5-20-2004

Remote support technology for small business

Michael Luciano

A Remote Service Solution for Small Business

By

Michael David Luciano

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

3/1/2004

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in Information Technology

Thesis Approval Form

Student Name: Michael David Luciano

Thesis Title: Remote Support Technology For Small Business

Thesis Committee

Name	Signature	Date
Prof. Daryl Johnson Chair		5/20/04
Luther Troell, Ph.D Committee Member		5/20/04
Charlie Border, Ph.D Committee Member		5/20/04

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Master of Science in Information Technology

Remote Support Technology For Small Business

I, Michael D. Luciano, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 5/20/04 Signature of Author: ______________________________

Abstract

Small business is in need of a more efficient solution for managing their Information Technology support needs. Due to small business's need for custom solutions, IT service providers must dedicate highly skilled personnel to client business sites, incurring high overhead costs and restricting their ability to apply their employee base to multiple clients. This restriction in cost and flexibility places a high cost burden on small business clients, straining an already limited budget.

The use of remote IT support technology may provide the basis for a solution to these problems. By applying remote technology, an IT provider could centralize their employee workforce, managing clients from a single location rather than dedicating manpower to client sites. If the technology was available to support such a model, this change in the methodology could result in a more manageable solution.

Small business had the highest propensity to outsource IT support for the management of their hardware, software, web hosting, server/host management, networking, and security requirements. Many remote tools currently exist to support these needs, offering solutions for access, alerts, system monitoring, diagnosis, and reporting of a client's IT infrastructure.

Using these tools for remote support, a remote solution showed the greatest ability to manage the software, server/host management, and networking needs of small business organizations. Web hosting service requirements were strongly supported as well, although the use of remote solutions would cause a change in the current overall structure of web hosting support, leaving the solution more difficult to implement. In the areas of hardware and security, although many of the primary needs for support were strongly addressed, flaws were discovered that made the use of the methodology less than ideal.

The primary flaws of remote support resulted from the inability to manage hardware device failure, the inability to manage the network medium, and security issues resulting from the ability to separate a system administrator from the designated system through denial of service type attacks. Although each of these flaws displayed a significant issue with the use of a remote management IT solution, it was determined that the risk of each could be limited through the use of redundancy, offering a feasible work around.

From both a business and a technological perspective, remote solutions proved to be a viable alternative to on-site support for the management of small business IT needs. The total cost of remote solutions is extremely comparable to the average yearly salary of an IT employee, typically offering the same potential for the support of a client's IT infrastructure as a one time investment. In addition, remote solutions offer significant savings to the provider in the reduction of administrative overhead and the increased potential for business expansion, allowing for significant cost savings to be passed on to the client. Although the use of remote technology does not offer a perfect solution in its support of small business, the functionality which is readily available presents the strong potential to increase the efficiency of current small business IT support methods and offer more cost effective solutions to small business organizations

Table of Contents

List of Tables

I. Introduction

Most current information technology support providers concentrate their service in an on-site format, utilizing the space and resources of their client so as to maintain the stability of specified equipment or data. Due to the manpower and space required to incorporate this kind of service into the regular workflow of a given business, this solution can be very costly. In a small business setting, this cost restriction can make an on-site support solution untenable, resulting in either the insufficient coverage of resources or the absorption of a heavy financial burden(McLellan, 10).

A major percentage of the cost associated with this restriction is incurred through manpower, requiring separate employees to handle each individual client. With the emergence of remote service and remote control technology, it may be possible to reduce this cost by increasing an employee's ability to multitask, and thus reduce the company's overall manpower. In addition, as a remote service solution would reduce the need for client localized personnel, it would fit more into the structure of small business and could prove to be a better overall solution.

Beyond the direct cost of manpower however, it is important to realize that the business world as a whole is evolving. Employees who once were expected to report every day to a fixed location are moving out of the office, either working from home or becoming completely mobile, moving to wherever they can best benefit the company. The application of information technology has seen massive growth over the last ten years, showing an exponential increase in the number of software packages utilized by businesses, and the reliance on computing technology to reach strategic objectives. This decentralization of personnel and computing resources coupled with the increased reliance by companies on information technology is making it much more difficult to provide cost effective support for the average organization(Carincross, xii-xvii).

The decentralization of company employees has made on-site solutions much less efficient, reducing the percentage of company resources a provider can directly support. In addition, the extremely high number of software and hardware packages being utilized in a single company, coupled with the increased importance that this technology has upon the company's profit potential, is making it near to impossible to provide experienced and reliable support to all facets of an organization(Houweling, 1).

Larger service organizations have incorporated this service aspect into their support model, providing dedicated technical assistance and utilizing remote service technology to assist their primary on-site methods. Companies with the financial stability to purchase this support can have all of their technical needs met in this manner at a cost which spreads well over the breadth of the organization("A New Model...",1).

For smaller companies and smaller service providers however, this solution presents significant problems. Smaller support providers generally do not have the resources necessary to hire new employees for each new business environment, and smaller business clients do not have the financial stability to hire a dedicated group to maintain the technical needs of their organization. For both of these problems, remote service technology may be the answer(Dash, 1).

The primary question regarding this solution is whether or not technology has advanced to a point where a remote solution can be used to completely cover the primary needs of the average small business, or if the use of an on-site solution is still a necessary facet to small business IT support. Although it is obvious that use of local manpower can be much more cost effective than employing complicated technological systems to accomplish the same task remotely, it is not clear that any of these tasks are of primary concern to the average small business.

In total, the technical support needs of the average small business are not nearly as extensive as those of larger organizations. If remote service technology could cover this small segment of needs reliably, small business would not require a dedicated on-site staff. On the service side, if this remote technology provided a stable solution to the primary needs of small business, it would increase the ability of service organization employees to multitask, reducing their overall staff requirements and allowing those with specific technical skills to spread their expertise over a number of remotely supported organizations(Apicella, 1).

Technology exists to cover many of the primary aspects of remote service, including system monitoring, remote resource control, and backup solutions. These tools have primarily only been used as complimentary solutions to a full support topology, but have the potential to handle the entire needs of an organization. After examining the current remote support tools available in the market and observing the remote methods of support being implemented by service providers, it should be possible to determine whether the use of remote technology can be applied reliably as a full service solution to the needs of small business.

The purpose of this thesis will be to investigate the current information technology support industry to determine if remote service is a viable solution, both financially and technologically, to the most common needs of small business. To determine the answer to this question, the primary needs of small business will be determined through the use of market research, forming a framework of needs that must be met by support solutions. Once these needs are established, each specific task will be examined from the perspective of both an on-site and remote solution determining the economic and technological viability of the support method. Finally, this information will be examined at a strategic business level to determine the efficiency of using a remote solutions as a whole to meet the information technology needs of an entire organization.

By comparing the overall cost, efficiency, and dependability of each support method, and examining the full service solution at the strategic level, it will be possible to determine whether the remote solution topology is a practical answer to the information technology needs and cost concerns of small business organizations. The objective of this document will be to generate an answer to this question, opening up new possibilities for small business IT support and detailing the advantages and shortcomings of using remote technology in today's current business environment.

II. Caveats

Though this investigation will examine remote service technology as a replacement to the use of an on-site support topology, there a number of situations where remote technology will never be applicable. As these situations are very specific, they do not reduce the validity of this investigation, and will not be considered when determining whether a remote system can act as the sole means for a small business's information technology support topology.

Caveat 1: "Installation Will Always Require On-Site Support"

No matter what technology is used, on-site personnel will always be required to install the initial system at the small business site. Hardware and software will need to be integrated with the information technology architecture of the small business, and technicians will need this access to the client's resources to set up the initial topology and to ensure stable end to end communication with the provider.

Caveat 2: "Clients Without Internet Access Will Not Be Examined."

To utilize any remote support topology, the provider must be able to access client resources via the internet. Clients which do not have internet access will not be able to benefit from the advantages that remote technology could afford them, and, as such, clients in this classification will be ignored for the purpose of this study.

Caveat 3: "Clients Will Be Assumed To Have Minimal Technical Expertise."

Although many small business organizations that require technical support will either offer a product or service which is technical in nature or have employees that have significant technical expertise, for this investigation, it will be assumed that the provider can only expect a minimal level of technical competency from its clients. By this assumption, to be deemed viable, remote support solutions implemented by the provider must be fully manageable without the utilization of any on-site assistance.

III. Business Analysis of a Remote Support Implementation

From a business perspective, the shift from on-site to remote solutions must be supported by the underlining small business framework before organizations will accept such a change to their service support environment. If the factors surrounding the implementation of a remote topology do not fit with the basic objectives of the average small business, then the technical feasibility of the solution will be unimportant, as businesses will not invest in the change(Morrison and Slywotzky, 22-26).

These business factors set objectives for the technological solution by detailing the major concerns of small companies, and creating restrictions that constrain the service support model to the limits of the average small business. Small business restrictions will act as the basic groundwork for each compared support solution, and will have a major impact in determining the feasibility of remote and on-site topologies.

Although these restrictions will result from the underlining business factors prevalent within small companies, the factors themselves will form an architectural framework that solutions must fit into so as to be feasible to the average small business. These business factors will be investigated from both a strategic and situational standpoint, examining how they mesh with both the overall concept of remote solutions and with the individual remote and on-site answers to primary small business needs.

A. Business Factors Supporting an Overall Shift to a Remote Support Topology

The average small company uses three major business factors to determine which information technology solution best fits the needs of their organization. Small businesses use the overall cost of the given solution, the ability of the IT service provider to meet schedules and deadlines, and the technical capability of the service provider as critical indicators of whether the solution will work for the needs of their organization individually, as well as in deciding between two competing service solutions(McLellan, 9) As these are the primary determinates of small business decisions surrounding their utilization of information technology, these same factors can be used to examine the strategic feasibility of an overall shift to a remote service topology in the small business sector.

1. Cost

Small businesses have a limited budget with which to spread across the breadth of their information technology needs, and thus are very concerned with the overall cost of a given solution. Although medium to large scale businesses are often able to spread the cost of high end solutions across the entirety of their organization, small companies are not able to employ such economies of scale to their advantage. Small organizations, because of this constraint, generally employ their information technology infrastructure in order to maintain a stable business environment rather than as a means of gaining a competitive advantage from the solution. These factors keep small businesses very cost conscious, and many devote considerable time towards reducing their overall expenditure in this regard(Kempf and Krammer, 1).

A major problem exists surrounding this idea however, as small businesses are extremely inefficient in managing the cost of information technology services. As per a Gartner Group study examining the 2003 business environment, the smaller the company, the greater the spending on outside IT services providers. For the business sector as a whole, overall spending on information technology solutions was reported as twenty-seven percent of the total IT budget, while small companies reported their spending as thirteen percent higher, at forty percent. In addition to this, as small businesses do not primarily use their information technology solutions to gain competitive advantages in their main line of business, this higher outlay leaves very little possibility for receiving returns on investment, and is often considered a sunk cost(McLellan, 10)

The forced focus on using information technology strictly as a means of keeping the business running has caused small businesses to spend money on support elements, often to the detriment of improvements to their existing system. This strategy often has the effect of impairing a company's ability to maintain current performance levels, paying out more funds to support their dependence on older, less efficient technology(Kempf and Krammer, 10).

Most of the cost constraints suffered by small businesses are directly related to the company's inability to directly afford the price of manpower associated with their information technology needs. For businesses whose main line of work is non-technical in nature, the cost of staffing a separate department to administer and maintain the hardware and software needs of their infrastructure is infeasible(Brown and Krammer, 10).

Currently, due to these budget flexibility limitations, the smaller the company, the more likely it will outsource its information technology support(McLellan, 2-7). Although this solution is a much cheaper and more reliable alternative to handling information technology support in house, small companies still incur the high cost of manpower associated with the service they require, showing that this choice is still only the better of two inefficient solutions.

The cost constraints currently hindering the ability of small businesses to support their information technology requirements demonstrates the need for a new support solution that makes more efficient use of manpower. To support this idea, Garter Group studies indicate that the budget pressure of maintaining their current information technology infrastructure is causing small businesses to look for other more cost effective alternatives to handle their IT needs. This did not however indicate that there was an expected overall decrease in the spending of small businesses to service the needs of their information systems, showing that, although small businesses are willing to incur the cost requirements of their technology infrastructure, they are currently looking for more efficient means of support(Kempf and Krammer, 12).

A remote service solution seems ideal to handle the cost constraints of small business. Remote systems allow the multitasking of information technology needs, reducing the overall cost of manpower incurred by either internal or external support organizations. This increased cost efficiency could transform the use of information technology systems within small businesses, allowing for companies to maintain a more up to date technology infrastructure, or allowing them to make more competitive use of their internal systems. As small businesses are already looking for more efficient alternatives, if remote technology can meet the needs of small businesses, the cost of the solution should prove to be a major benefit to incorporating the support design(Brown and Krammer, 10).

2. Timeliness

The most important factor for any business when making a final decision whether or not to hire an external information technology service provider, is the ability of the provider to meet schedules and deadlines(McLellan, 11). The presence of on-site personnel meets this need directly, but is costly to the client, directly increasing the cost of service by the salary of the dedicated personnel, as well as forcing the client to make workspace available for the consultant. In this design, cost can be saved by either moving the consultant off site, increasing the response time of the service organization to problems, or by lowering the consultant's dedication to the specific business, but each savings in cost equates to a loss of timeliness.

On the support side, a similar situation exists. To provide consistent responses to client problems proves just as costly, either by the dedication of a single individual to handle the needs of a site, or the cost of maintaining office space central to client areas, so as to reduce the time of travel. Beyond this however, support organizations are forced to incur the cost of redundancy, hiring many individuals of similar skill types to handle the needs of each client individually. Although these employees are not hired on a one to one basis for each client, each overlap of their employees significantly impacts the overall timeliness of their support design, adding travel and orientation time to each service call(Dash, 1).

A remote solution seems ideal when considering the response requirements of client businesses. If a remote service design could cover the needs of small businesses, the topology would remove the overall need for on-site consultants, allowing these same individuals to access client resources from nearly any distance. This implementation would allow the client to save the cost of creating workspace for the support professional while still receiving near immediate response time(Apicella, 1).

On the support side, it seems as if the cost of immediate service would be much more efficient under a remote design. The ability to service client problems from any distance would reduce the need for a physical company presence to be established in central client areas and allow service organizations to operate primarily from a reduced number of sites. Furthermore, with the ability to service client problems immediately without the dedication of a specific individual to a client site, and the elimination of travel time to handle a businesses most common problems, support organizations can utilize the benefits of redundancy, allowing their technicians to efficiently cover the needs of multiple clients. A remote support solution could also open up the possibility of using automated technology to monitor the working condition of a client's information technology infrastructure, allowing support organizations to handle service problems even before the client becomes aware of them.

If a remote support solution could meet the basic needs of small business, the topology would seem to have an impressive impact on a providers ability to efficiently and cost effectively respond to service calls. In addition, it is apparent that the cost requirement of maintaining high levels of timeliness would decrease greatly, allowing a major cost savings to be passed onto small business clients.

3. Technical Capability

Once the concerns of cost and timeliness were satisfied, most small businesses used the provider's overall ability to meet the current and growing technology needs of their organization as the next critical determinant in selecting an IT service provider. Incorporated in this requirement was the provider's ability to administer the hardware and software that was critical to their business, as well as the overall breadth of skills and knowledge maintained by the service organization. In this respect, most small business were looking for a provider who would be able to support to their business no matter what changes occurred in their company over the course of the future(McLellan, 9). This requirement poses some problems for service providers.

As was mentioned earlier, cost concerns are a primary focus for small businesses that are deciding on an information technology service provider. For the provider to keep costs low, only a small amount of manpower can be devoted to any given project. Although this low level of manpower could be enough to handle the administration end of their service initially, over time it is unreasonable to assume that this same level of manpower will contain the necessary skills and have sufficient depth to cover the growing needs of the organization(Houweling, 1).

To provide the necessary support, a provider could place technology specialists within central office locations, giving their organization the ability to limit their cost of coverage, but generalizing these skills does not work very well for small business support. Most small businesses find that packaged software does not directly meet the needs of their organization, causing most to invest in a custom solution(Kempf and Krammer, 12). These solution designs cause IT support personnel to have both site and skill specific knowledge, reducing the number of clients a single specialist can cover effectively, and increasing the provider's overall required manpower.

As the profit of administrating the information technology needs of small businesses is generated through servicing multiple clients rather than in the investment into a single large contract, the need to handle the growing needs of clients can cost a provider business. Unless a small business resides within the scope of coverage of a central office location, providing this kind of service to a single small business is unprofitable, forcing the provider to turn away available business and limiting the overall range of clients they are able to service. In the same respect, if an organization chooses to only service the immediate needs of businesses, it will be difficult to maintain clients as businesses evolve, effectively limiting the future potential of their own organization.

In this manner, manpower becomes a restriction to servicing small business information technology needs over the growth of organizations. Implementing any strategic level business plan which involves use of direct manpower to cover the evolving needs of clients will generate a significant amount of redundant overhead. This extra overhead increases the overall cost of operations for the provider, and creates an increase in the cost of service to the client.

Remote technology can be utilized to make more efficient use of a provider's skill base by increasing the overall area of coverage for each service technician. Ideally, remote service technology squeezes the number of central locations required by expanding the range of coverage. Service technicians and specialists are squeezed in the same manner, grouping more of the organization's technical knowledge into a single location.

Using this design, the need for redundancy at high level employee skill expertise is reduced, and problems that arise at a client site can be addressed by a team of individuals, making much more efficient use of the provider's employee base. This flexibility in the application of a provider's skill base can also expand business operations as a whole, giving the provider access to new clients that would have otherwise been limited by their proximity to a central office.

Lastly, if the skills required by the evolving needs of small business can be covered sufficiently through the use of remote technology, this business strategy would allow a provider to efficiently maintain clients throughout their entire existence, exponentially increasing the long term potential of the business. The centralization of a provider's employee skill set within such a topology should allow an organization to absorb any overhead costs associated with maintaining support over the evolution of their clients, by its ability to immediately apply the new expertise to the whole of its current client base and by using its increased expertise to target new market areas.

