Cisco that is compatible on multiple OS's, including Macintosh, Linux, and Solaris (internal VPN website). For OS's that happen to not be supported quite yet by this client (i.e. Windows XP), PPTP accounts are still available. In this way, QC exemplifies its philosophy again. The attitude is that the user should use the system that they are comfortable with, and the company will extend the appropriate resources to accommodate the user in his preferred environment. Obviously this approach comes with additional costs, but QC seems to believe the investment is worth it.

Both companies recognize the need to hold onto legacy equipment for people who don't have access to broadband service in their areas. Dial-up resources have been significantly scaled back, but they are still present. In this way, the companies have definitely had to maintain flexibility. These provisions also pose security problems though.
In discussing dial-up solutions, DT said,

> "We started using dial-up networking and what happened was we had a lot of problems with security. That was the biggest thing because dial-up networking was a client that

could only be configured so much. It was included in the operating system. It wasn't really designed for what VPN servers can now do. You put a lot of security inside the client"

On the other hand, at times, this aging solution is still sometimes useful. Although inherently slow, CL points out that there are instances where dial-up is much more cost-effective:

"There is a system here in Mission that you can dial into the local number and it's actually cheaper for the people and the company, for local people to dial the remote access box than to go to VPN."

In any case, it is apparent that dial-up remote access is not going to be entirely phased out until everyone can get affordable broadband service on their home or mobile computer.

Origins of each company's approach:

There appears to be a relationship between certain trends in the company's atmosphere and the type of approach that is taken (flexible or standards-based). At UNS, CL declares his company as "first wave" and a "first adopter of technology." He also acknowledges, "We were an early adopter and there was no track record as far as how secure the VPN box would be." According to CL, this pioneering stance taken by the company tends to increase security concerns, which therefore presents more of a need for standards and tighter control of users.

At QC, JF also describes the relationship between corporate culture (trends) and implementation approaches:

"I think really a corporation's culture drives what technology their using. So, certainly the culture at QC, being a very collaborative, very open atmosphere, you know, has forced several moves in the technology, or several ways of adapting the technology to adapt to that culture. I think that this is really the way it works. The technology we use is just enabling the corporation to continue doing what's it's done…"

JF talks about the origin of their flexible approach, and why it is important to provide multiple options in a company such as QC. Later, JF provides further justification for their flexible approach by discussing his thoughts on security, with a surprising twist:

"The key to encouraging an employee to do the right thing is developing the ease-of-use thing. If the methodology that you put, is very easy to implement, they are much more likely to comply with the policy… As soon as you offer a single solution, then we notice things will began breaking down. As soon as you don't give the flexibility choice to the user, they're going to do what they can to…I wouldn't necessarily call it exploiting the situation, but they are going to do whatever they can to simply their life. So, as soon as you start taking away options, then it probably weakens your security."

This was a very interesting set of statements because it thoroughly goes against common beliefs about security strategies. UNS and most others tend to think that successful security can be achieved only by tightly bound standards and limited choices. JF's thoughts were a drastic departure from this commonly held philosophy. It would certainly be advantageous to perform a study that tests these claims, by comparing the security compliance of users in a flexible environment with users in a tightly standardized environment.

- **Protocol and Authentication Choices**

Microsoft OS-integrated protocols vs. independent IPSec-based VPN clients:
All the companies that I investigated uniformly felt that IPSec was the best protocol. All of them also believed that PPTP had a weak and inadequate level of encryption, as well as flawed authentication methods. UNS has already phased out PPTP entirely. QC is in the process of eliminating all PPTP accounts, but it still uses this protocol for certain populations, such as XP users, since a compatible version of their Cisco client is not quite ready. Both UNS and QC have been testing L2TP, but neither have adopted it. It is clear that both companies don't generally trust embedded Microsoft security and they prefer independent, more configurable solutions instead:

> "UNS has its own VPN software that they require everyone to use so that they can provide a level of security that they are comfortable with. A lot of companies do that. UNS certainly does. The reason they do that is to give them added security above and beyond what Microsoft offers in its operating system" (GS)

In another section he mentions attempted security breaches with PPTP,

> "They were just using straight VPN, coming in with PTTP. We started to see problems with that. A few people tried to hack into it and that's why UNS wanted to go with a higher level of security."

At QC, JF claimed that the general IT community feels IPSec should always be pushed over Microsoft Windows solutions, whenever possible:

> "Generally the thoughts among the IT community are the more you can push an IPsec solution, the more you can push a solution that specifically has a different authentication method than just standard Windows logins, and this will be a better idea."

CL points out another "advantage" of IPSec. It is not proprietary:

> "When there is a choice, the company will choose standards-based implementations over a proprietary protocol unless there is a strong reason to go with the proprietary protocol."

Finally, CL also explains a very useful feature of their independent Nortel VPN client, called *split-tunnel,* that is not a part of Microsoft's solutions:

> "We went to the Nortel client because it supported the split-tunneling feature which allows you to say that one path, which goes back to the company is for their address space, but all the stuff for the global internet goes out through their local provider. So we didn't have to loop the global internet packets through our infrastructure because we felt that would just cost the company money."

Username/password vs. one-time authentication:

Individuals from each company mentioned the importance of changing passwords regularly and creating passwords that are hard to crack, using multiple character types and cases. They also mention that these important specifications are not enforced very well:

> "There is an issue with the passwords not getting changed often enough to fit policy…Every 45-90 days. It's not really enforced that well. Essentially, you have a password for life. It's been on the audit report for four years now."

QC has adopted an entirely new method of authentication called *token-based one-time authentication.* With this authentication, a user carries around a small electronic unit (the token) that is synched with a central server. The LCD display shows a 6-digit number that changes periodically (about every minute). When a user wants to log-in, he types in an easy password that he has chosen, followed by the 6-digit number that is currently displayed on the token. QC packages this type of authentication in its Cisco VPN client:

> "It is with these tokens that we generally pushed the implementation of authentication into an IPSec solution. There are no username/password pairs." (JF)

JF stands behind QC's decision to go with one-time authentication by pointing out the security flaws that exist with traditional username/password methods:

> "It's very hard to manage security of that authentication if it's just using a password. Generally what will end up happening is a user will give that to his family, or his wife or kids, or whatever. So, at that point, there is not much you can do. Obviously, the IT folks that are more sensitive to security issues are going to want to provide a solution that doesn't involve user name and password…You say, hey, use three different forms of characters in combination of upper and lower case, that sort of thing, you make it a very difficult password…A good percentage of the general population, of your folks working for the company, they aren't going to remember whatever password they have chosen when it has those strict rules…They are probably going to write it down, whether they stick it on their wall, or they put it in their planner, or Palm, or whatever. The worst-case scenario, which actually generally happens quite frequently is that they write it down and put it on their laptop."

Obviously, one-time authentication does have its drawbacks too. When asked about additional resource strains associated with this one-time authentication solution, JF said,

> "That's part of one of the acceptable trade-offs of providing security for the organization, and also providing more flexibility for the users. We are devoting a couple resources to the management of this system."

He further mentions the potential inconvenience of the token,

> "Certainly it's a lot more inconvenient for the user to use token-based authentication. If they are not with the device, they have to look for it."

Keeping track of this little unit could become an extra annoyance for the user and lost or destroyed units certainly can increase company overhead even more. Still, the security advantage is obvious.