B. Business Factors Resisting an Overall Shift to a Remote Support Topology

Although a remote service topology seems to satisfy the major concerns surrounding the information technology decisions of small businesses, there are some factors that could hinder the acceptance of the new design. These factors are not as prominent as the concerns that center around cost, timeliness, and the technical capability of the provider, but as they will have some impact on small business decisions, each requires examination.

One of the most common trends native to small businesses is the desire to keep tight, in house control over their information technology resources. This trend could prove to be problematic for a provider wishing to incorporate a remote service topology, as small businesses may be resistant to grant remote access to systems (Brown and Krammer, 2). Although the benefits of having a remotely monitored and supported system are substantial, small businesses may feel more comfortable with a more closed network, choosing to use an on-site service provider or handle their administration duties in house.

This issue can create problems for a service provider that employs strictly remote solutions, but the trend does not impact the actual solution as significantly. As remote service solutions can be employed in house as well as externally, allowing an organization to administer their own machines and maintain internal control over their company's data, the solution is still a viable method to meet the organizations needs. The problems emerging as a result of this trend will be born as a product of the internal or external provider's method of service, and not the inherent design of the solution.

Another issue surrounding the small business acceptance of remote service integration is the impersonal nature of the solution. Small businesses desire a close relationship with their service provider, and the use of remote technology may be too subtle for the company to accept(Kempf and Krammer, 10). Although this trend should not keep small businesses from employing the service solution initially, it may hinder the long term client-provider relationship. Without an on-site presence, it will be difficult for small businesses to observe the value of the consulting agency provides to the company. Additionally, with remote service, technical problems will be overcome using less invasive methods, and will be far less obvious to the client than if an on-site solution was employed. This background activity may be misconstrued as inactivity, leaving the small business with the false impression that the remote service provider is not fulfilling the requirements of their contract.

Although this can be combated by a service organization that keeps a client up to date on their support activities, this will not be as prominent a reminder as would be the obvious and ever present activities associated with an on-site solution

IV. The Primary Information Technology Needs of Small Business

The overall structure of small business makes the use of information technology unique within the framework of its organization. Lower manpower, a reduced budget, and the management of a small amount of overall resources all impact the manner in which information technology is used, and signify certain aspects of its application(Brown, 2).

The small business use of information technology tends to be very simplistic, using resources to act as a backbone for an organization's primary business activities. Most small businesses utilize their information technology topology as a means of maintaining a stable operating environment, and do not look to this technology to generate a return on investment. Instead, the information technology implemented in this manner is viewed simply as a cost of doing business, and is financially treated in the same manner as office space or utility costs(McLellan, 10).

Before examining the direct application of remote technology to a small business environment, it is necessary to specifically determine the primary methods in which this technology will be used within that level of organization. Determining the manner in which small businesses utilize their information technology resources will establish whether remote technology can be suitably applied to that environment, and will give a basis for comparison between using remote and on-site methods to solve the organization's need.

To determine the primary IT needs of small business, an examination was conducted into the technological solutions that were most commonly outsourced by service providers to smaller organizations. This data, generated primarily through the use of a Gartner study, was then compared to a separate investigation into the local information technology support industry to verify the data collected as well as to be complete about any emerging technological needs within the average small business environment(Hyder).

The results of the independent investigation supported the information detailed in the Gartner study, generating a basic list of the most common information technology problems that small businesses were most likely to outsource(Brown and Young, 28). The propensity of small business to contract out these solutions identified the concentration of their information technology budget, specifying their primary technological needs and determining which areas they had the most difficulty finding the skills to cover in house. By using this list of outsourced needs, it was possible to investigate the viability of applying a remote support topology to the small business architecture, examining the current applicable technology, financial feasibility, and effectiveness when compared with traditional on-site solutions.

These determined needs are investigated below, examining each level of functionality and feasibility individually, and using the information gathered to conclude upon the best method of support for each small business need. Rather than conducting these examinations in a descending order based on small business's propensity to outsource services, these studies will be performed in a more hierarchical manner, allowing each study to supply information to the next. In performing the investigation in this manner, it was possible to eliminate the reiteration of ideas and solutions covered in lower level investigations, and to better concentrate on the central concept of the current study. However, as the propensity of small business to outsource each technical need was considered to be an important piece of data, it was included in each study to be used as a point of interest and reference.

Propensity for Small Business to Outsource Support

Hardware Support	(Propensity to Outsource: 40%)
Software Support	(Propensity to Outsource: 40%)
Web Hosting	(Propensity to Outsource: 51%)
Server/Host Management	(Propensity to Outsource: 36%)
Network Management	(Propensity to Outsource: 25%)
Security Services Management	(Propensity to Outsource: 25%)

A. Hardware Technical Support (Propensity to Outsource: 40%)

Information technology hardware resources serve as the basic infrastructure that allows an organization to maintain a stable flow of business operations. No matter what advantage the business hopes to glean from their use of information technology, they will need hardware to do it. For the organization to reap consistent benefits from their investment, utilized hardware must be seamless and dependable. As this performance requirement demands constant support on a component of the organization that, although vital, does not fall within the main profit line of most small businesses, it can create problems for organizations that do not have the manpower to support it.

Although small businesses utilize their information technology hardware resources in the same manner as their larger counterparts, the financial burden of supporting these resources is often too costly for them to manage in house. This difficulty causes a sizeable number of small businesses to outsource their hardware support, eliminating the need for the hiring of personnel specifically assigned to these resources(Brown and Young, 28). As small organizations are likely to utilize hardware from a number of different vendors, outsourcing this need is attractive, as it places a significant burden of proficiency and knowledge of the industry outside the bounds of the organization. Although this solution takes a major strain off of the organization by keeping the majority of a company's employees devoted to the main line interests of the business, it is still far from a perfect solution(Brown and Krammer, 3).

Hardware support providers dealing with small business clients are primarily hired to keep designated equipment running smoothly, minimizing downtime in the case of hardware failure(Brown and Krammer, 7). This task is most easily accomplished by dedicating manpower to the business site for the consistent monitoring of hardware performance, allowing the provider to react to problems as they occur. However, this level of dedication is costly, and requires the small business to have sufficient physical space to devote to the outside consultant.

Alternatively, the service organization can dedicate manpower to a given area rather at a specific business site, spreading the provider's employee skill base across a number of different clients. This solution is more cost effective, but reduces the level of service the business can expect from the provider, as it adds the time of travel and response to overall down time. Using roaming personnel is also only effective if the provider is handling a number of different clients in the same general area, making it a very location specific solution. However, even if these problems were somehow circumvented and a low cost on-site technician was designated to a small business, there are still a number of issues surrounding this solution..

A single individual will, for the most part, only be able to handle one issue at a time, creating difficulties any time the information technology hardware infrastructure is suffering from more than one concurrent problem. In addition, the knowledge base of a single technician can only cover so much material, allowing for the possibility that problems will arrive that he or she cannot handle without assistance. In those cases, the technician will either be forced to communicate with their service organization and attempt to step through a solution, or a specialist will need to be sent to the business site by the provider. In either situation, the client will suffer an increase in downtime, either by the difficulties experienced in trying to solve a problem through an intermediary or from the travel time incurred while the specialist travels to the site(Brown and Krammer, 11).

These problems limit the provider in the same manner that they create problems for the client. While service organizations do not directly suffer the severity of impact to their business as would the client, these issues can restrict their coverage of small businesses in its entirety, causing them to only take on small clients when their needs fit a certain mold or when they reside within a certain area of coverage. Even more important however is the performance impact suffered in using this kind of support. Although a higher response time and increased down time are merely products of applying traditional support methods to small business clients, the lower level of service will be seen as simply inefficient, surfacing opinions which will inevitably hinder the overall profitability of the business(McLellan, 35).

Due to these issues, it is both difficult for small businesses to receive the resource hardware support they need and for service organizations to provide it in a cost effective manner. Remote technology may be able to solve these problems by removing the element of on-site personnel, yet maintaining immediate access to small business hardware. This solution would also allow providers to efficiently support more small business clients by giving them the ability to access a greater range of businesses, as well as utilizing an entire staff of skilled individuals to solve problems as they occur. Since this solution would not require the placement of personnel to a specific site or roam offices in client locations, the provider will be able to utilize the down time of their employees to solve problems more efficiently, and would see an overall lower cost to provide service.

1. Remote Hardware Support Technology Investigation

For remote hardware support to be feasible, the current technology available must handle remote access to client resources, the monitoring of client resources from the provider's site, the testing and diagnosis of remote systems, and the correction of client hardware problems. Each of these requirements have been examined individually below, investigating technology that best fit the specific hardware support constraint.

a) Remote Access to Hardware Resources:

To successfully support a client's information technology hardware infrastructure remotely, a provider must be able to gain access to client resources, regardless of their condition. Normally, if examining client resources during normal business hours, an individual at the client site can aid the service provider by handling the manual tasks of powering and rebooting machines when they are in a down or error state, but this is not the best solution.

Ideally, a provider needs to access client resources during off hours, allowing examination of resources and the conduction of tests while the client is not utilizing their hardware infrastructure. For full coverage by the topology, it must be assumed that, in these situations, client hardware devices will be powered down and no hands-on assistance will be available at the client site. There are a number ways that a hardware support service provider can meet these requirements.

Hardware devices can be activated, shut down, or reset remotely using 'Wake on LAN' technology. 'Wake on LAN' is an Intel networking technology solution that allows a user to remotely power on systems via a connecting network, by use of technology tied into a system's network adapter and motherboard(Networking, 1). The specialized network card is connected to two specific pc hardware components, plugged into a dedicated 'Wake on LAN' port on the motherboard and the power supply. The system sits idle awaiting a special packet, called a 'magic packet', to arrive across the network, and authenticates the exchange on the network card itself. Once authenticated, network management software is used to specify system start up through this process(Remote PC Wake-Up, 1).

In addition to manipulating the state of the hardware device, the provider will need to access monitoring software on the supported machine. Applications such as NetSupport Manager (Net Support Manager, 1), PC Anywhere (Symantec, 1), and NetOP (Caballero, 1) will allow a remote user access to a specific system directly, operating as if the user was actually sitting at the client's workstation. By using these packages, a hardware service support provider can access applications on client machines, making use of any installed hardware monitoring and troubleshooting software.

b) Remote Monitoring of Hardware Resources

Remote monitoring is not needed for all hardware resources. Only business critical devices, such as servers, require dedicated technicians to ensure the reliability of devices at all times. For those parts of a client's information technology infrastructure that are critical, at a minimum, the client should ensure that the cpu, memory, and disk storage functionality are constantly monitored(Adams et. all, 3).

There are a number of software packages that can accomplish this task. An application developed by Mercury Interactive, called SiteScope, monitors server resources, determining the stability of hardware, the number of system errors encountered, and the number of rejected client requests, giving a service provider ample warning of problems that develop on the client machine(SiteScope, 1). Another similar monitoring application is Intel's LanDesk Client Manager, designed to monitor computers for hardware problems and report any issues encountered with the device's hard drive, fan, power supply, or temperature(LANDesk,1).

By having constant data pertaining to the active working state of the hardware device, the provider can observe changes in activity that could be problematic, and prevent greater damage to the monitored equipment. Each of these packages are designed to alert a system administrator when a problem occurs and generate a report of the corresponding issue, allowing for the customization of events that will signal their organization when a supported system begins to behave outside its normal operating parameters.

Using applications such as SiteScope and LanDesk in conjunction with remote hardware and software access methods can allow a service provider to connect to client machines, observe the activity of critical client devices, and receive alerts when the monitored hardware begins to operate below optimum performance levels.

c) Diagnosis and Correction of Hardware Resource Problems

When a critical device enters an alert state, a remote hardware service provider must be able to act immediately, accessing the device in an attempt to diagnose and correct the problem encountered. There are a number of highly sophisticated tools that can aid the provider in this regard, allowing the organization to observe and manipulate the controls, constraints, drivers, and hardware settings so as to determine the source of the problem.

Sandra, a SiSoftware application, is a full service forensic hardware package that incorporates modules into its design depending on what hardware the support provider wishes to monitor. Sandra, an acronym for the system analyzer, diagnostic and reporting assistant, is an information & diagnostic utility, used to examine, benchmark, and generate reports on hardware devices. Although this tool is similar to those examined under the section dealing with the monitoring of hardware resources, Sandra is much more detailed in its reporting, making it not fit for everyday use(Who/What is Sandra?, 1).

Applications are advancing towards a more proactive use of hardware support applications, giving the user more power over the targeted environment. A product developed by Jungo, called WinDriver, allows an organization to access a target system through any network connection, and scan, detect, and test both attached devices and associated peripherals. By use of this technology, a service provider is able to step through nearly every device present in a client machine and search for faulty hardware. In addition to this, WinDriver also contains technology that allows the user to debug drivers, stepping through the code associated with hardware devices to determine if the hardware that is working improperly is getting the correct instructions for what it is trying to do (New Remote Hardware, 1).

New advances in embedded hardware support technology are also emerging, aiding a service provider in being able to remotely correct hardware problems. American Megatrends offers a product called the Mega RAC G2 that incorporates the access, monitoring, and maintenance into a single card. The Mega RAC G2 operates off of its own PCI card, creating an "Out of Band" access point, or a connection which does not rely on the client's LAN for contact to the client's devices. Beyond the stability of its access to client devices, the product offers an OS independent solution, allowing for the maintenance of machines no matter what the state of its software, remote control power cycling and rest capabilities, hardware resource monitoring and diagnosis, and secure access, lending an extremely powerful tool for remote hardware support(AMI, 1).

Using this range of technology, a hardware service provider can run a full service diagnosis on any supported system, test, and troubleshoot the drivers and devices that keep the system running. Doing so allows a service provider to control the operating activity of the supported machine, correct problems, and alert the client to irrecoverable errors in their hardware before the problem affects the operating activity of their organization.

d) **Remote Hardware Support Methodology**

With the technology available, it is possible for a hardware support provider to implement a scalable remote service solution, supporting varying levels of complexity and need at the client site by using multiple layers of support technology. To match the variation in each level of a client's information technology infrastructure, a different level of support and a unique set of support technology should be used.

Workstation support is the least critical facet of a client organization, but must be supported, as the state of the workstation often determines whether an employee can efficiently complete the work they are responsible for. Hardware issues can also tie up important organizational data, requiring that type of integrated support. For a workstation, a software access method is required, coupled with a diagnosis package so that technicians can remotely investigate device problems without being on-site.

Server hardware support is much more critical to the operation of a client business. Shared files, web access, or other resources could shut down an entire business if hardware problems occur, making integrated server hardware support extremely critical. There are a number of different ways to handle server hardware support, depending on the topology of the client organization.

If the service provider either holds ownership, has some say in the client's purchase of the device, or is dealing with relatively new technology, hardware access can be accomplished with the simple install of a 'Wake on LAN' capable PCI network card. Using this technology coupled with a software access package will give the organization full control over the client device, and allow them to manipulate the server's operating parameters whenever needed. An in depth monitoring application should be used to watch for abnormal events and activity, using built in alerts to notify the service provider in case problems arise. Finally, a diagnosis tool should be installed, giving the provider the ability to conduct tests and conduct deep investigations into errors when problems do occur.

If the provider is unable to use a basic 'Wake on LAN' network card to handle remote access to a client server due incompatible chipset technology, or if the server is extremely critical and requires a secondary point of access, the provider can use a full service hardware solution to meet the client's needs. Using a support card such as AMI's Mega RC G2 gives the provider very powerful access to the supported device with a very simple install. As the card provides hardware access, OS independent integration, monitoring, and diagnosis capabilities imbedded directly into its design, there is no need for any other tools to be installed.

2. Remote Hardware Support Business Factor Comparison

a) Cost Examination:

The cost of implementing a remote service topology is relatively small. The software and hardware methodology detailed in the earlier section examines the base technology required to cover each aspect of the client environment. By using this as a model for purchase and applying the pricing structure to overhead costs, it is possible to determine the total financial impact the provider absorbs with the support of each critical device.

For hardware access, if a hardware service provider has some influence in the client's purchasing of their information technology infrastructure or if the client already has 'Wake on LAN' capable motherboards within the devices they wish to support, only a 'Wake on LAN' PCI card is required for remote reset and boot. These cards are of relatively low cost, making them easy for the provider to keep many in their inventory for use with new contracts or replacement(ZDNET, 1).

Software access is more expensive than hardware, with prices scaled reciprocally against the number of licenses purchased in a package. Out of the three packages examined, only PC Anywhere requires a yearly renewal cost, the others having a one time cost associated with the purchase of the product, making it the most expensive of the three(Symantec, 1). The straight purchase price structure of NetSupport Manager (NetSupport Manager, 1)and NetOp (Caballero, 1) allow a provider some versatility, in being able to shift their licenses to different sites with the gain or loss of new clients. Both of these packages have reasonable pricing schemes, with NetSupport Manager being more cost effective with a lower number of users and NetOp cheaper on the high end. The inability of an organization to acquire the cheapest pricing on a 'pay as you go' format is limiting, but should only affect the provider while in the early stages of business growth.

Monitoring technology implemented into a remote support scheme can be rather expensive. Although the cost of using LANDesk Client Manager is very small, the capabilities that the software provides is limited, and should only be used for lower impact devices(LANDesk, 1). Although SiteScope is an extremely thorough monitoring application, offering a great deal of reports and alerts that would be valuable to the provider, its cost is rather prohibitive(SiteScope, 1). Since there are other, more efficient ways that the provider can monitor a client's critical devices, this software should be avoided altogether.

Due to the low cost of the product, critical devices should be covered by use of the Mega RAC G2 board. With a full service package embedded into the hardware of the product, the provider can avoid the costs of hardware access and monitoring, while establishing a second method of connection, adding more stability to the service(AMI, 1). For strict diagnosis, the provider should use Sandra which offers a great number of testing, troubleshooting, and reporting options at a very affordable, one time price(Who/What is Sandra?, 1). WinDriver software, although extremely useful in correcting driver problems, is too expensive to be used effectively in anything but the most critical device(Jungo, 1). A summary of the pricing schemes used for both low and high impact support are detailed below.

Low Impact Service (Cost to cover 100 machines)

Hardware Access	
Wake on LAN' PCI card	$1600
Software Access	
NetOP	$3800
Monitoring	
LanDesk Client Manager	$4900
TOTAL COST	$10300

High Impact Service (Cost to cover 100 machines)

Hardware Access/Monitoring/Diagnosis	
Mega RC G2	$59,985
Sandra	$19,999
Software Access	
NetOP	$3800
TOTAL COST	$83,784

b) Timeliness Examination

A remote hardware support topology offers advantages that can significantly increase a provider's overall speed of service. Through the use of remote access technology, a hardware service provider can gain fast easy access to a client's critical resources, monitoring and correcting issues without interfering with the client's regular business activities . The ability to have immediate direct access to the client system is a major advantage for both the client and the provider, and, although there is no dedicated manpower present at the client site, all system resources can be accessed, modified, and corrected from nearly any distance.

This topology also allows for the more flexible application of a provider's work effort, concentrating the activities of personnel on critical issues as they occur, rather than dedicating each employee to specific client site. This structure also allows for a provider to maximize the productivity of their workforce, applying idle employees to expedite the correction of immediate problems(Remote Support Buyers Guide, 1).

The primary problem with remote hardware support occurs when the provider requires access to the supported hardware in order to correct a given problem. Without an on-site technician, no physical examination or test of physical devices can occur. Although this will not prove to be a major issue when the provider is dealing with small problems, when dealing with more complicated hardware issues, certain physical techniques, such as device swapping, can be a significantly important method of test, and require a on-site technician to accomplish. Since the assets and locations of a remote service provider are not necessarily designed to be located in close proximity to its clients, when use of these techniques is required to correct a problem, this issue could significantly impact a provider's ability to quickly service the client, greatly affecting the efficiency of their support.

The provider will suffer this same impact in any case where a device suffers complete hardware failure. Even if the problem can be diagnosed remotely, if a part must be replaced, an technician must be on-site to remove the damaged part and install the new one. Although every second lost reflects poorly on the provider, when the device is critical to the business of the client, every bit of delay can be extremely harmful to the profitability of the client organization.

c) Technical Capability Examination

Using remote technology, a provider is no longer constrained by the limitations of dedicating technicians with specialized skill sets to a client site. When problems occur, they are handled using remote access methods to access client resources, and every idle technician can be used to identify and correct problems. By using software and hardware tools for remote monitoring, diagnosis, and correction, the provider can be alerted the moment the client system begins to work outside accepted parameters, quickly determine what problems exist in the client system, and correct them(Liam, 1).

The combination of these two aspects allow an organization to bring all of its available resources to bear against a problem discovered in its earliest stages. More importantly, remote hardware support handles these problems behind the scenes, and does not interrupt the regular flow of business with its activities.

Remote hardware and software tools allow for a technician to gather a large number of highly detailed reports regarding the inner workings of a client system. Through the use of these solutions, driver problems can be corrected, hardware functionality can be tested, and benchmark data can be used to compare the performance of a specific device over a significant period of time.

As mentioned in the discussion of timeliness however, the technical capability of the provider is hindered severely if devices need to be swapped out of client machines for testing purposes or if a part needs to be replaced completely. The inability to manage these critical tasks using the basic framework of a remote design is crippling to the provider's technical capability when operating under this form of topology, and cannot be corrected without on site assistance.

3. Remote Hardware Support Conclusion

Many tools currently exist to support a remote hardware service topology, providing methods of access, monitoring, alert, and diagnosis, which can be used to correct hardware issues from a remote location. A remote topology is very strong in dealing with critical devices, offering multiple methods of access and cost effective tools to benchmark, examine, and test problems occurring within a given system. Unfortunately, there are a number of significant drawbacks in using a topology of this kind to handle all of an organization's hardware support needs.

On the lowest level of a client organization, a remote hardware service provider must be able to support employee workstations. To accomplish this efficiently, a provider must be able to gain access to the given device and manipulate the system on both a hardware and software level. These requirements are not a major issue for support if the provider is contracted when the client is purchasing new hardware, such as in a point of transition, or if the client's current hardware is relatively new. Since the provider will generally not have control over these aspects however, leaving open the possibility that the client will be using older technology, supporting a simple bank of workstations can prove problematic.

Remote access and support is based off of some form of 'Wake on LAN' technology. To use this technology, a workstation must be using a chipset that is designed for this form of access. Although most new motherboards are made to compatible with this technology, older technology is not, preventing a service provider from using a 'Wake on LAN' PCI card to remotely power and reset the system.

This does not tend to be an issue when dealing with critical devices. Hardware that is critical to the workflow of a great number of employees or the profitability of the organization is almost always of comprised of newer technology, and compatible with remote boot support.

The most significant problem inherent to this topology is found in the physical manipulation of hardware devices. As a major facet of hardware test and repair, the inability to swap devices as a method of test or replacement is a major detriment to remote hardware support.

As a whole, a remote hardware support topology has a number of powerful tools that can be used to limit the need for on-site technicians to be present at the client site, but it does not eliminate the need completely. The inability to guarantee the ability to remotely cycle the power of every hardware device requiring support, and a provider's inability to physically manipulate client devices remotely make on-site technicians a critical aspect of any hardware support topology.

B. **Software Technical Support (Propensity to Outsource: 40%)**

Where IT hardware infrastructure is an extremely important aspect of small business operations, serving as the backbone for their information technology architecture, the tools that are used to manipulate data and complete the main line interests of the company are just as vital. Although not as prone to an outright failure, software resources span an even greater range of vendors and designs than hardware resources, creating a significant need for proficient support. As with hardware resources, most small businesses do not have the financial resources, manpower, or desire to devote a segment of their employees to manage these needs, so outsourcing becomes a viable alternative(Brown and Young, 28).

For most small businesses, access to an expert on utilized software packages is not a problem. Licensed software normally is provided with help desk support, packaging this knowledge resource in with the purchase of the application. Although this method of bundling product and service into a single package seems to be an efficient way of eliminating cost concerns surrounding software support, the truth is not so simple.

An information technology service organization filling the software support need through licensing, must bundle the cost of both the software product and support staff directly into their product. In doing so, the support organization must employ a sizeable overhead of help desk technicians to cover the needs of their expected sales. As this employee overhead is implemented as an estimation of marketing data, the company can easily under or over estimate the expected number of clients, making this a rather inefficient way of handling business, and passing on unnecessary cost to the client.

Most help desk organizations operate by use of a phone bank, answering problems as calls are received, and passing them to the correct tier of support personnel depending on the severity of the problem. This method requires the description of the problem to be related via phone, relying on the technical proficiency of the client to communicate his or her issue and the deductive skills of the technician to work through the client's difficulty with the software. Without the ability of the technician to actually examine the problem personally, forced to rely on the clients ability to follow instructions given and relate information, this method can become very inefficient and time consuming(Apicella,1).

The communication barriers present in this method of support could be corrected by the use of remote service technology. If the outsourcing agent could implement applications on the client side to allow for the remote management of a client's system, the technician would not have to rely on second hand information to correct the problem. By doing this, the technician could observe the problem without needing to be at the client site, and either quickly correct the issue or pass it up to another tier of support.

If applicable, this advantage would greatly benefit any support organization, increasing the timeliness of their efforts and reducing the overall cost of employee overhead. Furthermore, an organization that implements such a system would gain the advantage of locking in customers by having a more invested infrastructure with their clientele. Most businesses prefer to deal with organizations and processes that they are comfortable with, and would be less likely to change to a competing software vendor if their system was integrated in such a manner.

Overall, by implementing a remote management system for software support, a small business client could become a more profitable interest to information technology service organizations. This method could lead to a lower overall cost for software licensing, more efficient support for business clients, and even a more customized plan for sales related to small companies, as the software as a whole becomes easier to manage and the fluctuation of service support clientele becomes more stable. In any of these cases, the use of this technology would bring an advantage to both the client and vendor side of the support model, and thus merits investigation.

1. Remote Software Support Technology Investigation

A remote software support topology must be able to provide easy seamless access to a client's machine. The better the communication is between the technician and the client, the better the efficiency and quality of service will be. In addition to providing access, the topology must be able to generate clear concise data regarding the state of the given computer, giving the technician as much data as possible so as to provide immediate insight into the current state of the client's device.

a) Remote Access to Software Resources

To provide remote software support to a client machine, the service provider must be able to access client resources directly, allowing the provider to examine and manipulate software settings, and investigate problems as if the technician was present at the client site. There are a number of software packages that can accomplish this, allowing the technician to use a workstation to access and display the client's current software architecture.

As mentioned in the examination of remote hardware support technology, applications such as NetSupport Manager(NetSupport Manager, 1) and NetOP(Caballero, 1) will allow a remote user access to client machines, instituting some form of server/client relationship that will allow a support provider to access the desktop of a target machine. Although PCAnywhere, a package also motioned in the discussion of remote hardware support, offers stable access to designated machines, the software is designed more for software deployment than for software support, making it less useful than the other packages in this particular topology(Symantec, 1).

NetOp operates by the matching of two software modules. A guest module allows for the remote control of a host machine, while a host module allows local resources to be remotely controlled by the guest. NetOp creates a simple means of connection to a client machine, and offers seven different levels of encryption to ensure secure access. NetOp supports a good range of operating systems including Windows, Linux, Solaris, and OS2(Caballero, 1).

NetSupport Manager offers a more advanced method of remote access, allowing a provider to watch, share, or control the client machine, enhancing communication on both sides of the exchange. Much like NetOp, NetSupport Manager offers encryption up to 256 bits, allowing for a secure exchange of data to take place, and supports an acceptable range of operating systems including Windows, Mac, and Linux(NetSupport Manager, 1).

Remote desktop technology is also integrated directly into Windows allowing for the remote control between Windows machines. Although using this method of access, referred to a Windows Terminal Services, would greatly restrict the overall range of operating systems supported in a given network, for small businesses who strictly run Windows platforms, the access method is free, saving the provider from incurring the cost of new software licenses(Windows, 1).

b) <u>Remote Software Diagnosis and Reporting</u>

Once access to a client's software resources has been established, the provider must be able to quickly examine the settings of a given computer so as to highlight potential reasons surrounding any given problem. Although some software technical issues can be handled by simply examining the application used by the client when the problem occurred, others require more in depth analysis.

Access to a client computer allows a provider to manipulate and examine the settings on a client machine, but investigating every possible setting takes a significant amount of time, affecting the efficiency of the service provider. Good information technology software that deals with software technical support incorporates reporting tools bundled within its licensing package, allowing a technician to quickly gain a snapshot view of the settings of a client's operating system.

NetOp(Caballero, 1) and NetSupport Manager(NetSupport Manager, 1) software packages have inventory tools imbedded within their remote access software, giving the provider a simple method of determining the contents, both hardware and software, of a client's machine. By use of these tools, a malfunctioning application can be compared against hardware and software requirements and checked for conflicts with other applications immediately, solving many software technical issues in a very short period of time. Although these packages only report the basic inventory of a target system, information gained through this means could convey a solid understanding of the machine the provider is about to diagnose, increasing the efficiency of their troubleshooting and diagnosis of any given problem.

Both packages incorporate the ability to script and schedule tasks on the client machine, giving the provider greater ability to test and troubleshoot problems. Critical devices can be tested regularly, comparing the performance of vital software against standard benchmarks and past performance. Using software scripting and scheduling tools allow a provider to employ proactive methods to software technical support, reducing the number of problems that occur without warning.

In addition to using a bundled remote access and support packages like those mentioned above, a provider can employ tools specifically designed to gather information and diagnosis systems. One of these applications, Ecora Reporter, a tool developed by Knowledgestorm, has the ability to generate hundreds of different reports regarding a given system, giving very detailed and specific information regarding a client system in both text and graphical format.

At the most basic level, Ecora Reporter can track the inventory, examine setting changes occurring within a specified allotment of time, customize reports to discover specific facts about the state of a system, and compare the state of two separate systems to determine discrepancies in their performance. Ecora Reporter can also be applied at the network level, generating reports on an entire system of machines instead of examining a single device.

The powerful reporting and diagnosis tools imbedded into Ecora Reporter could give a provider a significant amount of flexibility, being useable on any Windows, Linux or Solaris platform, and allowing for either the examination of an entire network of machines at a moments notice or the troubleshooting of a single isolated issue Although this application is far too powerful to be used in supporting the average workstation, it is ideal for critical devices(Ecora Reporter, 1).

c) Remote Software Support Methodology

A remote software support topology only requires a few applications to access and gather reports from a client system. The exact number of applications used will vary depending on whether the system supported is a low impact or critical device.

For non-critical systems, only a single application is required to handle both support functions. By using either NetOp or NetSupport Manager software, a provider could sufficiently access the client site and utilize tools to report on the system's hardware and software inventory.

For critical systems, a more detailed reporting technique is required. For these machines, a combination of software packages should be used, using NetOP or NetSupport Manager as the access method, and using the extensive reporting tools offered in Ecora Reporter to monitor the activity of the client system. By using Ecora Reporter, the provider can generate information on past performance and compare the efficiency of the supported device to other similar machines. This method will generate information that can be compared to each new performance report, giving the provider an early indication of system problems, and leading to a more proactive system of support.

2. Remote Software Support Business Factor Comparison

a) Cost Examination:

Remote software support can be managed through a very simple pricing structure, requiring only applications to handle the access, reporting, and diagnostic needs of the topology. By examining the level of sophistication required within these applications to support an average device, it is possible to determine the average cost of supporting a small businesses environment.

Every machine, whether of minimal or critical importance, requires access. As discussed earlier, use of either the NetOp or NetSupport Manager can grant a provider sufficient access to a client system, allowing a technician to manipulate, troubleshoot, and test software on a target machine.

For an average workstation or non-critical device, these software packages can also act a technician's primary reporting and diagnosis tools. The imbedded hardware and software inventory function in each application provides enough information for a provider to solve the easiest of problems quickly, while providing data to gain insight into more difficult issues, making it sufficient for supporting the average non-critical system.

Pricing between these two packages is similar. NetSupport Manager has a better cost when a lower number of licenses are purchased(NetSupport Manager, 1), while NetOp is better on the high end(NetOp, 1). Since the provider will be dealing with a number of different small business clients, for this investigation, the pricing structure of NetOp proves to be more cost efficient

For critical devices, the reporting and diagnosis tools native to NetOp and NetSupport Manager are not sufficient. Critical devices require proactive support with faster, more efficient service, and, to accomplish this, a more advanced application is required.

Ecora Reporter can handle the needs of critical devices, providing a an extensive range of tools for reporting and diagnosis of a target system. The price structure of the application varies depending upon the platform used, but Knowledgestorm offers flexibility in their pricing model, selling licensing in a pay per use, subscription, or perpetual format. This pricing structure allows a given provider to ease into its support of businesses, either reducing their short term costs to better aid their immediate cash flow, or reducing long term costs once their client base becomes stable and the risk of buying idle licenses diminishes(Ecora Reporter, 1).

Low Impact Service (Cost to cover 100 machines)

Software Access, Reporting , and Diagnosis	
NetOP	$3800
TOTAL COST	$3800

High Impact Service (Cost to cover 100 machines)

Software Access	
NetOP	$3800
Software Reporting , and Diagnosis	
Ecora Reporter*	
(Pay Per Use)	$7500
(Subscription)	$17,200
(Perpetual)	$28,700
TOTAL COST	$11,300, $21,000, $32,500

*Estimates obtained assuming a windows system. Prices vary slightly depending on platform.

b) Timeliness Examination:

A remote software support topology offers a fast, highly effective means of dealing with client software issues. Connecting to client machines is nearly immediate by use of remote access applications, and the use of reporting and diagnosis tools in this format can quickly provide very detailed information, making for a very efficient process(Apicella,1).

For strict support of software problems, a remote support topology seems to have no significant drawbacks. Any powered machine that is connected to the internet can be accessed easily, examined just as if the technician were on-site. Reports from the problem device can quickly be examined for configuration issues and conflicts, or can be compared to other machines of same type to uncover problems with the client system.

Since most software problems will occur when a machine is in use, access to low impact software resources is generally not necessary during off hours. As long as the software architecture is kept constant between most non-critical devices, software problems generally deal with configuration issues, and can be solved quickly as issues occur(Dash, 1).

For critical devices, a more proactive approach is required. For these devices however, gaining off hours access to the critical system is usually not problematic, as devices of this kind are usually left in a powered, active state at all times. As long as a provider is able to access the critical device, proactive reporting, testing, and troubleshooting can be completed with a high level of efficiency, and help to better maintain the working condition of its software infrastructure without the need for on-site personnel(Adams et. all, 4).

c) **Technical Capability Examination:**

Remote software support technology grants access to client systems from a remote location and generates information regarding the state of monitored devices. These reports can be used to rapidly acquaint a provider's employees to the hardware and software makeup of a client system, to compare a problem system to a previous, stable state where the error was not present, or to compare one system to another, determining the differences that exist in each machine(A New Model, 1).

By generating regular system reports, it is also possible to duplicate the architecture of a given system, building a model of the machine that the central location of the provider. Using this as a tool for software support gives a provider the ability to test and troubleshoot problems without the worry of damaging the working condition of a client system.

Reporting and diagnosis software also allows for proactive support of software problems. Although most software issues will need to be managed on a case by case basis, critical systems that are kept in a constant state will be easy to monitor, making it easy to recognize any potentially damaging configuration changes or problematic events before workflow is compromised(Eagle, 1).

3. Remote Software Support Conclusion

The software support needs of small business fit very well within the context of a remote support topology. Access to client systems can be easily obtained through the use of a variety of different products, and the reporting and diagnostic software used to troubleshoot systems can be scaled to meet the needs of the most common or most critical systems.

The cost of supporting systems through this method is very inexpensive. For non-critical devices, the purchase of the software required to access client machines is a one time cost.. For more critical devices that require a higher level of reporting and diagnostic software, flexible price structures are available in a pay per use, subscription, or perpetual format, giving a business the ability to apply their budget in a manner which best suits the size and cost constraints of their business.

The performance of a software support provider applying this method to a number of clients could be enhanced greatly by use of this topology, allowing a single employee to simultaneously gather information on a number of different clients and supported devices. Information gathered and recorded in this manner allows for the easy orientation of new employees to a client site, proactive support of client software systems, and creates excellent reference material for use in troubleshooting problems. In addition, by centralizing the knowledge base of the organization, a provider can designate any of their idle work force to any problem, making efficient use of their employee assets.