- **Who should be granted VPN access?**

"Anyone that has a business reason, whose manager will approve the access request can use telecommuting facilities." (CL) At UNS, this is the vague guideline used to determine who should be given a VPN account. Should telecommuting candidates be selected more carefully than this? Should more extensive criteria be used when determining VPN access eligibility? The data reveals some possible attributes that can be surveyed and help the company make more sound decisions about who and where their private network is being extended to.

Large scale vs. small scale access:

The question naturally emerges about what would happen if telecommuting and VPN access were pushed out to a large majority of employees, rather than a smaller selective group. A user considers this:

> "I'm sure if everybody did it, it would start to get annoying. Because if everybody did it, it would be difficult to get a meeting scheduled." (KM)

This and a few similar comments, by both users and specialists, makes one consider the implications of bringing VPN into a larger arena. As it stands now, most telecommuters only work remotely on a part time basis, and the majority of a company's employees, on any

given day, are still working in the company offices. While in most cases, people are continuing to use it as a part-time tool, everyone that was interviewed indicated that the sheer numbers of users are quickly on the rise:

> "Because of the cable modem and DSL that came out we are getting more people starting to telecommute at home. They are not doing it full-time…They'll maybe work a half-day here and a half-day at home. We are getting more calls from different users than our normal ones that usually commute from far away." (DT)

It is important to be proactive and do some research to predict the issues that may arise, both socially and technically (especially in the realm of security), if VPN access is granted to a greater majority of employees. After all, the farther a company extends its network, the more vulnerable it potentially becomes to attacks.

Occasional users vs. frequent users:

Some employees have acquired VPN accounts, but they don't use it on any kind of regular schedule. They never really needed it in the first place, or they may have used it temporarily on a rare trip that they took, and then just left it dormant for a long period. DT mentions this while talking about the actions taken when a telecommuter is responsible for a security breach,

> "If it's maybe somebody that only logs in every six months, they'll probably just cut you off. And those are the people that cause problems because they don't keep their PCs up-to-date. They log in every six months and look what happens."

During an occasional log on, these people create weak links in the network, because they don't keep up with the current issues, virus updates, and other important VPN information, since they rarely use it. Companies need to be aware of this problem and either track how often users are logging in, or create temporary accounts which expire, for those who might need VPN access for only one specific period of time. It may ultimately be smarter to provide accounts only to those who will definitely be using VPN on a regular basis.

User profile and position in company

A company, or at least a direct manager, may want to look more closely at certain attributes of an employee and their position, when determining whether to grant VPN access. Elements they could look at include tasks the employee is responsible for in their position (whether or not these tasks are suitable for a remote environment), team participation, and extent of customer contact. GS describes the tasks he does remotely,

> "Everyday, I put in a certain number of hours at work and then I go home, hook up from home back to work, and finish up for the day. I email, research, compile code, come up with plans or whatever."

Much of the tasks performed by GS are individual and can easily be done outside of the company. When a person's tasks involve more management, team participation and organization, and frequent customer contact, it is not always such a good idea to be physically away from the company. KM discusses the facilitation of meetings with her team members,

> "I don't think NetMeeting is good enough because sometimes you have to be face-to-face. Face-to-face has its own value. People really need to talk to you and see your face. Occasionally a teleconference is fine, but people do need an interaction. They need a feeling that you are true; you are sincere."

DT talks about the difference between a help desk employee and a developer, in relation to telecommuting,

> "If you're a help desk person I discourage it because I like to have people on the scenes. If there are virus alerts, we get hit with them quite a bit, it's good to have people here because you are getting the latest information from people that are working with you on latest patches and fixes. It just depends on what your job is, if you're a developer and your programming in Visual Basic and all that stuff you can do that from home."

The types of considerations described above can aid all parties in deciding who is able to actually utilize a VPN access account in a productive and fruitful manner.

Increasing Central Control and Security in the Home Environment

One of the most interesting clashes that telecommuting introduces involves central control over resources. Usually in a corporate environment, all computers are networked and administrated centrally. Various activities are monitored, workstation applications are inventoried, and everything is consistently kept up-to-date by one entity in the company. Any changes or special needs (i.e. additional specialized software) on systems are documented, and even the network itself is tightly sealed off by firewalls, etc.

- **Challenges in the home work environment**

When a network is extended into employees' homes, many new elements are introduced, many of which, the company cannot control or even monitor, because of either technological limitations, or privacy and social issues. The data I collected often reflected these concerns. Those who manage VPN services don't seem to have a lot of faith in home user's adhering to the policies set forth or in the manner that users set up their home computing environment:**:**

> "Any solution that requires more than one or two clicks to get working, probably the home user, the employee, is not going to adhere to it…If the home user starts to expand his LAN, puts wireless access points on it, things like that, theoretically there are these holes that a corporation may not necessarily like…Certainly, you want to avoid the causal user that kind of is just stumbling around out there, and just interested in killing some time, and doing some mischief. So, there is no way you can protect against that. The home user, obviously, he has control over all those items." (JF)

JF also recognizes the difficulty of enforcing client box security,

> "The ideal way is that you protect the box that the information is on. Whether that's protecting access to the box, or encrypting information on the box, things like that. That really is the ideal way to ensure security, and you know there's always going to be a battle to be, how usable is that? Will people actually take advantage of that if you are attempting to enforce that rule? Up to this point, it's a difficult battle to fight."

One user described some of her behaviors while using VPN at home. Her habits seem to validate IT staff concerns. When asked about her use of firewall and anti-virus software, she replied, "No. I don't. But I bought my husband anti-virus software for his laptop." When asked about disconnecting her VPN connection while away, she said, "I don't usually go to lunch. But if I do, I just leave it online." She also told us that she didn't lock her computer while she was away either. Such issues are compounded by the fact that other family members are often using the same system, and therefore may potentially add conflicting software, make system changes, or acquire viruses on the machine.

- **Potential solutions**

Fortunately, the data also revealed some potential solutions to these problems. DT mentions that, in reaction to a recent virus outbreak, the company has decided to become more aggressive with its warnings and consequential policies about actions that will be taken if an employee negligently compromises the network:

> "Ever since we had the last virus outbreak with Nimda, about three weeks ago or whenever that was, yes. There were emails sent to people saying look, this is what's required to be on your PC at home. And there is a statement in their stating that if you don't comply to these … basically if you get caught, you get cut off…The thing is they can always find out who did it, so that would be a big embarrassment anyway if you don't have the firewall software."

CL talks about monitoring VPN activity and the accountability and cost-savings that it provides:

> "On the backend, everything that comes in through the VPN is monitored. We don't prevent anyone from doing anything but we do monitor so that if there is an attack we can trace it back. There is two reasons, one is accountability, but the other is if you are attacked, you can say it is just these three people and you can turn off the three people. If you cannot make that determination then you have to turn the entire service off, go figure it out and the re-certify everyone. It's just more cost-effective to watch."

At QC, JF discusses a fairly inexpensive firewall router that is very simple to configure and can be used in a home LAN to greatly increase protection:

> "Certainly, this is why the hardware-based things, like the Linksys boxes, are so popular. They are very easy, with very little configuration. You take it out of the box, you plug it in. You know, it generally works, and for the most part it's good. So, when home users do use something like that, you know we encourage it, because it is pretty brainless for them. It doesn't require a lot of thought. Once they get it in, they can ignore it. It all boils down to, that probably is the most expedient way of protecting things."