Remote software support technology also has the benefit of creating a learning environment for the client. Remote access applications can allow both the technician and the client employee to view the same screen, using imbedded tools for communication and demonstration to walk the client through a given problem, and explain why it occurred. This ability to educate the client on the use of supported software can benefit both parties greatly, reducing the number of overall service calls and giving the client better insight into the inner workings of the given product.

Remote software support technology is excellent when combined with the tools for remote hardware support, giving a provider full access to client systems, the ability to boot and reset physical devices, and the use of reporting and diagnostic tools which enable a technician to gather information on the entire system. When used as a single service for critical devices, the combined software and hardware support package can be an extremely powerful design, allowing a provider to monitor the full system performance of a supported device, while using its software and hardware performance history to recognize system problems immediately. Additionally, the ability to manipulate the power state of client machines empowers the provider with the ability to run tests during the client's downtime and troubleshoot problems due to system inventory or configuration changes, without subjecting the working condition of client devices to any risk.

A remote support topology is an ideal solution to the cost concerns and performance requirements of small business organizations. Use of this technology can make a provider much more efficient in its handling of clients, reducing the time and manpower required to solve each issue. In addition, by not requiring an on-site presence, a provider can nearly eliminate the costs of travel, handling client issues remotely from a centralized location and shifting the business to a more cost effective and cooperative organizational format. This increase in performance and reduction in overhead can pass on a lower cost to the customer, making the service more attractive to small business clients.

C. Web Hosting(Propensity to Outsource: 51%)

Small businesses showed the strongest interest in outsourcing their e-Business presence and web support to a provider rather than to hire the necessary personnel to develop and maintain their web presence in house(Brown and Young, 28). The cost of manpower associated with this business need requires a very specific skill base, and small businesses usually can not justify devoting time and money to something outside their primary business focus that can be so easily outsourced.

A web hosting service provider typically offers a client drive space to store files, an off site data center in which to house a web server, and is responsible for maintaining all equipment related to the client contract. Web hosting can be accomplished through shared hosting, where many different clients are allocated space on the same server, or dedicated hosting, where all client data is isolated on its own designated server. A web host service provider can offer server application support as well, fully managing the client's web solution(Underwood, 1-2).

The current methods being employed take advantage of small businesses inability to adequately manage their web hosting need in house by offering the physical space and expertise required to keep the small business web site up and running, but there are a number of issues with this basic design. Small businesses have a basic desire to keep their resources in house, and this solution places resources outside the bounds of their control(Eagle, 1). In a web hosting solution, the level of resources entrusted to an outside organization can vary greatly, from the most basic physical level of the hardware and software required to run a web site, to the manipulation of highly sensitive data required in a full e-business solution

This overall design is far from ideal for the provider as well. In assuming responsibility for client hardware, the web host service provider incurs significant costs regarding the physical space of the data warehouse, the safety measures required to protect the web hosting technology and secure client data, and the cost insurance to protect the business from liability in the case of a disaster. In an ideal situation, each of these costs are passed onto a pool of clients who absorb the financial burden, but this assumes an optimum level of businesses associated with the given provider. As the number of associated clients is reduced, the burden of these overhead costs reacts inversely, increasing the cost of service to each business. In this same respect, within the context of this topology, a service provider will be constantly faced with the problems of business expansion and reduction. As clients are gained and lost over the business life cycle, the organization will have to manage the times when business is tight and there are too few clients to cover their overhead cost effectively, as well as when business is profitable, and their space becomes inadequate. When dealing with small businesses, whose overall survival rate is much lower than their larger counterparts, providers are bound to see a significant amount of fluctuation in their clientele, making the problems of business expansion and reduction a major profitability issue(To Host… , 2).

In total, small business requires the skills and expertise of the provider, but would prefer to keep its resources in house. On the provider side, most of the profitability issues faced are as a result of the need to house and secure the resources of the client, and the need to manage the physical space and safety measures efficiently with the fluctuation of business activity. Through the use of remote technology, it may be possible to eliminate both of these problems.

If remote technology can efficiently allow an external service provider to manage a web hosting solution off site, both sides of the exchange can be satisfied by shifting the physical burden of server housing and security back to the client. Although the client will incur these costs directly, they will be at a level directly proportional to their desired web presence, and they will no longer be subject to price fluctuations suffered as a result of their provider's profitability. On the service side, this new topology would allow the more efficient service of small business web clients with significantly less financial risk, adding a much higher level of stability to their business and reducing the cost of overhead to manpower alone.

1. Remote Web Hosting Support Technology Investigation

A provider interested in managing web server technology located at a client site must be have reliable remote access to web resources, referring to both the hardware and software of the actual server and the interface of the actual web application. In addition, a provider will require tools for monitoring the activity of the hardware and software of the system and applications which designed to signal a technician in the case of a critical failure, so as to provide the timely response to server problems(Underwood, 4).

a) **Remote Access To Web Server Resources**

Managing a web server remotely requires access to both the hardware and software resources of the client machine. As the client's web based presence is dependant upon the combined package of devices and applications incorporated in the design of the web server, the provider must be able to manipulate and configure the device, regardless of the current working state of the machine(Web Hosting, 4).

The service provided by a client's web technology is critical, and the remote topology supporting it should use a high impact approach to ensure the stability of the resource. As the methods for providing hardware and software access to a critical device have already been examined in earlier investigations, the methodology of each will only be briefly examined.

For hardware access, the American Megatrends Mega RC G2 card can be used to provide 'Wake on LAN' functionality, allowing the provider to manipulate the powered state of the device at any time. The card also provides an secondary method of connecting to the client machine, stabilizing the provider's access to it through it's use redundant mediums(AMI, 1).

Either the NetOp (Caballero, 1) or NetSupport Manager (NetSupport Manager,1) application can be used to provide access to the web server's software. Each offers a simple client to host method for the manipulation of the server's infrastructure, allowing the provider to access other resident tools and applications as needed.

Each of these access methods are detailed under the remote software and hardware support investigations. More detailed information on these products can be found under these sections of the document, and should be referenced for greater understanding of the remote access methodology being used.

b) Remote Monitoring, Testing, and Diagnosis of Web Server Resources

Web server resource monitoring falls into three categories, supporting the client at the hardware, software, and web performance level. As a failure in any of these areas would result in an inoperable web server, each must be monitored for performance, consistency, and reliability, and tested under extreme conditions(Leong, 3).

For hardware monitoring, the web server is considered a high impact device. The methodology decided upon under the hardware resource monitoring section will be used to support this, using SiSoftware's Sandra application to generate regular reports and link alerts to the performance boundaries of the system. Combining this software with the Mega RC G2 card will give a redundant measure of protection to the server, giving the provider the ability to correct problems without access the system's OS, and creating a secondary point of access that can be used to correct problems on the client machine.

Since NetOp is already being employed as an access method to the software of the system, a provider can also take advantage of its software inventory function as the first method of software report. Combining this with the software monitoring capabilities of Ecora Reporter will generate a sufficient number of reports to allow a provider to proactively support the system, comparing the daily activity of the server to past performance, and using variations in the data to flag potential problems.

Web monitoring operates by executing tests against a target server, determining its maximum load bearing, and its performance under highly stressful conditions. Once these tests are complete, reports can be generated and saved so as to create a point of reference for future tests and to develop a system of benchmarking when examining similar machines. There are a number of web monitoring products available that can provide this functionality.

RadView provides three products, WebLoad, WebLoad Analyzer, and WebFT, to handle web server test and monitoring capabilities. The Web Load and WebLoad Analyzer work concurrently, flooding the web server with a number of real world simulated transactions, and recording the performance levels of the server as the load increases. This reporting function can also be used to monitor actual performance of the web server, using alerts to signal the provider in case of a problem.

WebFT is a complementary application, giving a technician the ability to generate custom test scripts and reports, automating testing of the functionality and design of a client's e-presence. As the design of every web server is different, this application can be extremely useful in being able to handle the web servers of multiple clients equally well(RadView, 1).

Empirix provides an entire suite of tools for web server support, offering applications for load and stress testing, real time reporting, and an integrated alerts to promote the stability of a client device. The Empirix test suite also allows for test and reporting customization, including a platform for test script creation within a portion of its software package(Empirix Test Suite, 1).

The company of Web Performance Inc. develops a similar package of tools, having two separate products that deal with the monitoring of web server technology. Their first product, Web Performance Trainer, handles server load testing by applying features of automated analysis, data replacement, authentication, session management, ramping load generation, network speed simulation, and load balancing of the test generation. Their second product, AlertSite, is a powerful monitoring application that determines the availability of network devices and tests, alerts, and reports information of website or application errors(Web Performance, 1).

Most of the above web monitoring tools are meant to be used from an external device, making them ideal for a remote support topology. Those that require a local application to provide alert and reporting information can be utilized through a remote software access solution on the web server, allowing for the use of a wide variety of tools in maintaining high performance levels.

c) <u>Remote Web Hosting Methodology</u>

A remote web hosting support topology must have both hardware and software access to the web server, allowing the device to be manipulated in any state, and to allow for regular monitoring and testing of the server. For hardware access, the

Mega RC G2 is ideal for this purpose, providing remote power cycling and a secondary means of contacting the server. For software access, as with previous remote support investigations, NetOp's remote access application can be used to allow a provider to access and manipulate software resources on a target server.

For the monitoring, testing, and diagnosis of software and hardware resources, a number of different applications and devices can be used. SiSoftware's Sandra (Who/What is Sandra, 1), coupled with the troubleshooting functionality imbedded in the Mega RC G2 card, can provide the necessary tools to maintain and monitor server hardware. On the software side, NetOP's ability to inventory a system can be combined with the reporting capability of Ecora Reporter to generate data on a given system, and monitor physical changes to the system or fluctuations in performance as they occur.

Support of the web server technology can be handled through regular testing and monitoring of the system. All three of the products examined through the companies of Radview, Empirix, and Web Performance Inc. offer products that seem ideally suited as a base for a remote topology, each having strong abilities to stress server capabilities and generate data to help determine the current state of the server against its optimal working condition. As there are a number of options to choose from to handle this aspect of support, the exact product or products used will be determined by the best combined package of cost, capability, and usability that match the needs of the client organization.

2. Remote Web Hosting Business Factor Comparison

a) Cost Examination:

The base requirements of the methodology implement a critical monitoring and troubleshooting solution to handle the hardware and software components of the web server. As discussed in the earlier examinations of remote hardware and software support, these costs are relatively low, providing a very economical solution for the remote service provider.

In supporting the actual application that drives the web server process, there is a significant differentiation in cost between the available products. Each of the three major software packages through Radview, Emperix, and Web Performance inc offer similar tools, but structure their licensing in a unique fashion.

Radview customizes their pricing structure on a case by case basis, offering different base costs dependant upon the number of simultaneous users and the level of extended or limited use required by the client. As this pricing strategy can become rather complicated on the broad level, the examination of Radview's cost structure will be constrained to only consider the needs of a remote web support service provider.

WebLoad Analyzer is the heart of the remote web monitoring solution, and assumes the most up front cost. The product is sold in a format designated by node, monitoring client web server activity through a set console, and issuing alerts as performance of a given server drops below specified benchmarks. Incorporating this design through Radview to handle a bank of one hundred web servers would cost approximately one hundred thousand dollars, with an additional twenty-five thousand dollars for each console node.

WebLoad is offered in a perpetual format, granting the provider the ability to conduct simultaneous web load and stress testing on one server for each license purchased. Using this software, the provider would need to estimate the number of tests that their clients would require in a given week, and purchase licensing accordingly. Using an assumption of use equating to five server tests per week, the cost of WebLoad averaged to about thirty thousand dollars.

As WebFT is only a scripting tool used to generate custom test methods and reports, it does not have the complicated pricing structure. WebFT is purchased on a per seat basis, locked to a specific machine, and costs two thousand dollars per license(RadView, 1).

Web Performance Inc offers two separate purchase plans for their Web Performance Trainer tool. The first package offers a performance based pricing model, offering a cost which is dependant upon the estimated user load the provider wishes to simulate. Available load simulation ranges from twenty-five to five thousand users, and costs increase with capability. For those businesses interested in an unlimited licensing format, Web Performance Inc offers a separate purchasing plan, scaling the capability costs to make its purchase more economical on the high end.

Included in the purchase of either package is a basic support plan, offering a low priority level of support with contact available by email. Cost for dedicated user licensing support range between seven hundred fifty and twelve thousand dollars, while unlimited licensing support costs about fifteen thousand dollars. Once purchased, support exists for the life of the product.

In addition to these costs, there is an upgrade charge associated with the product. Based on the client's licensing plan, this cost will be applied to the business anytime a major or minor version number changes in the software, requiring an upgrade in the current application code. This cost can be avoided by the purchasing of the premium service plan which provides these upgrades for free. As both the premium service plan and a single upgrade cost are exactly the same, this price structure is obviously designed to promote the premium service package and provide annual income to the business from its current clients. The upgrade costs and cost for premium support differ based on the number of licenses, ranging between two hundred and three thousand dollars for dedicated user licensing, and about four thousand dollars for unlimited licensing structure.

The purchase of Web Performance's Alert Site software is divided into four levels, offering more product functionality with each increased level of cost. These costs range between fifteen dollars and one hundred dollars, and are based on a per month and per device format(Web Performance, 1).

The cost of the Empirix test suite cannot be broken down as easily as the other two web performance products. The web performance tools and applications that are packaged together to support a web hosting environment are each tied together as a custom solution to the needs of their clients, and their actual product cost model is kept completely confidential, making price estimation very difficult. Still, some information can be gleaned on how well the pricing of the Empirix test suite matches up to the products of their competitors.

In a Gartner Group study of the Empirix test suite, some information surrounding Empirix pricing model is revealed. The study indicates that the "Price is an important differentiating feature for Empirix. Its testing and application performance management tools are aggressively priced to encourage enterprises to buy, try and buy more. The flexibility of the Empirix licensing structure is based on its modern, modular product architecture, which enables customers to buy what they need to meet initial requirements and then add incremental capacity as new requirements emerge. The monitoring tools are priced by the number of elements to be monitored and tests to be performed (which) enables enterprises to adopt the tool with minimal risk in isolated application environments and to pilot the product before a major investment." Gartner's strong endorsement of Empirix's web application performance package indicates that Empirix utilizes a flexible cost model, with prices scaled to the both the level and manner of its use, seemingly matching the needs of a remote small business provider(Empirix Web Application, 1).

In a more concrete representation of the product cost of Empirix's web application performance package, the sales department was able to generate a broad estimate for a small business web hosting provider. For a small business provider to apply the capabilities of Empirix's monitoring, alert, and testing applications in support of one hundred separate web servers, the sales associate generated an average total cost of about fifty thousand dollars(Quircach).

Remote Web Hosting Service Cost (Cost to cover 100 machines)

Hardware Access/Monitoring/Diagnosis	
Mega RC G2	$59,985
Sandra	$19,999
Software Access /Monitoring/Support	
NetOP	$3800
Ecora Reporter (Perpetual License)	$28,700
Hardware/Software SUBTOTAL	$112,484
Website Monitoring and Testing	
Radview:	
WebLoad (100 machines, 1 node)	$125,000
Analyzer (100 machines)	$30,000
WebFT (5 licenses)	$10,000
Radview SUBTOTAL	$165,000
Web Performance Inc:	
Premium Service Plan (1000 users)	$1995/year
Trainer (1000 users)	$7995
Alertsite (e-Business plan)	$0*
Web Performance Inc. SUBTOTAL	$7995 + $1995/year
Empirix Test Suite	$50,000**
TOTAL COST (Radview Solution)	$277,484
TOTAL COST (Web Performance Solution)	$120,479 + $1995/year
TOTAL COST (Empirix Solution)	$162,484

*Cost of this level of alertsite is included in the base solution

**Broad estimate and not be considered a locked price for the solution

b) Timeliness Examination:

In a traditional format, the client's web server is located off site, and the provider maintains the hardware and software related to the service at their own facility. Although providing support remotely and keeping all of the necessary resources at the client site allows a small business to maintain tight control over their web server, it separates the provider from the supported device, inherently reducing the overall efficiency of the solution(To Host… , 1).

The tradeoff in efficiency however is managed by the provider's ability to test and monitor a great number of systems from a single location. By using alerts and benchmarking to flag supported machines that exhibit problematic symptoms, the response time for support can be kept extremely low. Combining these techniques with the ability to manipulate the complete hardware and software of a client system can give a provider fast, powerful access to a supported web server, nearly matching the efficiency of a localized web hosting topology(Apicella, 1).

By incorporating the design of the high impact hardware and software device remote support strategies discussed in the earlier sections, the provider is able to create a dependable connection to supported machines. Constant monitoring of supported devices can occur during and after normal work hours without infringing upon the normal workflow of the business, and alert mechanisms and scheduled testing can keep the provider constantly informed of the machine's current level of performance. Although none of the provider's employees will be on-site to physically manage the web server, the tools present in the software, hardware, and web maintenance can devote an entire team to any given problem at a moments notice.

c) **Technical Capability Examination:**

A provider using a remote service topology to support client web servers has access to many of the same tools as those who provide support in an on-site format. Very few restrictions exist to hinder the accessing of client resources in this manner, creating a very flexible and powerful design to satisfy customer demands.

As mentioned in previous investigations, remote hardware and software of web server technology contains the same benefits and face the same restrictions found in the remote support of any critical device. Although remote technology is very powerful in its ability to access, monitor, and test the performance levels of a given machine, using a remote methodology, there is no way to actually manipulate the physical components of the server in a cost effective manner. Remote support can still be used to manage critical devices, but this inherent flaw in the design makes remote service support an inferior solution when compared against an onsite methodology.

In contrast to this, web server application software seems ideally suited for a remote support solution. As the web server is designed to exist as a near permanent facet on an external network, access, testing, and troubleshooting of the device can occur with minimal changes to the client machine. Using technology that is currently available, a provider can embed alerts into a client system, and use them to monitor and test the capabilities of the server. Information generated from these activities can provide benchmark data pertaining to performance levels, and can be used to recognize design issues resulting from such things as insufficient bandwidth and faulty hardware, allowing for the preemptive correction of possible future problems.