Companies may want to consider providing all their VPN users with these routers. It could ultimately prove to be an insurance tactic that is very cost-effective.

Another potential solution to help standardize and secure the home work environment is found in a certain application, used by QC, called Citrix. Citrix runs on a centralized server and provides application and data storage services, similar to a remote desktop environment. While users sometimes experience slow performance, it carries many advantages, as JF describes,

> "It's one way to conserve software licensing. It's also version control, and things of that sort of nature. It's convenient, because it allows people to share applications and share resources, without having to be pushed out on the client level… It's like a centralized workstation… (Citrix) potentially encourages them to store their data in a more central location, potentially a location that's physically inside the company, and that sometimes may limit the amount of company-sensitive material that the user is going to have on his home machine… Inherently, it becomes a lot easier to protect data that way."

If this sort of technology is improved and expanded, companies may be able to set up a VPN client that only works inside such a centralized workstation application (company resource access would only be possible within this centralized workstation). That way, a user could essentially be using an IT-regulated machine, inside the company, the entire

time he is connected on the VPN. It would definitely be worth researching what it would take to implement such a system.

Company Reliance on Home Internet Service Providers

CL brought up a topic that I never considered. He talked about the ISP providers that company employees select at home, and the arising disagreements over companies using them as a cost-free bandwith solution:

> "The other issue with cable is with some providers … If they suspect that you are on VPN then they will throttle you back to 28.8 speed. That's an @Home policy issue…They know that you are using it for business and that technically violates your agreement with them… you run on certain ports with certain protocols for all the VPN, so they can just figure that out and push you down in the priority queues. We fought with @Home a little bit about that because we were looking at putting in a cable presence in here but they wouldn't back off."

Companies openly recognize the savings they enjoy at the "expense" of ISPs:

> "Ultimately, the concept is that does save the corporation funds. It moves the corporation through having to basically operate like an ISP provider for their employees, you know offering T1 connections into the company, to having annexes dialing, and various other dial-up solutions, having to pay those monthly occurring costs."

The issue is that ISPs always charge businesses significantly more for internet service than they charge recreational home users. That is a standard business practice with almost any type of resource. Companies now are basically taking a financial shortcut by using cheaper consumer products to extend their network for their employees. In fact, in most cases the company doesn't pay anything. Employees usually pay for their own ISP service. Furthermore, in many cases, our data showed that people who do VPN over cable or DSL specifically got their high-speed connection for the purpose of work, not personal use. The question is whether this is a fair situation. The argument is complicated though. Certainly, the employee/VPN user appreciates the enticing freedom of not being tied to his office and being able to work from inside his home. It does seem like the cost is worth it to the user. The broadband providers, on the other hand, obviously don't share the same enthusiasm. Then again, are they really being cheated? VPN-enabled companies, after all, have created and delivered an almost entirely new market of potential customers to these cable and DSL companies. Therefore, one would think, in the long run, that there is some benefit to the ISPs, and that this is a win-win-win situation for all sides. It would be interesting to get statistical data on the financial benefits for each side (i.e. cost savings, increased revenue from larger customer base), in order to reveal the real truth here.

4. Recommendations

This section identifies areas that warrant potential further investigation. They are ideas that I generated throughout the processes of the study, but were outside the scope of this project.

Security Compliance in Standard and Flexible Workplaces

This recommendation is to conduct a Quantitative Analysis that examines user's compliance with security policies in both standard and flexible work environments. This idea comes

from one of the most interesting themes in our analysis, which were the differing philosophies between the companies deploying VPN solutions. An interesting project could be conceived by identifying anywhere from four to six companies that deploy VPN solutions, examine each philosophy and classify it as either Standard or Flexible. Once this has been established, it would be interesting to question a large sample of users from companies in each classification (Standard and Flexible). The quantitative analysis would have yes/no, multiple-choice questions that could be mathematically converted into a statistical format for analysis. An example of a quantitative analysis on this topic can be found in Appendix C.

Integrating a VPN Client Into a Centralized Workstation System

Expanding the concepts behind the Citrix application, used at QC, could potentially provide a key solution to the issues of standardization and security in home telecommuting environments. If an IPSec VPN client could be tightly integrated into a Citrix-type of system, so that the VPN was only accessible within this central workstation, it wouldn't matter what operating system or software was installed on the client machine. Furthermore, if firewall and anti-virus functionality were built into this centralized system, client machine security configurations would be irrelevant. As long as the centralized workstation application and VPN client component are compatible on the client computer, there would be nothing more to worry about. In the future, I would like to investigate the viability of such a solution and eventually develop a prototype. Possible drawbacks of such a system may be slow performance, limited application options for users, and difficulty in using specialized applications that are not provided on the central workstation. If successful though, such an implementation could prove to be a major advantage to IT groups in any company. It could also mean less technical problems for VPN users.

Are Consumer ISP Providers Truly Being Taken Advantage of by VPN-Enabled Companies?

I learned in my study that the policy of some ISPs prohibits VPN use through their connections. If a VPN is detected, the ISP penalizes that user by severely limiting his bandwidth during any active VPN session. This is done because the ISP feels that companies are unfairly taking advantage of their consumer products. On the other hand, I also learned that many VPN users only have a high-speed broadband connection because they use it to connect to their company, and that if it weren't for their VPN needs, they would simply have a dial-up connection instead. Looking at it this way, VPN-enabled companies may be delivering a whole new customer base to ISP companies. A research study should be conducted, in the future, that statistically analyzes the financial benefits enjoyed by these ISPs, specifically because of this new customer base. I could also examine how such benefits compare to the cost savings enjoyed by those companies who are indirectly using their bandwidth.

5. Conclusion

This research project began with the more general topic of social implications on computer networks. I specifically selected virtual private networks because they are inherently a result of the social need or desire to telecommute. Because of the many technical components that this area is concerned with, it was apparent that I needed to first become familiar with the technologies that were involved in virtual private networking for

telecommuting. Consequently, I began this study by researching how the various protocols work, their strengths and weaknesses, and the different ways that virtual private networks may be implemented.

This qualitative study generated many interesting emergent themes that could be further investigated or authenticated in subsequent studies. Unfortunately, time and resource did not permit me to push my project into this next phase of research. In this paper, I have reported only what I consider to be the most important and useful themes that have surfaced from the data.

6. References

Virtual Private Network Technical Papers

Gleeson, B., Lin, A., Heinanen, J., Finland, Telia., Armitage, G., Malis, A., "A Framework for IP Based Virtual Private Networks", RFC 2764, February 2000.

Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

Kent, S., Atkinson, R., "Authentication Header (AH)", RFC 2402, November 1998.

Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

Hazeh, K., Verthein, W., Taarud, J., Little, W., Zorn, G., "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

Simpson, W., editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

Townsley, W., Valencia, A., Rubens, A., Pall, G, Zorn, G., Palter, B., "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

Qualitative Research Methodology

Button, G., Dourish, P., "On "Technomethodology": Foundational Relationships Between Ethnomethodology and System Design"

Corbin, J., Strauss, A., "Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory"

Kiesler, S., Sproull, L., "Connections: New Ways of Working In The Networked Organization"

Lofland, J., Lofland, L., "Analyzing Social Settings: A Guide to Qualitative Observation and Analysis", Third Edition, Wadsworth Publishing Company, 1995.