3. Remote Web Hosting Conclusion

Use of a remote topology to provide web server support provides a small business client with the security of keeping tight control over their own resources, while allowing a provider to avoid the risks and costs associated with maintaining local control over client machines. Although this methodology seemingly shifts a higher burden of costs back to the client, forcing them to purchase and maintain their own hardware, the shift in resources actually reduces the overall cost of the client/provider relationship.

By keeping the physical resources at the client site, this topology significantly reduces overhead, shifting the service costs of housing and insuring of the device on the provider side with the client purchase of a physical asset. Since this exchange of costs removes a significant amount of redundant overhead requirements from the provider's cost of doing business, the provider is able offer a significantly lower cost to its clients(Underwood, 4).

Supporting web server technology is no different than supporting any other critical device. Use of remote access to software and hardware allows remote monitoring, testing, and management of the machine, allowing the provider to a keep close watch on the working condition of supported devices. As web server technology regularly operates over some form of network medium, the tools used to manage the web application can be tested and maintained efficiently though an internet connection. Examination of tools through companies such as Radview, Empirix, and Web Performance Inc. have powerful functionality, mirroring nearly all of the capabilities that would be available to an on-site professional.

The greatest drawbacks to a remote service provider arise by the intrinsic inability to physically access the client's device. As discussed under the investigation of remote hardware support, without the sue of on-site personnel, the replacement of hardware relating to the supported device can be both costly and inefficient.

A client will also suffer from some response issues due to the provider's reliance on the internet medium to gain access to the server site, but this deficiency is seemingly overcome by benefits of the solution. With the cost savings that can be passed onto the small business, the provider's ability to combine powerful technology and the whole of their employee base against problems that arise, and the unobtrusive nature of the overall method, the delay caused by internet support should be considered only a minor detriment to the use of the topology.

At first glance, remote web server support would only be truly useful to a select group of small businesses that are both willing and able to acquire their own web server, but the cost savings achieved by removing the overhead of environmental controls, security, and housing of servers has the possibility of making the topology attractive at any level(Underwood, 1-4). Remote web solutions provide constant monitoring and strong technical capabilities, with very little associated drawbacks. This reduction in cost coupled with the local control of resources seems to be an ideal fit for the needs of the small businesses, and should allow for providers to profitably offer more cost effective and efficient service.

D. Server/Host Management (Propensity to Outsource: 36%)

Although software technical support is used to troubleshoot problems and offer assistance to clients on using specific tools and applications, there are more complicated issues surrounding the software side of a business's information technology architecture that need to be managed. As small businesses cannot usually afford the cost of hiring these individuals directly, the management of these resources is usually outsourced, using an external service provider to support company servers(Brown and Krammer, 28).

As in the web hosting support model, server hosting can be accomplished in a shared or dedicated model, giving the client the ability to customize their level of desired support as well as the level of interaction the external provider will have with their data. An outside service provider assigned to fill the server/host management support role for a small business acts in a consultant capacity, building an overall framework of software applications that will allow each employee to efficiently complete their work. In general, a provider acting in this capacity is responsible for maintaining the access and integrity of company data by providing hardware support and monitoring for server equipment, while implementing corruption and fault solutions to protect against data loss(Underwood,1).

The most important role that the service provider fills, deals with the upkeep of this architecture, keeping the company's software up to date with patches and fixes, and rolling out any necessary upgrades to the organization's software as needed. With the outside organization keeping current on the changes to the company's software, the business can focus on its main profit generating activity, allowing the provider to maintain their software resources in the background(Brown and Young, 30).

The problem with this system of support is in finding an ideal time and situation for upkeep. Ideally, the installation of new software, patches, and fixes should occur at the point when the company is utilizing the least amount of resources. Generally, this time occurs off hours late at night or on the weekends, when the provider can take the time to install and test the new system, leaving sufficient time to correct any issues which may arise from the instituted changes. Since the technicians completing the install will be from outside the business, this creates some logistic issues for the organization.

Unless the small business is willing to allow technicians from their service provider free range of their facilities during the company's off hours, they will have to assign some of their own personnel to the project, even if only to give the outside organization access to the physical site. Computing resources will have to be made available for test any time the provider rolls out applications, causing the business either to pull systems from their regular assigned tasks, or not test them at all.

On the provider side, sending technicians out to client sites to perform software roll outs every time an update is needed can prove extremely costly and can tie up personnel from more important tasks, making the process very inefficient. This issue is most significant in those cases where problems prove insurmountable in the time allotted, and a trip to a client site generates no results.

In those cases, all company expenditures surrounding the trip to the client site are most likely wasted, and must be scheduled again so as to fulfill the provider's responsibility to the client(Brown and Krammer, 11).

It may be possible to avoid these issues by the use of remote technology. If an outside organization could be given restricted access to small business information technology resources, it could be possible to push new patches and software installations electronically, removing the need for any on-site presence. Solutions could be tested from within the provider's organization, using a model of what systems are installed on each of the client's machine, and utilizing all of their available personnel and resources to troubleshoot problems. If problems are not able to be handled in the time allotted, the provider would be able to roll back the client's software architecture to its previous state without any real tangible loss of resources. Ideally, by use of this topology, the provider could shift their small business support completely into the background, accomplishing their purpose with the absolute minimum impact on client operations.

1. Remote Server/Host Management Support Technology Investigation

Remote server and host management depends upon technology that can compress data for transfer over the internet, encrypt data to ensure the security of transfers, and handle the multicast deployment of software to client machines. Using this technology and these techniques, a provider can manage a client's information infrastructure by remotely deploying applications and patches to client machines and backing up their business critical information by regularly transferring information from the client to the provider's site(Greenhill, 1-7).

a) **Remote Software Deployment**

To deploy software applications or patches to a client site remotely, a provider must have control over the software and hardware infrastructure of the machines that are to be upgraded. Since the machines are not in close proximity to the provider, changes to the software and hardware inventory of client machines can occur at any time and without warning, leaving client resources in a state that could cause installations to fail. Using the hardware and software remote management applications discussed in the earlier sections of this document, a provider can verify the proper state of each machine that is to be upgraded, identifying any problematic changes to hardware or software before actually going ahead with the deployment. The static nature of the client machines should be grounded in policy, the client reporting any changes to its machines to the provider so as to keep them up to date, but using remote management applications can act as a final verification, avoiding any unexpected results from the upgrade(Greenhill, 1).

Once the ready state of machines within the client network is verified, there are a number of application packages which can accomplish the compression, transfer, and installation of software to a client site. Since the most efficient software deployment solutions are designed to multicast installations across a network, they can be easily ported to a remote solution.

CenterRun's 'One Touch' software delivery system offers many automated functions that would allow a provider to roll out software efficiently to a client site. The 'One Touch' software package pre-builds an application on a deployment server, breaking down the target application into its basic component files, and builds a reliance tree to store a local dependency model of the application. Once this is complete, the deployment server can automatically make use of software requirements, version numbers, dependencies, and pre-installation and post-installation procedures every time they wish to install, update, or remove the application from a client site.

Using this functionality as a base, the 'One Touch' system incorporates the ability to automate minor and major deployments, building them off site on the deployment server to verify the correct configuration, and rolling them out for full application installations, security patches, software updates, configuration changes, or bug fixes. Use of the configuration error checking on the deployment server can greatly reduce the risk of damaging the integrity of the client's system, and the ability to automate software roll outs can greatly reduce the time required, making the entire process extremely fast and dependable(CenterRun, 1).

New Boundary Technology offers a similar application in their 'Prism Deploy' software package. Prism Deploy is a software deployment application which is designed to port application packages over the internet based on a group membership scheme. Groups are defined by function, bucketed together by their use in the organization. Once these groups are defined, software deployment can be accomplished rapidly, the Prism Deploy system spawning out bundles of software which each group will need to accomplish their role in the organization. Patches and updates can be rolled out automatically with this system, porting out the fixes to the required machines based on their grouping, requiring very little human interaction. In a similar way, new machines brought into groups will automatically be updated with the required software upon their integration with the network, allowing for the business network to be instantly standardized as machines are added or removed through changes in the business architecture. Making this system even more powerful is its ability to utilize Microsoft's Active Directory as its group membership scheme, giving the user a powerful means of instantly absorbing a business network into the deployment architecture of the Prism Deploy application package(New Boundary, 1).

The company of ManageSoft offers another option for remote deployment. The ManageSoft software package contains a great deal of the functionality found in 'One Touch' and 'Prism Deploy', providing the ability to remotely transfer applications, fixes, and updates to a number of devices. In addition to this however, the ManageSoft package turns an organization's local servers into error checking devices, giving an organization the ability to automate deployment troubleshooting within the confines of their own network, instead of at the deployment source. ManageSoft also offers added functionality in its license management and IT asset tracking software, allowing a business to constantly monitor its hardware and software resources and keep track of its licensing renewal schedule(Managesoft, 1).

b) Remote System Backup

Unlike other remote solutions, a remote backup service does not require control over a client's hardware and software resources, although use of this kind of technology can be useful in increasing the organization's reliability. The most prominent technology costs for the solution are found in the maintaining, securing, and updating of the data itself, requiring a great deal of storage memory, failsafe equipment, and intensive processing to be accomplished effectively(Cartright, 1-2).

A remote backup solution requires the regular compression, encryption, transfer, and storage of sensitive data, coupled with a reliable means of restoring information in a timely manner. There are a number of different software packages that offer these capabilities, each having the possibility of fulfilling a client's needs when combined with stable data storage technology. A few examples of this can be found in the software packages developed by Arkeia, Remote Backup Software, NovaStor, and ZipToNet.

Arkeia's product, Arkeia 5, uses client side encryption coupled with multi flow and multiplexing functionality to maximize speed and allow for simultaneous backup and restoration. Arkeia incorporates error checking methods that monitor network and system faults, ensuring the reliability of transferred data by restarting the process whenever data corruption is detected. Arkeia is also modular, allowing for it to cover the needs of nearly any size of organization. Arkeia handles the security of data through three levels of data verification for access and data transit protection methods that can employ either DES or Blowfish encryption. Each Arkeia license includes software for one master server, one backup server, and up to 200 workstations, allowing for a great deal of flexibility in managing the gain and loss of machines in a client network environment(Enterprise, 1).

The RBackup application, offered by the Remote Backup Software corporation offers a similar package of remote backup and restore tools as Arkeia, employing methods of compression, encryption, and scheduling to ensure the stability of critical data. Each RBackup server can operate several modems simultaneously, and handle thousands of Internet connections at the same time through Cable Modem, DSL, or any Internet connection. RBackup also offers more prepackaged functionality than Arkeia, having a number of imbedded tools that allow for a user to manipulate, transfer, or generate reports upon the secured data. RBackup contains an impressive array of encryption methods, supporting DES 56 bits, TDES (Triple DES) 168 bits, Rijndael AES (new US Federal Standard) 128 bits, Rijndael AES 192 bits, Rijndael AES 256 bits (most secure), and Blowfish variable key length to 448 bits(Remote Backup Solutions, 1).

NovaStor exhibits a similar format as the above two remote backup solutions, but employs methods that give the solution a more efficient architecture. Instead of backing up the a company's data in its entirety, NovaStor uses Fastbit technology to recognize changes to blocks of data, and extract the exact segments where the modifications occurred. The ability to trace incremental changes at the binary level allows for a significant reduction in overhead for data transfer, leading to a very fast and efficient system for transferring data. In addition, NovaStor's offers a complementary product to the NovaNet Web application, called Open File Manager. This application removes the need to lock out users during backups by allowing the server to monitor the use of data, and back it up incrementally as portions of the data become available. As this functionality would allow a provider to backup data at any time, regardless if the data was currently in use, the Open File Manager would be an extremely powerful tool when used in a remote setting. As seen in previous remote backup packages, NovaStor can utilize DES, Triple DES, or blowfish encryption, displaying functionality that is competitive with other solutions(NovaStor, 1).

ZipToNet is a client driven application that uses an automated FTP framework to provide a remote backup solution. As long as an FTP site exits on the server targeted for storage and the client has the correct permissions to access its resources, no changes need to be made on the server side to handle the solution. Client side software enables both incremental and full backup solutions to duplicate critical data on the remote server, transferring information under the protection of 256-bit blowfish encryption(ZiptoNetX, 1).

c) Remote Server/Host Management Methodology

Managing server and host resources remotely requires very few components and is a fairly straight forward process. As a provider offering this kind of service only needs access to the client network and devices, and does not require the remote control of client resources, there is very little need for the use of multiple applications within the framework of the solution. The compression, encryption, and transfer of data can all be accomplished through software packages designed for either application deployment or data backup, fulfilling nearly all of the requirements of the remote topology through two pre-packaged software solutions. As choices made between these applications will vary based on the budget, business needs, and preference of the provider and their clients, a better assessment of their individual value can be made after examining the business factors surrounding each separate solution.

Beyond the specific technological needs for backup and deployment, a remote server/host management topology requires the provider to have some ability to configure client devices into their proper state before transmitting information, to test configurations after software has been installed, and to roll back the entire process if the deployment or restoration of data fails.

Although some of these techniques can be managed through the use of the base remote deployment and backup applications mentioned earlier in this section, the use of a remote software support application would make for a more complete solution and should be included in the base methodology.

2. Remote Server/Host Management Business Factor Comparison

a) Cost Examination

(1) Remote Deployment Costs

On the deployment side, Prism Deploy's software solution is the most economical for a small business solution. Prism deploy offers a small to mid business perpetual licensing package giving an organization the ability to cover just under five hundred devices at the cost of thirty-five dollars per machine. With initial licensing, the company includes a year of support, and charges only seven dollars a machine for service thereafter(Butorac).

Although the Managesoft solution fits the technical needs of the remote server/host management topology, its pricing scheme is restrictive to small business solutions. Managesoft's has no specific small to mid business licensing schemes, offering a minimum licensing package of eight hundred devices at the cost of one hundred dollars per device. The cost of support is set at twenty percent of total licensing cost, equating to a minimum cost of sixteen thousand dollars per year. Although not ideal, these costs are not completely prohibitive for use in a remote topology. For a remote service provider, these costs could be grown into, diversifying the number of licenses across a number of small business and thus taking advantage of technology that the small business client would not be able to acquire on their own. However, as it is unlikely that a provider would have the deep level of clientele required to utilize eight hundred licenses in the earliest stages of their business, a provider would have to port all of the devices of their clients over to Managesoft solution after their business profitability rises enough to make the solution viable. As eight hundred devices in a small business support format could mean any number of clients, spanning a nearly unlimited range of distance from the provider, the chances that a provider would decide to switch solutions, especially to one with such a high cost, is very unlikely(Managesoft, 1).

As of this point, CenterRun is no longer an option for remote small business deployment. The organization has been recently acquired by Sun Microsystems, and their deployment product has been incorporated into Sun's N1 provisioning server. Since this product is no longer applicable for the support of small business deployment, no cost schemes for its purchase will be examined within this investigation(Sun Microsystems, 1).

Remote Deployment Solution Costs (Cost to manage 100 workstations):

Deployment Solution:	
Centerun	N/A
Prism Deploy	$3500
Managesoft	$80,000 (800 device minimum coverage)
Support:	
Centerun	N/A
Prism Deploy	$700/year
Managesoft	$16,000/year

(2) **Remote Backup Costs**

Arkeia's backup solution is packaged in a way allows the purchase a single perpetual license for each client network, offering software for one master server, one backup server, and up to two hundred workstations. Each license costs six hundred ninety dollars, with an annual charge of four hundred dollars for software support, making the solution extremely affordable and scaleable to the needs of most small businesses(Enterprise, 1).

Remote Backup Systems have incorporated a perpetual business license within their pricing scheme. As the initial cost, for a provider to manage one hundred clients remotely and purchase support for the first year, the cost is three thousand four hundred forty-seven dollars. Network licensing can be upgraded to manage upward shifts in the number of devices present in the client network, and maintenance agreements can be renewed for three hundred ninety-nine dollars each year(Remote Backup Solutions, 1).

The NovaStor solution is offered through the purchase of two separate software packages. NovaNet Web software if offered at a cost of approximately nine thousand two hundred sixty dollars per one hundred users, and the Open File Manager software is available for an approximate price of one thousand nineteen dollars per twenty-five workstations. A basic technical support package is included in the price of each license, but extended support is available, priced uniquely for each business situation(NovaStor, 1).

ZipToNet offers an unscaled multi-user licensing option, priced at forty-nine dollars per user. This license includes email technical support, and is designed to back up to a single server. The license architecture can easily be divided to incorporate the structural requirements of a provider managing multiple client networks, and higher levels of support can be purchased for those networks which require more direct assistance(ZiptoNextX, 1).

Remote Backup Solution Costs (Cost to manage 100 workstations):

Backup Solution:	
Arkeia	$690 (license supports 200 clients)
Remote Backup	$3447
NovaStor	$9,260
ZipToNet	$4076
Support:	
Arkeia	$400/year
Remote Backup	$399/year (1st year included)
NovaStor	Basic Service Included
ZipToNet	Basic Service Included

b) Timeliness Examination

A remote server/host management topology utilizes the same principles as one developed for on-site support. As most deployment and backup solutions are already designed to be automated over networked connections, utilizing an off-site system for these purposes simply makes more use of the existing capabilities of remote backup and deployment software.

Overall, the biggest disadvantage to the timeliness of a remote solution is in the propensity for data to become corrupted and require data packets to be retransmitted over the increased distance of the network connection. The risk of data loss associated with such common problems as network collisions, heavy network traffic, or faulty network segments, increases greatly as the methodology expands beyond the bounds of the client's internal network, and the topology continues to lose a level of efficiency with each additional measure of the Internet that is relied upon(Greenhill, 1).

Although this loss in efficiency can never be eliminated completely, remote deployment and backup solutions incorporate measures that can limit the risk of this problem. Most application packages of this nature employ compression schemes that reduce the overall data transfer to the bare minimum, To compliment this, each solution is often coupled with error correction software that verify packets between both transfer points, ensuring both the validity of each packet of data, as well as preserving the completed portion of the exchange, protecting against a complete loss of connection(Cartright,1).