McCracken, G., "The Long Interview", 1988.

General VPN Articles

Brown, B., Lewis, C., “Best Practices For VPN Implementation”, http://www.bcr.com/bcrmag/2001/03/p24.asp, Business Communications Review, March 2001.

Boros, D., Crowe, A., Habinc, R., Meeker, S., “VPN”, http://www.emory.edu/BUSINESS/et/P98/vpn/.

Enterasys Networks, Inc., “White Paper: Virtual Private Networks A Technology Overview”, http://www.enterasys.com/products/whitepapers/vpn/9011742.html, 2001.

Fred Parker Marketing., “The Manager's Roadmap to Virtual Private Networks”, http://www.fredparkermarketing.com/vpnrm.htm, 2001.

Green, T., “Trimble Navigation Finds VPNs useful for remote access”, http://www.nwfusion.com/research/2000/0814featsidetwo.html, Network World Fusion, 2000.

Internet Week, “VPN Alliance: White Paper”, http://www.internetwk.com/VPN/paper.htm.

Mitchell, B., “Introduction to VPN”, http://compnetworking.about.com/library/weekly/aa010701a.htm.

Taylor, L., “VPNs Are Hot, but What Are They?”, http://www.intranetjournal.com/articles/199911/ft_11_16_99a.html, 1999.

Core Competence, Inc., “VPNs: Virtually Anything? (A Core Competence Industry Report)” http://www.corecom.com/html/vpn.html, 2001.

7. Appendices

A. Interview Questions

This section contains the two sets of questions used to facilitate our interviews. The two sets pertain to Network engineers and users of VPN telecommuting technologies.

- **Interview Questions for Network Specialist**

Generic Information

1. What is your position/title in the company?
2. What does your position entail on a typical day?
3. How long have you been with the company?

Telecommuting/VPN

4. What is the company policy regarding telecommuting? Is it encouraged/discouraged?
5. What is the company policy regarding VPN? What industry standards do you follow?
6. What technologies do employees use when telecommuting? VPN, Dial-up, etc.?
7. Can you describe in detail the VPN technology used by your company? Does this solution give priority to some users and not to others?
8. How did the company decide on this VPN technology? (cost, speed, security)
9. What type of authentication of users has the company used? What happens when someone leaves the company?
10. Compare the current VPN options with old dial-up solutions.
11. Has VPN saved the company money?
12. How does your company manage VPN? Do you outsource it? Have you changed VPN solutions/services?
13. How do deploying these options introduce problems or change the way people work? (i.e. did your job change, did you have to learn new technological information).
14. How has VPN changed telecommuting? More popular, more accepted?
15. Is your VPN secured? Any security breaches? What strategies does the company use to make VPN secure?
16. How has VPN affected the performance of the network? Where are VPN entry points?
17. Has the hardware configuration of the network undergone reconstruction as a result of more/less requirements?
18. What technologies/applications do VPN users use? PcAnywhere, NetMeeting? Which ones are better? Why?
19. Have the changes in technology (use of VPN) changed the way the company does business?
20. Has it changed the corporate culture?
21. Has VPN been adopted for other uses, i.e. communications with vendors, secure e-commerce, etc.? (site-to-site connection)
22. Do you use VPN?
23. Did you have an Internet connection at home before the company introduced VPN?
24. Has your family started using the Internet more as a result of it being readily available inside your home? If so, is this good/bad?

- **Interview Questions for Users of the VPN**

Generic Information

1. What is your position/title in the company?
2. What type of work do you do in your position on a day-to-day basis?
3. How long have you been with the company?
4. Are you married? Do you have kids? Whom do you live with?
5. How far away do you live from work (distance and time)?

Telecommuting

General Telecommuting:

1. Where do you spend most of your time doing company-related tasks?
2. How often, if ever, do you telecommute? Why and where do you choose to telecommute?
3. Describe the work (tasks) you do while telecommuting (at a remote site)?
4. Compare the tasks you do remotely with the tasks you do locally? Do these remote tasks require access to the company network? If so, why?
5. What remote connection solutions are available to employees? Which one do you use? Why?

VPN Client Setup:

6. What specific type of VPN account is it (i.e. PPTP)?
    a. How long have you had this account?
    b. Have you set up this VPN connection on a remote computer? Is it currently working?
    c. Do you actively use it (when was the last time you logged in on the VPN)?
7. Do you have a network at home (hub, routers, Ethernet, wireless, etc.)?
8. Describe the primary computer that you connect via VPN (system specs, network card, etc.)?
   Is it a laptop or desktop computer? What OS is it running?
9. What type of Internet connection do you have? Who is your ISP? Why did you choose this particular company and type? Who pays for it?
10. Why did you get an Internet connection in the first place? Did you have an Internet connection before setting up the VPN?
11. If you chose a high-speed option (i.e. cable, DSL), was this choice primarily made because you would use it for work?
12. How has such a connection in your home affected your family life and habits?
13. Do you run anti-virus and/or firewall software on your computer?
    a. Why did you choose to install this software?
    b. Did you buy it or did your company provide it to you?
14. What was your experience in setting up the VPN connection on your remote computer? How long did it take?
15. Did you contact IT support during the setup process?
    "yes"
    a. Were they able to help you with any problems?
    b. How long did you have to talk to them?
    "no"
    c. How did you get the information to set up everything correctly?

VPN/Telecommuting Usage/Productivity:

16. What are your specific uses for VPN?

17. What is your experience so far while doing work over the VPN?
18. How do you compare this experience with working in your office at your company?
19. What possibilities/limitations has telecommuting created for you?
20. Which place do you prefer to work in? Why?
21. How does the performance of the connection compare to the network connection at work?
22. Are you more productive at home or less productive, than when you are at your company office? What do you suppose accounts for this increase or decrease in productive work?
23. What distractions affect you at your company office? What about at home?
24. How often do you use VPN (i.e. in a single week)? How long do you tend to stay connected?
25. Do you leave your VPN connection running while doing non-work related activities? Or while you are away from your computer?
26. How has VPN affected your work schedule? Has your schedule changed based on usage related factors?

Security/Performance Issues on Local Machine (client-end):

27. Who has access to the computer that is set up with the VPN connection? Does anyone outside your family use these computers (i.e. children's friends)?
28. Any other "VPN users," same or different company? Conflicting interests?
29. Is your computer password-protected in regards to various accesses (such as administrative privileges)? Does your computer have file shares or printer sharing?
30. How does your computer handle the additional memory and processing requirements of a VPN connection, a software firewall, and/or anti-virus software? Are you still able to efficiently use the applications you need? (Does your computer lock up?)
31. Are you aware of the company policies regarding VPN use? Where would you find the policies? Are they easily accessible?
32. How would you improve the telecommuter experience at the company?

Collaborative Tool Usage (over VPN:)

33. Do you work in a team environment?
34. How does telecommuting over VPN enhance/detract from the team?
35. Do you use any collaborative tools over VPN? (i.e. NetMeeting) Who advocates/discourages their use? Did you use any of these tools at all before you started telecommuting?
36. Do you find these collaborative tools facilitate or hinder productive work within a team atmosphere?
37. Do you feel that telecommuting itself has had any negative effects on your ability to work in a team atmosphere?

Other Social Questions in Relation to Telecommuting:

38. How has telecommuting effected your relations with other co-workers?
39. While telecommuting, do you feel "in touch with" or "isolated from" your workplace? Explain?
40. Is telecommuting encouraged/discouraged by your supervisor/boss? By your department? By your company as a whole?

B. Coding Procedures

- **Open Coding**

General Subject Info

Dan: What is your position/title in the company?

Chris: Senior Telecommunication Engineer … I work for Corporate Staff, effectively my organization is responsible for network security and it's a sub organization of the organization responsible for network design.

Dan: What does your position entail on a typical day?

Chris: Some troubleshooting … engineering of secured solution, we also do routing design, router configuration … consulting with other people on staff, consulting with the business units on how they approach things.

Dan: How long have you been with the company?

Chris: In this job 10 years, but with the company 23.

Dan: What were you doing before this?

Chris: Working the field as systems analyst, doing fly-fix work in the mainframe environment.

Company Policy

Dan: What is the company attitude regarding telecommuting? Is it encouraged/discouraged?

Chris: In a cost-effective approach, it is encouraged. We've had in telecommunications or remote access we're probably rst wave company we're not typically bleeding edge for things, but would be first adopters of technology.

Dan: What is the company policy regarding VPN? What standards do you follow?

Chris: Anyone that has a business reason, whose manager will approve the access request can use telecommuting lities.

Telecommuting Technology Used

Bryce: What technologies do employees use when telecommuting?

Chris: Since we were an early adopter, we standardized on the Nortel VPN solution which has a dedicated client on the kstation. There were three reasons for that design. One is, since VPN is a high bandwidth, high workload uirement, encrypting and decrypting packets requires a lot of workload, we push that o into a separate infrastructure, separate machines to do that work because we felt when you put 2,000 or 3,000 people out there .. putting that out on another box like a firewall, typically will overload the box and you end up with a performance issue. We went to the Nortel client because it supported the split tunneling feature ich allows you to say that one path, which goes back to the company is

for their address space, but all the stuff for the global internet goes out through their local provider. So we didn't have to loop the global internet packets through our infrastructure because we felt that would just cost the company money. We were willing to accept that there is a minor risk with that, that someone could compromise the VPN workstation and get to the network.

Bryce: So there is a secure tunnel running parallel to the ISP connection?

Chris: Yeah, you're running ISP connection and all the local address spaces goes down that directly, anything to our address space is actually the only one going down the tunnel.

Bryce: The client is smart enough to know which way to go?

Chris: We actually send it routing tables from the box that says these address spaces go through the tunnel, the rest ship out through the ISP.

Performance Issues

Bryce: Does that slow things down at all?

Chris: Well, it only encrypts the packets that need to be encrypted. The only issue is, you have to have the client, a dedicated client to run which is probably more secured. We just felt that the user would not put up with either the slowness of wrapping it through our internet connection or … I want to go to the internet, and I have to take the client down, oops I want to go back into the company let me bring the client back up … they would be doing it about thirty times a minute. It's too much user hassle.

Dan: Would you say that the VPN solution puts a large workload on the company network?

Chris: Relatively for us, no. Most of our stuff is internal, we have just engineered it so that it wouldn't affect the firewalls.

Infrastructure Changes

Dan: Has telecommuting taken a load off of the network?

Chris: Previously we had a large dial-up, remote access group, we had dial up VPN boxes all over the network, but we scaled back and there was a large 800 number contingent and given that we were probably paying 8 cents per minute for all of those calls, we realized millions dollars of savings in deploying the VPN.

Dan: So that has all been taken down since using VPN?

Chris: …been scaled back quite a bit. The 800 number access is for a handful of selected people. The other remote access dial in still exists, but you have to dial up, like there is a system here in Mission that you can dial into the local number and it's actually cheaper for the people and the company for local people to dial the remote access box than to go to VPN. Because locally with an ISDN you pay 0 cents a minute if your in the same CO so it costs the company the cost of the ISDN line, whereas if you are going with an ISP, you have to pay for the ISDN line and the ISP pipe and so your paying probably $50 dollars/month instead of $20.

Dan: Have they actually taken out hardware? Modem pools, things like that?

Chris: Some of it has been scaled back … actually it's more likely been redeployed in other places where we need that dial-up. And the solution is world-wide, it's also into the international divisions. Both the remote access and the VPN access is gatewayed into to places in the US, one in England and one in Australia.

Type of User Internet Connections

Bryce: Do most people still use the dial-up VPN? Or local ISPs?

Chris: The company arranged when we first rolled out VPN for a $15 a month fee with UUNET, who was our main ISP provider at the time and given manager approval that can be reimbursed. So there has been a big push to get people to VPN and ISP. And you can get an ISP for $15 a month for 250 hour, so unless you don't sleep you should have plenty of time.

Bryce: Since cable and DSL, have most people moved away from that?

Chris: In selective areas, particularly in the development sites people have moved to cable and broadband a lot of the other uses, particularly the service people are still on the dial-in VPN?

Bryce: More developers telecommute?

Chris: They've always been big in the development community telecommuting.

Dan: Has there been a problem with the availability of cable and DSL with VPN?

Chris: DSL is still a hard thing to get, so is cable. The other issue with cable is with some providers … if they suspect that you are on VPN then they will throttle you back to 28/8 speed. That's an @home policy issue.

Bryce: The service provider will actually give you less service?

Chris: Because they know that you are using it for business that technically violates your agreement with them for cable.

Dan: There a way to block that?

Chris: Yeah, you run on certain ports with certain protocols for all the VPN, so they can just figure that out and push you down in the priority queues. We fought with @home a little bit about that because we were looking at putting in a cable presence here but they would back off with that which broke off our negotiations.

- **Axial Coding**

Contrasting VPN Implementation Policies

I. Flexible vs. Standard Approach
Page: 23
[CL]##Standardization ()##; ##VPN solution ()##
Page: 23
[DT]##VPN authority: =all decisions centralized at corporate (Software Review Board)##
Page: 23
[JF]##company VPN philosophy: =be as flexible as possible##
Page: 23
[JF]##VPN authority: =centralized##; **Having all networking centralized is not always popular with remote sites**

A. Pros and Cons

1. VPN client
Page: 23
[DT]##VPN client software priority: [customizable]##
Page: 23
[DT]$$<internal development>Unisys likes to make its own products and/or customize partnered products to their own liking$$; ##development and deployment control: =high##
Page: 23
[JF]##priority factor in VPN client software: =flexibility/support for multiple OS's##
2. OS
Page: 23
[GS]##computer lock-ups: =no problem on Windows 2000 systems, but some problems on Windows 98 (not as stable)##
Page: 23
[DT]##software standards for remote users: =strongly recommended (down to the most recent service packs)##; $$<corporate software tests>Corporate testing must be completed before software makes standard list.$$
Page: 23
[JF]##alternative OS: =large Unix community##
3. Firewall/anti-virus software
Page: 23
[GS]##firewall/anti-virus software: =uses software provided by company (Norton Anti-virus)##
Page: 23
[DT]##firewall use: =mandatory##; $$<control over home PC>control over home PC's is inherently very weak$$;
Page: 23
[DT]%%broadband (always on and faster) → easier to spread and get viruses%%; ##accountability (trace virus source): =high##; ##firewall compliance: =good?##; ##motives for firewall use: ="embarrassment" of getting caught (transferring virus)##
Page: 23
[CL]##firewall/anti-virus requirements (passive – strong)##
4. Remote desktop software
Page: 23
[GS]##remote desktop software: =terminal services; \why?: =faster##