By using software packages that employ error checking and data correction schemes, the risks and efficiency problems associated with the topology can be limited to an acceptable level of risk for business use. Although the solution will always be less efficient than one employed in a client's internal network, remote server/management can still be considered as a quick efficient means of transferring data, making it acceptable for the deployment and data backup needs of small business.

c) **Technical Capability**

As mentioned earlier in this investigation, the remote deployment of applications and software is only an expansion of the current methods used in an on-site design. Many software packages exist to enable multicast installations, allowing a company to upgrade entire networks of devices in a single session. Although this solution is usually applied within the confines of an internal network, expanding the boundaries of the client server topology does not hinder the usefulness of the overall design.

For deployment, there are four major aspects which need to be managed in a remote topology. Delivered data must be compressed for fast transfer of applications to client devices, examined for its validity, and corrected in the case of a corrupted transfer. Lastly, once software is deployed, the topology must allow for the configuration to be tested, assuring that both the client machines and installed applications are left in a stable state. Although most software deployment packages handle compression and error checking inherently as part of the software package, testing the overall solution is a more complicated endeavor(Greenhill, 1-7).

On a large scale, it is unlikely that a provider would wish to install remote software management applications on every machine across a client's network However, when dealing with small business clients, this solution can be used as a possible means of configuring and testing applications after deployment. Since the biggest drawback to remote deployment is in the ability of the provider to directly manipulate client resources after the initial data transfer occurs, this low cost solution gives access to powerful "hands on" functionality.

Backup solutions require a similar level of functionality, requiring high levels of compression and error checking for fast, efficient transfers of data. In addition to this however, remote backup solutions must be encrypted to protect a client's data from theft as it is transported over the public network. However, as data is only being stored offsite in its raw form, and since data integrity is monitored while being transferred, there is no need to test the state of the data once it arrives, making the addition of a remote software management application to the solution unnecessary(Planning, 1).

Each of these needs are handled adequately by the current remote backup application packages currently on the market. With high level compression and encryption methods embedded directly into each software solution, remote management of a client's backup and restore needs can be extremely stable. Once these aspects of the data transfer are acceptable to the client, the functionality of the solution mirrors that of on-site methods, showing no reduction in the provider's ability to manage the backup and restoration of client data.

3. Remote Server/Host Management Conclusion

Remote software deployment and data backup solutions require technology that can lower the security risks and overhead that are associated with extending a client's data beyond the scope of their internal network. Prepackaged software solutions currently exist on the market that contain tools of encryption, compression, and error checking, reducing these risks and shrinking the virtual gap between the client and the provider. Using these tools in combination with a remote software management tools can give a provider "hands on" functionality, enabling them to transfer, secure, and correct the deployment and backup of data in a very efficient manner.

The overhead for this solution however is rather significant. To handle remote server/host management in this manner, software management applications must be installed on every device that is to be involved in an exchange of data. Without such software in place, a provider could not ensure that the machine was in the correct state to accept data, could not test any deployed solutions after a transmission occurs, and would not have the access required to roll back solutions when necessary. Although the cost of these solutions is still far less than what would be required to hire a separate staff to manage each small business site, it involves the installation of software on a great number of software devices, and the continued management of every client site for the addition, loss, or change to client machines. Depending on the level of fluctuation present in the client's topology, this constant maintenance could force the provider to manage each change on-site, greatly hindering the efficiency of the overall solution.

On the deployment side, remote software/host management is constrained by the time frame in which rollouts can occur. Inherently, remote deployment will take more time to transfer data based on the distance between the client and the provider, has an increased susceptibility to error as it passes over a greater distance of the network, and requires more time to manage than an on-site solution. These factors place significant restrictions on a provider's ability to find time for the configuration of the client network, the initial transfer of data, and schedule contingency time in case there is a need for a rollback.

For remote backup and restoration, the total cost of the solution is very deceiving. Although the implementation of remote tools requires very little capital, the actual maintenance of information is a much more costly issue. Running data servers requires space, power, environmental controls, and must be redundant to protect the needs of the client. As each of these needs completely nullify many of the low overhead advantages present in remote solutions, it greatly harms its attractiveness. For small clients, it may be possible to apply this solution in the same way as was discussed in the remote management of web hosting, keeping the client data on-site and only managing the transfer of data across the client's internal network. However, this technique keeps the client's data all in one place, increasing the risk of data loss and lowering the effectiveness of the provider's service.

Beyond these drawbacks however, the remote management of small business servers and clients is a very viable solution. Although the methodology does not completely replace all the functionality which can exist through an on-site or traditional data warehouse solution, the savings in cost passed on from a provider's reduced manpower and other overhead requirements should make it extremely attractive to any organization with a constrained budget.

With the availability of prepackaged solutions to handle the core needs of the deployment, backup, and restoration of data, the transition from on-site to remote solutions can happen rather easily. This, combined with the restrictive budgetary business trends that are currently being employed by most organizations, suggests that there is a desire for new techniques of this kind in the current marketplace, and suggests that remote deployment and backups solutions should become more of a mainstream solution in the near future.

E. Remote Support for Network Operations (Propensity to Outsource: 25%)

The need for the consistent performance and reliability of network resources has led a large percentage of small businesses to outsource their networking needs. In the small business context, network operations support is designed to cover a multitude of issues related to the interconnectivity of the client's information technology infrastructure and is primarily focused upon keeping all of the client's technology components communicating with one another at an optimum level of performance(Brown and Young, 28).

A client network in this context can be defined as a connection of local area networks and wide area networks that must be able to communicate with one another, client workstations, and any existing network servers(Goodness et. all, 1). At the most basic level of support, these resources are passively monitored using tools and techniques that, generally, do not increase network traffic. For more complicated network architectures and for higher levels of support, active monitoring is used, generating test packets and isolating problem areas to more effectively observe the activity of the network. Although this method generates significantly more network traffic than passive techniques, it allows for a more proactive approach in supporting network operations. Active monitoring can include techniques such as time physical and logical monitoring, maintenance and configuration of networking hardware, performance management, fault protection and correction, and the optimization of data flow, allowing the provider to take a full service approach to their networking support strategy(Carr, 3).

The main problem for small business network operations support is that it requires a great deal of dedicated time to properly monitor the network. At the lowest level of support, a small business can rely completely on passive monitoring to ensure their network is up and running, but this method still requires a technician monitor the flow of network traffic. For active monitoring, the time and resources devoted are much greater, requiring additional space, equipment, and manpower to run tests across the network architecture. As the level of dedication on the part of the provider and as the required resources increase, so does the cost, putting a financial strain on both sides of the business equation(Cottrell, 1).

Network operations support could seemingly benefit by the use of remote technology, allowing the provider to limit the level of resources dedicated to the client site. If a network could be monitored remotely in this manner, the provider would benefit from being able to keep employees centrally located, using their entire skill base to correct problems as they arise. In addition to multitasking the efforts of personnel, with the ability to apply network testing applications to client networks in a remote format, it could be possible to multitask the provider's resources as well, using the same information technology components to manage the networks of multiple clients. By shifting the burden of manpower and monitoring equipment to the site of the provider, costs could be significantly lowered and client constraints surrounding resources and space requirements could be eliminated, greatly increasing the overall efficiency of the solution.

1. Remote Network Support Technology Investigation

A remote network support topology relies upon the ability of applications to monitor, test, troubleshoot, and administrate the servers, clients, and connections that makeup a client's network backbone(Goodness et. all, 7). These needs require an administrator to have remote access to critical machines and networking devices, allowing for the observation and manipulation of the state of the network at any time.

Many of the facets of remote network support have already been discussed in earlier investigations of remote support technology. As a client network will consist of all interconnected devices within the information technology architecture of a given small business, the support technology that currently exists for software, hardware, host, and server management is all directly applicable to a networking solution. Considering that each of these areas have already been examined for their feasibility in a remote topology, the investigation of remote network support will be strictly focused the management of the client medium and of networking devices.

Out of all the possible disciplines of information technology, network support is the area where remote management is most prominent. Networking devices are designed to function on a shared medium and deal with the flow of data across a defined segment of a network. This inherent design makes the incorporation of remote access technology within networking devices easy and rather common.

Remote access solutions for networking are generally seen in two basic forms. On the hardware side, they are seen in the actual devices such as hubs, switches, and routers that manage data across the network. On the software side, they are seen in supplemental applications that provide tools to remotely manage existing networks.

a) Remote Networking Devices:

There is a great deal of variety in the networking hardware that is currently available in the world today. The simple classification of a device, such as a hub, switch, or router, can no longer define the true nature of each piece of networking hardware, as even the simplest of devices can incorporate a great deal of extra functionality. In this same way, internet appliances have emerged to have a strong presence in the market, cultivating networking technology to meet very specific purposes(NetReach, 1).

Remote management technology for networking devices can be viewed in this same way. Not every specific device is designed to be managed remotely, but the capability for remote management functionality exists in almost every product classification. The devices which have the capacity to operate remotely have an increased cost and require more configuration than less sophisticated devices, but they are obtainable and are very common in existing business networks.

The primary protocol responsible for remote management of networking devices is SNMP, or the Simple Network Management protocol. Applications of SNMP involve software on both the server and the client, and functions by allowing a remote device to access a standard set of statistical and control values on each networking device. Querying these values allows the client to obtain information on the networking device itself or on the state of the network where it resides, including such information relevant to the monitoring of TCP, IP, UDP, and device interfaces(An Overview of SNMP, 2).

Networking hardware devices that are designed for remote management are constructed in a fixed format, normally hard coded with SNMP functionality that cannot be extended or modified. Although this seems to be a limiting factor in the application of imbedded SNMP technology to existing networks, as was briefly mentioned earlier, the actual limitation has led network technology providers to develop a tremendous variety of devices that cover the most prominent remote management needs(An Overview of SNMP, 2) .

The actual functionality of remote management capable networking devices are similar to those already examined in the previous investigations into remote technology. Imbedded functionality includes boot capabilities, software access, configuration, test, alert, and monitoring of both the device itself and the medium on which it resides. These capabilities, although static in each networking device, make the remote management of networks a very viable and available option, applicable to any business in the current marketplace.

b) Remote Networking Tools and Applications

While the SNMP protocol is static within networking devices, SNMP management software can be designed to examine the management information database on each device, and take advantage of what attributes are available. Devices will have preset functionality, but if their database contains unused attributes, these too can be queried and examined, adding to the troubleshooting ability of remote support. More importantly however, these attributes can be gathered as an entire set from each unit and can be compared to determine the specific differences between each device, making use of SNMP based software excellent for remote support. (An Overview of SNMP, 2). The power and versatility of this protocol has made it a primary facet in the development of many remote networking support applications, and has made customized remote network support applications relatively common in the realm of technical support.

Sun Microsystems offers remote networking tools and applications called Solstice Enterprise Agents, available on the Solaris operating system. These agents make use of both the SNMP and Digital Management Interface protocols in expanding the functionality of remote management. DMI is the base protocol for the remote management of most server/host devices, using a base level of remote procedure calls to affect the state of a given machine. Through the use Solstice Enterprise Agent applications, Sun has merged these two worlds into one, mapping SNMP requests to DMI requests and visa versa, allowing for network commands to be batched together efficiently and easily through a single interface. By using both of these protocols as a base, the functionality available is nearly unlimited, only restricted by the data that can be queried from each specific network or computing device(Sun Network Management, 1).

Vantage Console Manager is a full service remote networking application that incorporates SNMP to utilize a wide variety of functionality. The Vantage Console Manager can map an entire network of systems and devices to a single workstation, and provides connection and control to both computing systems and networking devices alike. This framework allows for a great deal of troubleshooting functionality, including the ability to reboot devices or perform a wide range of diagnostic procedures. The application also includes the ability to monitor network activity, allowing a user to examine the type and level of traffic that exists on a given segment of the network.

Vantage's most powerful capability is found in its ability to use SNMP to "trap" certain events, recognized by state changes in the specific networking device, and automate responses to instantly handle the current network state. These responses can be designed to handle a number of different roles, configuring the system as an alert, logging, or even corrective mechanism in response to a specific set of circumstances(Vantage, 1).

On the lower level of network support, there are a number of very useful, low cost tools that can be used to monitor and manage network performance remotely. Many network packet sniffing applications, or programs which allow a user to monitor a given network or segment on a packet by packet basis, are readily, and even freely, available for download, giving any organization and excellent resource for network support. Although, for remote support, some applications, such as Ethereal, would require a remote software access methods to make use of the technology from an off-site location, there are those that are designed in this manner, incorporating remote functionality directly within the framework of the software application(Ethereal, 1).

Wildpacket's RMONGrabber technology expands the base packet sniffing technology into a remote format by the use of a custom networking device, called an RMON probe. By use of this design, a provider could limit the management overhead required when using multiple access and monitoring applications, allowing multiple networks and multiple data flows to be monitored simultaneously and easily through windowing functionality built in to the base interface. In addition to this, because RMONGrabber is centered around a static hardware interface system, the application incorporates some extra functionality, allowing the user to build peer maps that are based off of the current network architecture, perform high level analysis on the network state, and generate data and reports based on historical network activity(Network Administration, 1).

c) **Remote Network Support Methodology**

Supporting the networking needs of small business from a remote location will require a unique mix of hardware and software tools for each individual client. The use of equipment and applications cannot be completely standardized, as different business architecture's will require different kinds of equipment depending on the number of devices, users, and the level of expected network traffic. An initial assessment will have to be made for each business that is supported, and the necessary topology will determine the networking devices required.

Some aspects of the methodology can be standardized on a high level, across all of the organizations supported by a provider. A common interface should be used to interact with whatever tools and devices each client requires, giving the provider a standard means of monitoring, testing, and configuring the current state of the network.

As a total solution, a remote network support provider will need to install devices to manage the flow of traffic across a client network and configure them to be accessed remotely. Software will be used to both generate network information and device comparisons through SNMP, as well as to manage the data collected from the SNMP queries on each device. In addition, tools should be used to monitor such things as total network traffic and the load on critical devices, giving the provider the ability to recognize potential problems before they affect the stability of the client network

2. Remote Network Management Business Factor Comparison

a) Cost Examination

As was discussed under the remote network methodology, the hardware costs for the support of a small business network will vary greatly between each client topology. With a completely variable amount of workstations, servers, and network load, it is impossible to predict the networking devices that will be required, so as to average the cost over a specified number of clients. Beyond this restriction however, there are some constants within the remote networking schema that can be used to gather some relevant cost information.

Although it cannot be directly quantified, network hardware that can be configured remotely will always require a greater investment of capital than devices that are strictly designed for local configuration. The extra functionality found in remotely configurable devices is becoming more mainstream, but until it is the standard, there will be an extra cost associated with its purchase(NetReach, 1).

A remote network topology taking advantage of the SUN Solstice Enterprise Agents would require two separate licenses to manage both SNMP and DMI. Each license is perpetual, priced at eighteen hundred dollars each, and has no limit to its use on client's or servers across the organization. Support can be purchased for each individual agent on an annual basis at a price of six hundred dollars. The software can only be run on a SUN operating system, requiring some significant overhead in using these tools to manage a client's remote support needs, but, as the software cost is not scaled by its use, it can be a very cost effective solution if applied to a number of different networks(Sun Network Management, 1).

For those who wish to use to the remote network monitoring design offered by WildPackets, licensing must be acquired for both EtherPeek NX, the local monitoring software, and for RMONGrabber, the software which allows this data to be transported across a switch or other network "blockage" (Lipkind). Both licenses for the WildPackets software are bundled with either twelve or twenty four month support and are priced in a manner that makes the larger service contract attractive, having only a five hundred dollar difference between the two levels of service.

Where the EtherPeek NX software is not limited by the number of clients it can manage, the cost of RMONGrabber is further divided between one which is able to retrieve data from up to five segments and one which has unlimited segment retrieval capabilities, making the pricing structure flexible for the management of small business clients(Network Administration, 1).

Vantage Console Manager has a two tiered pricing scheme, with a cost of one thousand dollars for the base product and additional two hundred dollars for every device the application can monitor simultaneously. For service, ASP Technologies markets two different service plans, offering both twenty four hour/seven day support and eight hour/five day support. Each of these plans has a cost which is based off of the total price of the purchased product, costing twenty-five percent and seventeen percent respectively. In addition to these service packages, ASP Technologies offers onsite training for Vantage at a price which varies with the time allotted and the level of expertise desired(Dickerson).

The nature of this scheme is a bit restrictive for use in a remote small business support methodology, as it would force a provider to purchase a different base license for each separate client location. This base cost structure seems better designed for large businesses who intend to hook up many devices to a single license, and not the management of many smaller networks. However, with the tremendous functionality found in Vantage, it is possible that this single product could replace the hardware, software, and networking needs surrounding many critical devices, making it cost effective on the higher end of small business support, and at least worth consideration for some client network topologies.

Remote Networking Management Costs (Cost to cover a large network)

Sun Solstice Agents	
SNMP Licensing	$1800
DMI Licensing	$1800
WildPackets	
EtherPeek NX (12 month support)	$3495
EtherPeek NX (24 month support)	$3995
RMONGrabber (12 month support, 5 segments)	$500
RMONGrabber (24 month support, 5 segments)	$600
RMONGrabber (12 month support, unlimited segments)	$2500
RMONGrabber (24 month support, unlimited segments)	$3000
Vantage Console Manager	Variable
TOTAL COST (Idealized for a single large Network)	Variable*

***Dependent upon network size, level of support required, and types of devices**

b) Timeliness

Regardless of whether networking support occurs on-site or remotely, there is always a remote aspect inherent to the monitoring of networks. Information must be scanned on a network segment and passed onto a server which can analyze the data. Remote networking support only expands the distance where these packets are passed, adding only a very small amount of delay to the monitoring process. As the distance between the client and the provider increases, some instability risks are assumed as a product of expanding the process from the controlled area of the private network to the Internet. These risks are relatively minor however, and should not deter small business organizations from employing remote network monitoring techniques.

As in the investigation into remote hardware and software support, networking devices can be manipulated and configured easily, with no significant impact to operations. Software tools that utilize alert mechanisms can be used to flag problems on network segments immediately as they occur, making troubleshooting fast and seamless.

c) **Technical Capability**

Remote networking hardware employs hard coded functionality which allows for the configuration of networking devices and the manipulation of a device's powered state from a distance only limited by network access. As networking devices are designed with great variation in functionality, devices can be purchased to support the specific needs of almost any client, lending the provider some extra flexibility in implementing a given client network.