Page: 24
[DT]##remote desktop software: =no standard##; **people use NetMeeting and Terminal Services if so desired**
Page: 24
[JF]##remote desktop software: =Timbuktu; \used by help desk for troubleshooting: =yes; \standard: =no standard##

5. Centralized workstation
   Page: 24
   [GS]##storage of files: =centralized, work machine.##; ##remote desktop use: [consolidation (keep links, files, applications, etc. all in one place), avoid redundancy, save space on home computer for recreation##
   Page: 24
   [JF]##advantage of central server applications: [conserve software licensing, version control, share applications and resources not on client machines]##; $$<using a central server (i.e. Citrix)>JF believes that such an application could potentially encourage employees to store their data in a more central location that is physically inside the company (behind the company's powerful firewalls). The goal is to minimize the company-sensitive material that employees have on their home machines. This may be another clever way to protect data.$$
6. More extensive enforcement of policies in home

Page: 24
[DT]##home LAN policies from company: =none##
Page: 24
[DT]##aggressiveness of policy enforcement: =high (since virus outbreaks); \measures taken: =not complying with standards will get your access disabled indefinitely.##
Page: 24
[JF]$$<Linksys advantage>Linksys routers provide a win-win situation. They are easy to configure and also provide strong security to the home user. Perhaps such a piece of equipment could become mandatory for VPN users, since maybe favor it even voluntarily$$
Page: 24
[JF]##most important security area: =client box##

B. Network specialist point-of-view
   Page: 24
   [JF]##VPN's inherent loss of client machine control (solutions): =educate the user, awareness, encourage proper use of software firewalls, hardware routers##
   Page: 24
   [JF]%%<user compliance/ease-of-use>usability → compliance to security policies%%
   Page: 24
   [JF]##faith in user's adherence to security policy: =rather low##
   Page: 24
   [JF]$$<faith in user>JF seems to be highly skeptical of user's willingness or inherent ability to keep their home computing environment secure. He mentions quite a number of times that you need dummy-proof solutions in order to get people to follow policy correctly$$
   Page: 24
   [JF]%%<flexibility/security>single solution, limited options → security breakdown%%

Page: 25
[JF]$$<battle of flexibility vs. company protection>JF now calls this an opposing battle, but this is also a paradoxical relationship. A few lines earlier, he talked about how these things actually go hand-in-hand%%
Page: 25
[JF]%%<available tools/productivity>more tools to enable employee → higher productivity%%
Page: 25
$$<Policy limiting application use>CL thinks that there should be some limits on applications used over VPN.$$

C. User experience
Page: 25
[GS]##improving VPN experience: =don't block file-transfer feature on IM applications##
Page: 25
[JF]$$<customer satisfaction levels>What are these levels? Who sets them? What exactly do they consist of? Are their customer satisfaction levels set for VPN users?$$

D. Company atmosphere
Page: 25
[JF]##company philosophy/support: =encouraged, "empowers the employees"##
Page: 25
[JF]$$<corporate culture>JF thinks opposite effect than we guessed. He believes a corporation's culture drives their technology. QC is a very collaborative, open environment. This has led to evolutions in technology to complement this atmosphere. VPN only reinforces the environment that already existed here, and it is a more a product rather than a cause of this type of atmosphere.$$
Page: 25
[CL]##Company support of telecommuting; \support justification##; ##technology adoption stance (first adopter, resistant)##

E. Provisions for legacy solutions
Page: 25
[RS]##problem with dial-up VPN: =encryptions eat up 60 percent of bandwith, painfully slow to begin with##
Page: 25
[DT]%%dial-up VPN → limited security and configuration options%%; $$<dial-up VPN>Security more reliant on client machine. Dial-up protocol in OS was not originally designed to be used for internet tunneling, just straight line connections.$$
Page: 25
[DT]%%broadband VPN → more control and security%%
Page: 25
[CL]##Scaling back old dial-up (yes - no)##; $$<When dial-up is preferred>Chris claims that sometimes it is more cost-effective for the users and the company to dial the remote access box rather than VPN. Still, depending on what you are doing, I think the poor speed of a dial-up wouldn't make up for the cost-savings.$$; $$<Reallocation of equipment>Chris makes an important note that when equipment is scaled back it is often still put to use in other places, where it might still be needed. For example, many areas still don't have broadband widely available to home users. These people must still have the option to dial in.$$

II. Authentication Solutions

A. Username/password vs. one-time authentication
   Page: 26
   [MS]##password policy: =change password every three months##
   Page: 26
   [JF]##facing security risks: =enforce IPSec, one-time authentication##
   Page: 26
   [JF]##preferred authentication method: =security token, no username/password pairs##
   Page: 26
   [JF]$$<relationship between one-time authenticate and IPSec>I wonder, specifically how IPSec and one-time authentication are related to each other. Are they dependent on each other, to any extent? How, exactly are they utilized together?$$
   Page: 26
   [JF]##downside of passwords: =hard to manage, enforce privacy of passwords, give or make available to others##
   Page: 26
   [JF]##overhead of token-based security: =extra management resources##
   Page: 26
   [JF]##downside to token-based authentication: =inconvenient carrying around and keeping track of token##
   Page: 26
   [JF]%%<difficult passwords/security issues>difficult passwords → user more likely to write it down and neutralize it's extra security impact%%
   Page: 26
   [CL]##password changes (easy – difficult)##; $$<Importance of pasword changes?>What would be the importance of easy password changes? Maybe it would encourage people to follow policy and change their password on a regular basis, or perhaps just less calls to IT help.$$
B. OS-integrated authentication vs. VPN client software
   Page: 26
   [GS]##Microsoft OS security: =not sufficient, additional client required for adequate security##
   Page: 26
   [RS]##PPTP vs. L2TP: =more people currently use PPTP##
   Page: 26
   [GS]##extra security measures: =tunnel within a tunnel (split-tunnel)##; ##security breaches: =a few hack attempts##
   Page: 26
   [DT]%%protocol security: IPSec better than PPTP%%
   Page: 26
   [DT]##PPTP use: =none (phased out)
   Page: 26
   [JF]##favor Microsoft: =no, not in terms of their VPN provisions##; ##PPTP support: =discouraged, being phased out, still used by some##
   Page: 26
   [JF]$$<L2TP use>Why is this protocol still being considered in the face of IPSec, which is seemingly preferred by everyone? Is there anything that L2TP can provide that IPSec can't? Do they work together at all?$$
   Page: 26
   [JF]$$<Microsoft product security>QC seems to have similar attitudes to Microsoft, pushing usability and flexibility over security, yet JF tends to avoid

Microsoft VPN methods because of their low security, although he does mention "ease-of-use" as an important advantage of L2TP$$
Page: 27
[CL]##VPN client software [(split tunnel) (supports IPSec)]##
Page: 27
[CL]##authentication protocol source – preference of company (standards-based - proprietary)##