Remote networking software allows for networking devices to be queried for information pertaining to their state and the state of their associated network segment. This information can then be used to compare and contrast the state of other devices, other segments, or saved data from a query of the same device or segment at a different period in time. As these queries can be customized and automated, the provider can remotely generate a tremendous amount of valuable information pertaining to a client's network state, and thus supply some very powerful functionality to the topological design(An Overview of SNMP, 2).

The biggest drawback found in the in the technical capability of a remote network support topology is in its inability to manage the network medium. Although devices can be managed and configured, and the state of the network can be determined easily, there is simply no remote way to replace broken network segments or damaged networking devices without having some form of on-site presence at each client site, exhibiting a major flaw in the use of a remote topology.

3. Remote Network Management Conclusion

The base structure of networking technology fits very well with the needs of a a remote support topology . As remote support relies upon the existence of network technology to make its entire design possible, the monitoring and troubleshooting of such technology does not require much beyond the tools and applications that are currently available.

At the heart of remote networking technology is the SNMP protocol, allowing for the manufacture of remotely configurable devices and the generation of software which can gather data from a targeted network device or segment. As SNMP software can be used to gather any information found in the attributes of a networking device, network troubleshooting is made extremely easy, as the technology allows a provider to customize software tools on a client by client basis. The combination of SNMP hardware and software technology allow for a provider to have near complete control over a client network, making the topology a very powerful method of IT support.

The one aspect which is not handled well by a remote networking support topology is in the management of the medium. When facing problems relating to a broken network segments or a damaged network devices, the provider has no on-site personnel to incorporate what would normally be an easy fix to the problem. As the topology does not incorporate methods which would allow for easy travel to the client site, the actual replacement of networking components from within this design could easily incorporate an unacceptable addition of cost and client downtime that would make it unattractive to small businesses.

This problem can be managed through the use of redundancy in networking technology. Although this method would incorporate a higher level of cost, requiring the near duplication of every segment and device within a client network, it would allow for the provider to reduce the threat of downtime to the client. Although damaged hardware would eventually need to be replaced, this method would reduce the critical nature of the fix, and lower the overhead cost associated with travel to the client site.

A remote networking support topology relies on technology which is already present within networking devices and software to carry out the configuring, monitoring, and troubleshooting of a client's network backbone. A tremendous amount of hardware and software currently exists on the market to fit the needs of nearly any small business client, at a cost which is both scalable and affordable. These factors make network support very suited for use in a remote topology for small business, offering the benefits of cost and functionality at a similar response time, to both the client and the provider.

F. Security services/management (Propensity to Outsource: 25%)

In dealing with small business clients, the burden of security mainly falls on the network. Primarily, the role of security services management is to protect resources on a point to point basis, securing data throughout the entire lifecycle of an information exchange. To accomplish this, service organizations offering security consultation utilize a bundled package of software and services used to monitor and manage entry, data flow, and access to resources across a client's network. Security is often overlooked by small businesses when allocating their information technology budget, but, since small business IT infrastructure often acts as the backbone of the company's profit making activities, it is, in actuality, a significant organizational need(Middleton, 1).

The data that is generated by the every day activities of a company is an extremely valuable resource that needs to be accessible and protected at all times. Information, although intangible, is usually an organization's most valuable asset. What a company knows, the processes it follows, and the information it holds on clients, products, and services, are central to its business. Due to the sensitivity of this information, allowing this data to exist unprotected could hinder the profitability of a company, resulting from the loss of important information, theft of company resources, or client liability.

To ensure business stability, data must be secured, requiring a dedicated group of employees to manage the resource. A security services provider is responsible for the installation of security management tools and the monitoring of client workstations, servers, and network connections. In addition to these tasks, a security services provider is usually responsible for initiating business policies and procedures that aid in protecting company resources(Blake, 1)..

For the security services organization, the cost of overhead in taking on a new client is high. Constant monitoring of client resources requires a constant devotion of skilled personnel, passing on a significant amount of cost to the client. Considering the low budget normally allocated to information technology resources for an average small business, this cost very difficult to manage.

The only way to truly protect a company's data is through constant skilled management of its network, making it difficult for a small business to employ the measures it needs to secure its vital information. Using an on-site format, this method can prove far too costly for a small business forcing it to choose between incurring the high costs of support, or leaving their data susceptible to attack(Ranum, 1).

A remote technology solution could be the answer to this problem for small businesses. If a security services provider was not required to devote on-site staff to manage its clients, the organization could multitask its employees between different projects, utilizing alert software to determine if there was an intrusion on the network In addition, if the provider was able to access the client network remotely, any investigation into the client system or tests run against security countermeasures could be completed from their home company site, lending a wider diversity of skill, manpower, and tools to the solution of any problem.

A remote solution for IT security would provide benefits on the provider side as well. The business of security services deals in an extremely competitive market, where cost cutting is a common measure taken to attract new business. By multitasking employees, a provider would become far more efficient in their managing of clients, both in their ability to solve problems faster, and by the application of less devoted manpower to a client site. This increase in efficiency could eventually lead to an overall decrease in overhead, allowing the company to operate with a lower level of income, and pass on a reduced level of costs to its client base.

1. Remote Security Support Technology Investigation

Security is a very broad area, including a variety of tasks such as the securing of physical resources, information management, policy management, system administration, and network design. Although the entire range of security risks is of consequence to a client's business, an organization that is providing remote support for a client's security needs will only be providing a limited version of this spectrum, offering services that will secure access to a client's data, devices, and network.

Although the activities of a remote security provider may touch upon the physical aspects of security management, this will most likely be in the form of consultation, pushing most of this responsibility to the client organization. As the aspect of physical security will be, at best, a secondary objective of a remote security provider, it will not be examined in depth in this investigation, focusing primarily on managing access, monitoring network activity, and troubleshooting security problems as they occur.

a) Remote System Administration

On the software side, the protection of data begins with the ability to restrict access and monitor activity on the client network. In an on-site solution, a system administrator is normally responsible for this, designing policies to grant authenticated users access to internal systems and devices, while monitoring system logs for activity that could threaten the organization(Frisch, 202).

In a remote format, the role of system administrator does not change. For the topology to be effective, a system administrator must be able to accomplish the same tasks that are required of one located on-site, over a secure connection.

Through the use of the Secure Shell Protocol, an administrator can access domain controllers within a client organization over a secure connection, providing direct access to logs and control over the target domain. Secure Shell is a product designed to replace unencrypted access tools such as telnet, rlogin, and remote shell with a secure tool for remote access Secure Shell employs DES, 3DES, IDEA, and Blowfish encryption, making it a very useful tool for accessing and manipulating sensitive information pertaining to the client network(SSH, 1).

Although this secure access is a vital requirement for remote system administration, remote security requires much more functionality then the simple use of SSH can afford. To truly secure the business operations of multiple clients remotely, a system administrator will need software that manages and streamlines the devices, information, and processes existing at each business site in such a way as to make it easy to manipulate.

Smartline offers a group of products that fulfill this need. Smartline offers software which gathers information on the day to day operations of a given network, and allows system administrators to assign permissions to both hardware devices and TCP/IP ports, merging many of the system administrator's duties to ease the management of the client site. The company also offers a remote task management application, specifically designed to give a system administrator near to full control over the security of every device and available process in the client network, lending a significant amount of functionality through a single centralized GUI(Info Security, 1).

Lastly, a remote topology requires an automated monitoring system in order to get the attention of a system administrator when something unexpected occurs at the client site, such as an intrusion on the system or an unscheduled change to a critical configuration. Although this tool could be a vital element to any support topology, it can be extremely useful for providers who will be managing multiple client networks using remote support architecture. System Administrators will more than likely be assigned to manage multiple small businesses, and alert mechanisms provide a very strong means of prioritizing their attention.

The company IPSentry develops network monitoring software that seems to meet this requirement. When configured to a given network, the software continuously monitors nearly every aspect of a given system, generating information on such things as networking devices, servers, ports, drive space, and event logs. Once this information is generated, the software is able to analyze this data, flagging problematic occurrences. Once these events are flagged, the application is able to directly contact responsible system administrators through email, beeper, or phone, alerting them to the event(IPSentry, 1).

b) Remote Security Support Methodology

Although there are a multitude of software and hardware packages which can be implemented to secure a small business client environment, in the simplest scenario, there only a few technological aspects which are needed to bridge the gap between the remote provider and the small business site.

The most important aspect of this topology is the provider's ability to access the servers and domain controllers that manage the client network. Without the ability to perform the most basic system administration tasks such as checking logs and manipulating system files, securing a remote network would be nearly impossible. As was discussed earlier, through the use of SSH, a system administrator can access client resources easily and securely, relying on the embedded encryption to protect the confidentiality of the exchange Although there are other technological solutions which could replace SSH for this purpose, since the protocol covers a wide range of administrative tools and is easy to implement, SSH will be used to fulfill this aspect of the remote security model.

Accessing resources remotely adds a level of difficulty to everything that is required of a system administrator. Those utilizing an on-site topology have the advantage of examining the physical components of a network, giving a much better perspective on the client's topology than those who can only rely on reports generated from the client network. As a remote security provider for small business will likely have a number of different clients to manage, it is extremely important for the provider to be able to examine, manage, and easily manipulate every aspect of the client site. As was mentioned earlier, Smartline's software line offers administrative packages which can accomplish this, and its products will be examined in attempt to match the topology's needs in this manner.

Lastly, a remote security provider will be multitasking a number of different client sites, and will be forced to rely on electronic monitoring and automated alerts so as to best direct the attention of their system administrators. The packages offered by IPSentry meet this need, offering a wide range of detection and alert options, and will be used to fulfill this aspect of the remote security topology.

2. Remote Security Management Business Factor Comparison

a) Cost Examination

Licensing for SSH is free for non commercial clients, but has a cost of one hundred sixteen dollars per license for business or educational use. For a service provider to adequately provide remote system administration to small business clients, a separate SSH license is needed for each server or domain controller within the client's network. As this is the only cost associated with the technology, expansion of the client network can be handled by the provider without a significant impact to overhead cost(SSH, 1).

For Smartline software, the company offers two kinds of licensing which could be applicable to small business clients. The first and most cost effective of these purchasing packages offered is called a "site" license An owner of a site license is granted the right to apply a given software package to a maximum of two hundred computers within a single network domain or network group. As most small business clients should fall into this basic format, the licensing structure is very feasible for use in a remote service topology. The site license cost for DeviceLock, PortsLock, and Remote Task Manager are fifteen hundred dollars, two thousand dollars, and sixteen hundred dollars respectively. In addition to these, the Remote task manager also come available in smaller license packages, allowing for the purchase both ten and twenty license packs, making it more applicable for very small networks.

For those small businesses with more complicated network architectures or those who have more than two hundred devices which need to be supported, Smartline offers a "world" licensing package. The world license grants an organization the right to install a given software package on up to two thousand computers on all domains within a single geographical area. Although this license is far beyond what a remote small business service provider would need to support, it grants the service organization the flexibility to manage special clients with complicated network structures as well as the maintaining the business of clients through the growth of their organizations. The world license cost for DeviceLock, PortsLock, and Remote Task Manager are four thousand five hundred dollars, five thousand five hundred dollars, and five thousand one hundred ninety-five dollars respectively(Info Security, 1).

IPSentry also has a flexible licensing structure, offering both a "site" license and an "enterprise" license which could be applicable to a remote service topology. Unlike the Smartline licensing packages however, the higher level package is more flexible, granting an owner the right to install and run the licensed software on multiple machines, at multiple locations, within a single corporate entity. IPSentry offers a number of different products to monitor a variety of different activities, with a cost base which ranges, on the enterprise pricing structure, between five hundred dollars and one thousand nine hundred ninety-five dollars(IPSentry,1).

Remote Security Management Costs (Cost to cover 100 machines)

SSH	$116/server or domain controller
Smartline	
Device Lock (Site)	$1500
Device Lock (World)	$4500
Ports Lock (Site)	$2000
Ports Lock (World)	$5500
Remote Task Manager (10 license pack)	$350
Remote Task Manager (20 license pack)	$600
Remote Task Manager (Site)	$1600
Remote Task Manager (World)	$5195

IPSentry	
Single License	Variable($99-$465/device monitored)*
Site License	Variable($365-$1,795)*
Enterprise License	Variable($1995-$8195)*
TOTAL COST	Variable(Dependent Upon Client Needs)

***Ipsentry pricing is dependant which devices need to be monitored, and will vary greatly from network to network.**

b) Timeliness:

The use of remote technology to manage small business security does not significantly impact a provider's response time. Through SSH technology, the access and deployment of applications, patches, and other files can be done quickly and easily, losing only what time is required to transfer data over the Internet. As much of the duties of system administration only require access to logs and other information pertaining to network activity, the use of remote access to manage these tasks is fairly common(Frisch, 1-2).

The key to remote management however will be in the use of tools and applications to make each site as easy as possible to manage. As a provider will be managing security for multiple clients, each site, although unique in structure, will require a common internal architecture. By organizing each client in this manner, a given administrator will not lose any significant time adjusting to each individual site as problems occur. Remote management tools, such as those found in Smartline's Remote

Task Manager software, can be found in many forms, and should be used consistently across a provider's client base to make the management of each site as similar as possible.

Although a remote system administrator operating out of this methodology will rarely view events that occur in real time, IPSentry software can allow for a better concentration of effort, signaling the designated administrator when security issues are most crucial. Since IPSentry can contact responsible individuals through a variety of different communication devices, the system is flexible, and can be tailored to achieve the fastest response time possible.

c) **Technical Capability:**

For the easy management of each client, a greater effort must be placed in the initial implementation of network restrictions and monitoring schemes than on a system which was overlooked by a full time, local system administrator. Managing the security of multiple sites requires a significant level of automated management to be present in the client network, so the attention of the administrator can be directed towards only the most pressing problems.

Through Smartline software, the extension of user, group, and world permissions to devices and ports allows for a more advanced network design, giving the administrator more control over the capabilities of the average user. By use of the DeviceLock and PortsLock applications, these newly attributed rights are checked each time a device is accessed or each time a user attempts to access a given port, allowing them to be monitored and logged, generating valuable information that would not otherwise be available for the administrator's use(Info Security, 1).

Once the implementation of the network is complete, remote management of the network differs very little from an on-site topology. SSH employs powerful encrypted tools which grant an administrator secure terminal to access local accounts, and the ability to move and manipulate files on the client network. Since any security management software installed on the client network can be utilized through access to an account with the appropriate rights, the secure remote communication granted by SSH makes maintenance of the client network fairly simplistic.

3. **Security Services/Management Conclusion:**

Using a remote topology to manage the security of a given network uses nearly the same applications and techniques as an on-site provider. Since most of the software used to manage security resides on a local server or domain controller at the client site, as long as these tools and information can be accessed securely through the internet by a system administrator, both methodologies can work equally well.

For a remote security topology to work effectively, a more complex and thorough initial installation of tools and applications is required on the client network. Servers for secure remote access, applications used for monitoring and alerts, and automated tools used to ease the tasks of the administrator must be implemented to ensure that a remote administrator is able to fulfill the duties of the position. Although there is a significant amount of overhead involved in establishing this topology, there are a significant number of benefits that come with its use.

As with the other small business needs, by using a remote topology to manage the security of small business networks, a provider can multitask sites and centralize their operations to gain the maximum possible effort from their employee base. The cost of purchasing the extra software required to support the needs of a remote administrator are outweighed by the savings generated in centralizing the provider's employee base and in the reduction of multiple works sites to a single center of operation.

Unlike the other small business needs however, the remote management of security comes with significant risks. Although the software available seems to provide all the necessary tools and applications to manage a site securely over the internet, the methodology inherently relies upon stable access to the client network to regularly monitor the system.

Although all of the remote service support techniques require access a primary means of maintaining support over a client organization, in other investigations, this was viewed as a minor detriment to the use of the technology, simply impacting response time, and not a direct failing of the methodology. In remote security support, this is not the case.

System security administration requires regular monitoring of the protected system and constant manipulation of permissions, files, and user rights to handle the needs of the given client or its employees. Even the smallest impact to this could cause employees to become unable to access necessary data or devices, halting some measure of the client's business activities. On the server side, a denial of service attack could render such a topology completely useless, giving an intruder the ability to separate a system administrator from the network before attacking the system. Although a backup system could be used to communicate between the two systems, the risk of being separated from the client network will always be present.

Even with this risk however, for those clients who have a small network to manage, the employment of a remote security service provider may meet their needs. The cost savings found in a provider's ability to multitask operations and workflow could make remote administration an attractive option. Since a provider will have a significantly smaller number of resources to cover than in larger business topologies, automated monitoring implemented at the client site should be able to adequately handle the information technology security needs of most small businesses.

G. Small Business Needs Conclusion

After examining the technology currently available in today's marketplace, it is apparent that the knowledge exists to manage the primary needs of small business through the use of a remote support topology. The tools required to remotely access, troubleshoot, and manipulate client devices are readily available through multitude of different information technology providers. More importantly, the use of this technology passes on significant savings due to an increase in work efficiency and a decrease in required overhead, stemming mainly from a reduction in required manpower and physical bases of operations. Even with these advantages however, the use of a remote topology as the only means of providing information technology support to small business clients is far from a complete solution.

A remote support topology is at its strongest when dealing with issues that are related to the support of software, networking, or server and host management. When dealing with problems in these areas, each critical element of client resources can be accessed quickly and easily, the tools available in a remote format offering similar functionality to those that would be used in supporting the problem on-site.

In the area of Web Hosting, remote support is a possibility, but the topology is constrained, as it requires the client to purchase their own web server and maintain it on their own site. As this is not the traditional format for web hosting, even though the technology strongly supports a provider's ability to manage a web server through a remote topology, use of these tools to fulfill the small business need cannot be viewed as a complete success.

The most significant problems for a remote support solution are revealed when attempting to manage hardware or security needs for small business. Unlike the other small business needs, each of these areas of support has an intrinsic flaw which can never be completely covered by the technology currently available, leaving major risks to the business stability of any client that utilizes the solution.