III. Who should be granted VPN access?
Page: 27
[CL]$$<Business Reason>What is considered a business reason? I wonder if this is a loosely based term, or if there is a more formal definition used.$$; ##approval process to get VPN account ()##; $$<Access Request>What is involved in an access request? I am curious what the procedures are for an access request. Does it only require a direct manager's approval, or must other sign off on the request as well?$$

A. Large scale vs. Small scale access
Page: 27
[MS]$$<telecommuting on a large scale>Telecommuting may be great on a small scale. When only a minority percentage are utilizing this option and they generally do it on a part-time basis, it seemingly works beautifully. What happens, though, if and when telecommuting is taken on in a much larger scale? What would it be like if the majority of employees in a company were telecommuting and working outside of the office? How would all dynamics be changed at the company? What issues would this create?$$
Page: 27
[CM]##personal attitude on expanding telecommuting: =doesn't believe "everyone" should do it, hard to schedule meetings##

B. Occasional users vs. frequent users
Page: 27
[DT]##biggest security risks (employees): =occasional users (aren't aware of current issues, don't have PC's up to date)##; $$<occasional users and security>Perhaps a good policy is only to give a VPN account to people who use it frequently. Employee's use frequency could be monitored and those who don't use it enough could be disabled. Temporary access can be given for those employees that need it for a rare trip, and they can be issued a company laptop that is guaranteed to be up-to-date.$$
Page: 27
[CL]##VPN effect on telecommuting: increase in "casual" telecommuting ()##

C. User position in company
1. Tasks suited for telecommuting
Page: 27
[GS]##remote tasks: [email, research, planning, compiling code]##
Page: 27
[GS]##tasks not able to do remotely: =none (because of today's high quality broadband connections and modern software)##
Page: 27
[GS]**Less productive at work because so much time is spent answering colleagues' questions.**
Page: 27
[CM]##tasks suited for home: =coding##; ##tasks suited for company office: =learning something new; \preferred learning environment: =likes company office because of the available "experts", face-to-face##
2. Manager knowledge of employee work habits

Page: 28
[GS]##productivity and telecommuting: =variable with different users (managers know which users can be productive and which can't)##
Page: 28
[GS]##manager support of VPN/telecommuting: =some managers don't understand, discourage it, others are more progressive; \why?: =worry about loss of control##
Page: 28
[MS]##productivity effects: Depends on tasks, people involved; **Not concerned with hours spent working, only that projects are done within an appropriate time limit.**
Page: 28
[DT]##telecommuting majority: =part-time {part-time…full-time}##

3. Team participation
Page: 28
[CM]##considerations for telecommuters: =maintains consistent schedule, reassures team of availability; \maintain consistent schedule; \accessibility to team members##
Page: 28
[CM]##team membership: =yes, project manager (yes…no)##
Page: 28
[CM]##attributes of a good telecommuter: =consistency, easy to get a hold of##
4. Extent of customer contact
a. *Example:* Help desk employee vs. developer

IV. Company reliance on home Internet Service Providers

A. Are corporations taking advantage of home ISP's?
Page: 28
[GS]##ISP subsidy: =pays himself##; $$<ISP subsidy>company will pay, but only for slow dial-up. This is not particularly useful.$$
Page: 28
[DT]##ISP fee reimbursements: =yes (if investment is proven worthwhile)##
Page: 28
##cost advantage: =company no longer acts as ISP provider##
Page: 28
[CL]##Split tunnel (yes - no)##; $$<Split Tunnel Explanation>Split tunnel feature allows global internet traffic to go directly through their local provider without having to loop through the company infrastructure first. It does present a minor security risk. This feature chose cost over security. Routing tables are sent to the client, so it knows which packets to send through the VPN tunnel.$$
Page: 28
[CL]##company subsidy for ISP service (yes - no)##; $$<ISP Reimbursement>This reimbursement must be requested and the decision is made on a case-by-case basis$$
Page: 28
[CL]##Availability of broadband consumer solutions (good, poor)##; $$<Corporations vs. ISP Providers>Interesting clash between corporations with VPN solutions and consumer ISP providers: Companies are now basically extending their network for their employees by using consumer products, which are obviously much cheaper. In fact, in most cases the company doesn't pay anything. The employee pays for their own ISP. Furthermore, in more than a couple of cases, I have found that people who do VPN over cable or DSL, specifically got their high-speed connection for the purpose of WORK, and not

personal use!! Is this a good business plan? YES! Is it a fair situation? Well that's where things can get rather hazy. Obviously, the employee/VPN user appreciates the enticing freedom of not being tied to their office and being able to work from inside their homes. So far, it seems like the small cost seems worth it to them. The broadband providers on the other hand couldn't possibly share the same enthusiasm. But then, once again, are they really being cheated?! VPN-enabled companies, after all, have created and delivered an almost entirely new market of potential customers to these cable and DSL companies. So, one would think, in the long run, this is a win-win-win situation for all sides. I guess it is a matter of perspective…$$

Page: 29

[CL]$$<Hiding presence of VPN tunnels>One would think that it is technologically possible to hide these encrypted VPN tunnels from the ISP providers. Is there an implementation of VPN that could sneak through unprotected?$$

B. Is it fair for ISP's to limit bandwith to customers while using a VPN connection?

VPN User/Company Profiles and Technology Risks

I. What type of user makes a company a strong first adopter candidate for VPN technologies?

Page: 29

[CL]&&propeller heads = technology geeks, enjoy new technologies&&; %%<Tech skills/New technologies>general technical proficiency of company employees → unafraid to play with new technology%%

A. Position at company (nature of skills and knowledge)

1. Knowledge of security issues surrounding VPN

Page: 29

$$<Advantage of developer VPN users>Telecommuting has always been a bigger deal in the development community, according to Chris. Why is this? Is it because they are more technologically-inclined (personal attributes), or is it more a function of the environment required to perform their work functions (job attributes)? If Chris' statement is true, I wonder what implications this has on a company's deployment of VPN. If a very large percentage of telecommuters in a particular company are developers, then the company is dealing with a much more specific subset audience of users. Are their common characteristics among most developers that may be useful to a network design team to know when implementing VPN? For example, maybe developers tend to be more tolerant about using a less user-friendly but greatly more robust (i.e. secure) VPN client. Here is another instance: Suppose developers are more aware and proactive about computer and network security at home. Along these lines, a company could be more reliant on its users to take the necessary security measures to protect the company's confidential information and vital servers. With this said, a company could feel more comfortable trying out new features and methods in VPN. They wouldn't be forced to rely on older, proven technologies that have been thoroughly tested in security, but still pale in comparison to the efficiency and scalability of some new cutting-edge solutions. It seems that Unisys may possess this luxury. Chris claims they are first adopters, and that they started using VPN long before other companies of similar stature. This says something about the faith and trust they have in their telecommuting employees.$$

Page: 29

[MS]**Mobile executives: CEO's and other executives have always been very mobile. These people must often go on road trip campaigns for the company,

and during these trips they need access to a broad range of information in the company. The cell phone has followed a similar path. Initially, it was only used by executives who needed to transfer information to each other from remote locations.**
Page: 30
[DT]##extent of mobile VPN users: =many engineers##

2. VPN use behavior
Page: 30
[GS]##connection when away: =no, disconnects whenever not using VPN##
Page: 30
[DT]##successful telecommuting candidates; \good: [developer]; \\what makes a good candidate: [higher home productivity]; \bad: [help desk]##
Page: 30
[CM]##positive security behaviors: =writes everything on server## $$<store data on server?>I wonder if she also stores all of her data on the server as well, instead of on her home PC. This is something that JF mentioned was a potential advantage with the Citrix network desktop solution$$
Page: 30
[CM]##use of anti-virus software: =no, but gave a company copy to husband (installed…not used); \anti-virus software is company-issued: =yes##
Page: 30
[CM]##single session duration: =8 hours##
Page: 30
[CM]##unattended connection: =leaves it on when she goes to lunch, etc.##
Page: 30
[CM]##locking the home computer: =no##
Page: 30
[CL]##trends of broadband use across employees ()##; %%<Developers vs. Service people>Developers are more likely than service people to use cable and DSL.%%

B. Home situation
1. Home network configuration
Page: 30
[GS]##home LAN: =wires every single room, COX cable modem, 6-8 computers; \main usage: =set up user environment to test applications from home##
Page: 30
[GS]##motive for broadband: =personal (would have it even if he wasn't using VPN)##
Page: 30
[MS]##home internet connection: =56K modem; \why?: =never home##
Page: 30
[DT]##cable modem prior to telecommute: no (been telecommuting before cable modem available)##; ##broadband value to user: = high##
Page: 30
[JF]$$<Linksys advantage>Linksys routers provide a win-win situation. They are easy to configure and also provide strong security to the home user. Perhaps such a piece of equipment could become mandatory for VPN users, since maybe favor it even voluntarily$$
Page: 30
[JF]##home network vulnerability: =wireless access points##
Page: 30
[JF]##personal broadband use: =cable modem##

Page: 31
[JF]##motive for broadband: =had before VPN, personal motives##
Page: 31
[CM]##Motive for fast internet connection: =strictly work##

2. Family computer use
   Page: 31
   [GS]##different accounts for family members: =yes, separate password-protected accounts##
   Page: 31
   [GS]##password protection of account: =yes##
   Page: 31
   [CM]##password protection of home VPN computer: =husband and her each have own separate account (strong…weak); \purpose of passwords: =kids accessing the internet##
3. Other VPN users in household
   Page: 31
   [GS]##other VPN users: =none##

C. Occasional vs. frequent VPN use
D. Company controls over VPN client computers
   1. Policy compliance
      Page: 31
      [GS]##policy compliance: =yes, knows them and follows them##
      Page: 31
      [CM]##awareness of company policy: =unaware (ignorant…knowledgeable)##
      Page: 31
      [CL]##hardware security defense (low – high)##; $$<Consequence of early adoption>"VPN stuff is sandwiched between firewalls…" High strength hardware security was important because of early adopter stance that company has taken (using relatively untested, cutting-edge technologies).$$; ##monitor (all – some)##; $$<Reasons for monitoring activity>Reasons for monitoring all traffic coming in include tracing where an attack came from (*accountability*), *damage control* (turn service off on infected host before more malicious code is sent), and *cost-effectiveness*.$$
      Page: 31
      [CL]##policy for dealing with security breach over VPN (manager – direct)##

II. Company Priorities
   A. Flexibility/broadness of support
      Page: 31
      ##operational priorities: =flexibility and wide supportability over cost and security?##
      Page: 31
      ##assumed prioritization: =1.user flexibility, 2.security, 3.cost##
      Page: 31
      [JF]##ease of deployment vs. scalability: =prefer scalability, choose multiple solutions to accommodate all users, sometimes at the expense of security (one solution…multiple solutions)##
   B. Cost
      Page: 31
      [DT]##telecommuting priority: =company's benefit (productivity and efficiency)##
      Page: 31
      [CL]##Cost/security priority (cost - security)##; ##user/security priority (user -

security)##; $$<Split Tunnel Reason>Split tunnel only encrypts the packets that go through the tunnel. Implemented to *improve* user experience and performance$$
Page: 32
[CL]##catalyst for VPN implementation (user demand – cost savings)##; $$<Cost vs. Demand>While cost was the real catalyst, demand started the wheels turning.$$
Page: 32
[CL]$$<cost over security>CL once again indicates that this company will choose cost over security most of, if not all of the time.$$
Page: 32
[CL]##company priorities: (1) cost, (2) functionality, (3) supportability##
Page: 32
[CL]$$<Aggresive push for telecommuting>Cost savings have caused company to actually aggressively push certain people in small offices to work at home. This to me, is a real strong shift beyond simple encouragement. The telecommuting is no longer a voluntary alternative for the employee. I wonder if CL was actually implying that there is literal pressure on some people to work at home. That changes many dynamics of telecommuting and even opens up certain VPN security concerns$$

C. Security
Page: 32
[MS]##ideal company priority: =security##
Page: 32
[DT]$$<increased expense of viruses>Does increased virus infections, etc. neutralize savings in other areas from VPN? Big losses were experienced when Code Red and Nimda viruses brought down facility for days!$$
Page: 32
[MS]##considerations in VPN planning: [high security, number of users, stability/reliablity]##
Page: 32
[MS]##realistic company priorities (because of slumping economy): =1. Cost, 2. Security, 3. Maintainability/support, 4. Usability##

D. Usability

E. Functionality

C. Possible Quantitative Survey Tool

Security Compliance

All of the following questions refer exclusively to computers used for VPN access into your company

1. What type of internet connection do you have?
   (1) cable
   (2) DSL
   (3) Dial-up (56K)
   (4) Wireless
   (5) Other

2. Do you have firewall software installed on your computer?
   If yes,
   A. What brand is it?
      (1) Symantec Norton Personal Security
      (2) ZoneAlarm
      (3) BlackIce
      (4) Guard Dog
      (5) Other
   B. Was this the application distributed to you by your company?

3. Do you have anti-virus software installed on your computer?
   If yes,
   A. What brand is it?
      (1) Symantec Norton Anti-virus
      (2) McAfee
      (3) Other
   B. Was this the application distributed to you by your company?

4. How often do you check for operating system updates, such as service packs and security patches?
   (1) Once a week
   (2) Once a month
   (3) Less than once a month
   (4) Never

5. How often do you check for software updates, including service packs, security patches, and new virus definitions?
   (1) Once a week
   (2) Once a month
   (3) Less than once a month
   (4) Never

6. How many others use your computer on a regular basis?

7. Do other users use a personal or guest account to access your computer? (*yes/no*)

8. Do other users have access to any company files that reside on your hard drive? (*yes/no*)

9. Does any other person have the ability/knowledge to connect to the company network using your VPN account? (*yes/no*)

10. Do you disconnect the VPN connection when you are away from your computer? (*yes/no*)

11. Do you lock or log off your computer when you are away? (*yes/no*)

12. Do you write your VPN or local system passwords anywhere? (*yes/no*)
    If yes,
    A. Where?

13. Do you have your VPN password electronically saved on the login prompt so that you don't have to input it every time you log in?
    (1) Yes
    (2) No
    (3) This option is missing or disabled

14. How often do you change your VPN password? (*choose closest approximation)*
    (1) Every 30 days
    (2) Every 60 days
    (3) Every 90 days
    (4) Never
    (5) I use token-based authentication

15. Where do you store the majority of company files that you use while telecommuting?
    (1) Locally on home desktop or laptop
    (2) Remotely on company desktop or company server

16. If installed, do you ever temporarily disable your firewall or anti-virus software? (*yes/no*)