For hardware support, the flaw in the topology is very prominent. Any device that suffers a complete failure will always require on-site manpower to replace the technology. No matter what measures are taken to secure the client site against such an incident, hardware failures will eventually occur, and the problem simply cannot be managed remotely.

In security support, although the issue with a remote solution is not as obvious, the impact of its failing is far more significant. Utilizing the network to manage security is only viable if the provider can maintain stable and secure access with the client site. As many electronic threats center around the "denial of service" to a given organization, the primary requirement of the remote solution will always be in risk of attack, creating a method of security that contains a major inherent flaw.

It is important to note however that, although both of these problem areas create drawbacks to the use of a remote solution to handle the small business needs of security and hardware support, its use cannot be ruled out completely. Although each of these risks cannot be entirely circumvented, there are some techniques which can be used to limit the impact of the topological flaw on the client, making the risk acceptable to small businesses that are willing to exchange some extra risk for a significant cost benefit.

For managing hardware support in a remote topology, redundancy seems to be the primary solution. By using secondary devices to lessen the impact of hardware failure on a small business environment, the provider can replace damaged equipment without inhibiting a client's normal business workflow. As the client's business activities are not hampered by the provider's inability to immediately replace the damaged device, the topology becomes much more viable.

However, since the solution will still require the remote provider to travel to the client site for the replacement, and the client still faces the risk of having their business activities halted if the redundant device were to fail, a remote topology cannot truly match the stability of on-site support. In addition, the cost of providing redundant technology to implement the technique could considerably reduce the cost savings a provider is able to pass onto the client.

For security, the use of a secondary or even tertiary method of access could protect a provider from being completely cut off from a client site. Although this risk can never completely be removed, as each point or method of access used would always be vulnerable to attack, use of separate access methods would lessen the possibility of an such an event from occurring, making the solution much more stable. Although, as with hardware support, the use of this solution requires an additional cost to maintain the backup methods and mediums of access, it is still seems to be the most effective solution. With the risk of isolation dramatically lowered through this technique, remote security could be very attractive to those small businesses who require a provider to manage their security needs.

As a whole, the needs of small business organizations seem to be very manageable through the use of a remote support topology. Through a variety of hardware and software tools, each need of small business can be met in a manner which could make it attractive, both though its savings in cost and its unobtrusive nature, for small business use. Although managing every small business need in a purely remote format is not currently possible, supporting a subset of these needs, or employing a method of support that uses a remote format as its primary method of support, is certainly an employable solution.

V. A Final Comparison Between a Remote and an On-Site Topology

With the determination that current technology exists to support a small business's information technology needs on some practical level, a comparison needs to be made to determine if the economic impact of using technology to reduce manpower, multitask employee effort, and reduce a provider's overall fixed overhead will be significant enough to promote a shift to this new ideology.

By its design, a remote service topology shifts the burden of work from manpower to software and hardware, utilizing monitoring and alert methods to minimize the amount of dedicated work a given employee needs to apply to each client site. This increase in production per employee should inevitably result in a reduced need in overall manpower for the provider, generating significant cost savings. So as to be modest with the initial assessment, for this comparison, it will be assumed that this centralization and multitasking of a company's full skill set will allow every three employees working within a remote support topology to handle the work of four employees working on-site. Although there are additional savings accrued by such an organization through the centralization of administrative overhead, these benefits will also be ignored for the moment, in an effort to make the most fair assessment of the basic solution.

There are two separate ways this benefit can be examined. An organization could either reduce manpower and generate more revenue from maintaining a smaller staff of employees to manage its current client base, or an organization could expand, taking on new clients and generating new profits out of its increased efficiency. Although basic business theory dictates that the profit generated by a company will be more substantial than its overhead, thus making the expansion to new clients the most advantageous use of the new found capital, there is no guarantee that clients will be immediately available. As market conditions will generally dictate a provider's ability to expand in this manner, the reduction of a provider's overall employee base becomes much more quantifiable, and, as such, will be used for this assessment.

Although each individual client and each managed small business need will require a unique set of tools and technology to support, an average theoretical cost can be obtained from the evaluations gathered within each small business need investigation. To simplify the cost assessment, the examination will assume the support of the full client base of a single provider, generating a random array of needs as case model for each support topology. In a true working environment, the technological skill sets of many employees will overlap between each of these small business needs, allowing for a higher level of multitasking by the provider, but, so as to further reduce the complexity of the cost assessment, it will be assumed that employees are inflexibly dedicated to a specific need..

So as to examine the cost from an enterprise level, in the previous small business need investigations, each assessment considered the management of one hundred devices. Although we will use these underlining values to determine the cost for the current feasibility study, the total cost given will be used as a ratio, adjusted so as to match the requirements of the proposed environment.

A recent Gartner group poll lists the average total cost of a single information technology employee at seventy thousand dollars(Berry and Mok, 5). Using this cost per employee as a basis, with the reduction of a single employee from each project, this value can be applied against the technology cost of each small business need, to determine the overall gain or loss attributed to the new topology.

A. Case Study Comparison

The client base for the mock provider will consist of four small business organizations, each requiring a different level of support due to variations of size, business activity, and infrastructure. Using the stipulations detailed in the previous section, the needs of these organizations will be met using a remote service support topology, comparing the final technology and manpower costs to the manpower cost for an on-site solution.

The first organization in the mock provider's client base is an advertising agency. The company has a small number of employees, but their company relies greatly upon graphical design tools and their ability to secure their work against disaster or theft. The entire organization operates on a single network, and network traffic mainly consists of saving and restoring projects out to a few local servers.

Small Business A: Advertising Agency	(45 Employees)
Workstations	45
File Server	2
Web Server	1
Requires Backup Services?	Yes
Requires Deployment Services?	Yes
Requires Network Support?	Yes
Security Requirement	High

The second organization supported is a small law firm with a sizeable number of employees. Each employee has access to a workstation, and most of the employees rely heavily upon their ability get to data, stored both internally and externally, to handle their current case load. Although there is not a high reliance on specific software applications and tools, the ability to use the network to save, retrieve, and secure information is a critical need. As with the first small business client, the nature of the client's business requires a high level of security against disaster or theft of its business critical information.

Small Business B: Law Firm	(100 Employees)
Workstations	100
File Server	5
Web Server	0
Requires Backup Services?	Yes
Requires Deployment Services?	No
Network Support?	Yes
Security Requirement	High

The third organization is a small magazine publisher, with only a handful of employees that utilize information technology resources. The company is mainly concerned with a low level of technical support and the maintenance of its web server, the primary advertising agent for its customer base. Although the company is concerned with the security of the web server and its content, the organization does not rely upon any critical data to perform its business activities, and is thus not overly concerned with theft. In addition, as the organization only produces a single magazine on a quarterly basis, it prefers to handle data backup internally. Although the company has access to the web, it does not operate off of an internal network, and thus requires no network support beyond that offered through its internet services provider.

Small Business C: Magazine Publisher	(20 Employees)
Workstations	5
File Server	0
Web Server	1
Requires Backup Services?	No
Requires Deployment Services?	No
Requires Network Support?	No
Security Requirement	None

The last organization in the provider's client base is a large construction company that requires support for its administrative branch. The organizational branch manages internal accounting information, as well as work information pertaining to the company's past and current business clients. The company uses a few data servers to archive past information, and requires security to protect its critical data. Although the most recent data is kept locally on the workstations of those employees dedicated to each current project, archived information from past projects is considered vital, and must be backed up off site.

Small Business D: Construction Company	(60 Employees)
Workstations	60
File Server	2
Web Server	0
Requires Backup Services?	Yes
Requires Deployment Services?	No
Requires Network Support?	No
Security Requirement	Moderate

By examining the needs of these small business clients, a few budget factors become more clear for the provider. First, although each of the four small business clients will require different levels of support depending on the specific needs of their organization, support of non-critical devices can be applied to the whole of the provider's client base In addition, many of the needs of critical devices can be modeled after the non-critical units, building upon licensed software from lower support schemes. These two factors will allow for a provider to purchase a more cost effective and flexible licensing scheme, and the total budget of the schema will scale beneficially as the provider's client base increases.

Secondly, it is clear that the number of critical information technology devices that require support within each client organization are few. Although this trend will restrict a provider's ability to take advantage of high volume pricing packages in their critical device support schema, it will also make the cyclical gain and loss of small business clients manageable, as well as reducing the overall cost for purchase on the higher levels of technology.

Lastly, the networking and security needs for these small businesses, although a primary need, do not involve complex information technology architectures. The need for support in these areas stems from the managing of a few servers and the protection of critical data. Although there are many complex tools available for remote administration of networks and security, for the most part, these will not be required by small businesses, as basic system and policy management should be able to cover the need sufficiently.

Using the information gathered from the remote support technology investigation, the cost analysis performed under the business factor comparisons for each small business need, and the trends established within the client examinations, an estimated budget requirement can be generated for the cost overhead required to implement a remote support solution.

1. Remote Support Overhead Cost Schema

Non-Critical Devices:		**Number**
Workstations Requiring Support		210
Support Type Required	**Technology**	**Cost**
Hardware/Software Support	Wake on LAN NetOp LANDesk Client Manager	$30, 870.00
Non-Critical Device Subtotal		**$30,870**
Critical Devices:		**Number**
Web Servers Requiring Support		2
File Servers		9
Support Type Required	**Technology**	**Cost**
Hardware	Mega RC G2 Sandra NetOP	$7,216.73
Software Support	Ecora Reporter (Subscription)	$18,920.00
Web Server Support	WebLoad (2 machines, 1 node) Analyzer (2 machines) WebFT (1 license)	$3,200.00
Critical Device Subtotal		**$29,336.73**
Client "A" Requirements:		
Support Type Required	**Technology**	**Cost**
Workstation Software Deployment	Prism Deploy	$1,575.00
File Server Backup	ZipToNet	$81.52
Network Support	RmonGrabber (5 segments) EtherPeek	$500.00 $3,495.00
Security	SSH IPSentry(Site)	$116.00 $297.00

Client "A" Subtotal		**$6,064.52**
Client "B" Requirements:		
Support Type Required	**Technology**	**Cost**
File Server Backup	ZipToNet	$203.80
Network Support	RmonGrabber (5 segments) EtherPeek	$500.00 $3,495.00
Security	SSH	$116.00
	DeviceLock(Site)	$1500.00
	IPSentry(Site License)	$395.00
Client "B" Subtotal		**$6,209.80**
Client "C" Requirements:	**Technology**	**Cost**
None	None	None
Client "D" Requirements:		
Support Type Required	**Technology**	**Cost**
File Server Backup	ZipToNet	$81.52.
Security	SSH	$116.00
Client "D" Subtotal		**$197.52**
Total Remote Support Overhead:		
Support	**Cost**	
Non-Critical Device Subtotal	**$30,870.00**	
Critical Device Subtotal	**$29,336.73**	
Client "A" Subtotal	**$6,064.52**	
Client "B" Subtotal	**$6,209.80**	
Client "C" Subtotal	**$0**	
Client "D" Subtotal	**$197.52**	
Total	**$72,678.57**	
Average IT Salary	**$70,000.00**	
Cost Difference	**(2,678.57)**	

2. Case Study Conclusion

Using the results of the above data, some prevalent trends become clear regarding the cost overhead associated with the remote support of small business clients. First, although the technology costs are lower on a per license basis, the raw sum of devices that need to be supported causes the majority of the costs to stem from the software and hardware support of each organization. With eighty-seven percent of the total cost for the schema packaged within these two small business needs, and the provider's ability to take advantage of economies of scale by licensing the hardware and software dedicated to these needs across its entire client base, the topology appears very economically and physically manageable.

Secondly and in association with the first trend, the total costs associated with the specific needs of each organization are very low, allowing a provider to tailor its support to each client without sinking a tremendous amount of capital into the establishment of the support topology. Although the costs stemming from remote hardware and software support will still be significant, these costs are sunk, and can be shifted to be the base of a remote support topology for new clients or with the expansion of clients already associated with the organization.

Lastly, the total cost of the remote support topology overhead and the average cost of a single IT employee are nearly identical. At first glance, these figures seem to indicate that, if by the use of remote topology, a provider can reduce their IT employee base by one for every four clients it supports, the cost benefit will be nearly even between the two methodologies. However, as many of the unquantifiable benefits of utilizing a remote support topology are not included in the cost evaluation study, such as the centralization of a company's employee base, the total multitasking efficiency gained from the solution, and the reduction in physical asset and administrative overhead across the company as a whole, this seemingly similar cost value actually shows tremendous value in the application of a remote solution to small business clients.

VI. Conclusion

Supporting small business organizations is a complicated issue for information technology service providers. Although there are a number of significant IT needs in which small companies require support, including hardware, software, web hosting, server/host management, network, and security, the profit potential of providing service to these businesses is usually not worth the dedication of a company's personnel and resources to the client site.

In response to this, most IT service providers concentrate on large businesses, attempting to maintain a small number of big business contracts rather than to delve into the small business market. Large businesses can guarantee longer contracts to supporting organizations, and can thus secure the provider's investment in capital more directly than their smaller counterparts. In addition, this business strategy will result in having the majority of a provider's employees dedicated to a few locations, making its overall work force both cost effective and easy to manage. Although this strategy ignores a great number of possible clients and makes the competition for large business clients very fierce between support organizations, there are a number of hindrances that cause even the most successful provider's to ignore this market segment.

Small businesses are far more unstable than large organizations, having both lower revenues and operating capital that is mostly generated through loans or from the short term potential of their endeavors. Due to this, these businesses tend to have a lower budget to spend on their information technology needs and wish to engage in shorter contract agreements with providers, thus increasing the provider's overall risk of investment. As the revenue from many of these organizations would be needed to match the profit gained from a single small business, administrative factors such as the need to hire more personnel so as to handle a greater number of client sites and the expansion of business infrastructure to cover new client areas can increase the overall cost and business risk to providers significantly. In addition to this, as the support requirements of each small businesses will be different between organizations, maintaining a skill base to meet the needs of each individual company can make the support of a large number of small businesses untenable.

All of these factors combine to form a very restricted market scenario, where a large number of IT service providers fight for the contracts of a small number of large business organizations. Due to the risk associated with small business support, these large businesses have the leverage to set costs and restrictions alike, placing support organizations in a very difficult business environment. In this same respect, small businesses can not find cost effective support to cover the specialized technology needs of their organization, forcing them to engage in longer service contracts or pay higher costs, reducing their overall business stability.

The use of remote support technology can greatly reduce, if not eliminate, many of the hindrances facing small business information technology support, and address these overall market issues. On the administrative side, by use of a remote service topology, a provider can support a great number of small business organizations from a single centralized location, eliminating the need for dedicating personnel to client sites or hiring personnel with identical skill sets to manage different geographic business areas. By eliminating these hindrances, a provider's cost of doing business is greatly reduced, allowing the organization to offer lower cost alternatives to small business clients.

From the investigations completed on the basic information technology needs of small business, it is clear that the use of remote service technology is a viable alternative to on-site support. The hardware and software tools exist to remotely power, access, configure, test, and troubleshoot client devices, sufficiently covering the most significant small business IT needs in a cost effective manner. The topology is made stable and efficient through the automation of tasks and the use of applications which monitor and report upon the status of supported devices, and very little technical capability is lost in using remote service technology to bridge the gap between the client and the provider. On its own however, a remote service topology is far from a complete solution.

The primary drawback to using a completely remote support topology is dealing problems resulting from complete hardware failure. As the provider will have no employees based on-site to deal with problems of this nature, the company will be forced to send an employee out to the client site to deal with the problem, resulting in a loss of productivity and money for both the client and the provider. Although the use of redundant hardware can limit issues of this nature, reducing the impact on the client, the risk of complete hardware failure can never be completely eliminated in this methodology.

The inherent reliance upon a communication medium between the provider and the client in a remote topology creates another major risk to remote service providers. Any problems experienced with the communication medium can completely prevent a remote service provider from carrying out their client obligations, creating a dangerous bottleneck for overall efficiency. The severity of this problem can be reduced by implementing multiple methods of communication to establish a stable backup system for accessing client resources, but, as this problem will exist individually for each separate medium, the problem can never be completely eliminated.

These problems, although revealing significant drawbacks to the use of the topology, do not completely invalidate the solution. The risk associated with this form of support are outweighed by the economical, efficient means in which it can support a small business client base. By using redundancy to reduce these risks to acceptable levels, many small business clients should be willing to accept the remaining risk in order to receive the IT support they require to maintain their business operations.

In today's business world, companies are working towards the streamlining of their workforce and administrative overhead, while increasing the overall efficiency of their business operations. For IT service providers, a remote service topology offers all of these advantages, reshaping an inefficient disjointed business model with a centralized cost efficient design. With the support needs present in the small business market and the topology's ability to efficiently manage them, the future of the industry may be ready for overall shift away from the prevalent on-site industry trends of the last decade to a remote support design. Even without this however, a remote topology built using current technology is a stable alternative to the traditional methods of IT support for small business, and offers great potential for growth and profit within the IT support industry.

VII. Further Investigations into Remote Service Topologies

This investigation is based on a theoretical level, as resources were not available to gather and test the components of each small business need solution to verify that their documented capabilities matches the actual performance of the product. With the proper funding, each small business need could be investigated separately in such a manner, creating a physical representation of each theoretical remote service solution.

Although this study focused on the support of small business organizations and freelance providers, remote technology could be just as powerful an asset when applied to different client business architectures. Mid-sized and larger organizations have their own separate set of business needs that need to be fulfilled, and the use of remote service technology could help them support their IT support requirements more efficiently. Also, as was discussed in the investigation, the adoption of such technology lends to a more streamlined business architecture, and such a study may be interesting to those organizations that wish to restructure their own internal IT support workforce.

Lastly, while this investigation focused solely on the remote tools and applications currently available for use by providers, advances in the field of remote technology are occurring rapidly, changing the overall limits and capabilities of remote support. A look ahead at these developments and at the possible impact they will have on remote service solutions could address some of the major drawbacks associated with the use of a remote support topology, and give insight into the future of the IT support industry.

VIII. Lessons Learned

In its conception, this investigation of the use of remote technology to support the IT needs of small business was to be primarily taken from a market perspective, the information gathered from current IT support and small business organizations. Unexpectedly, when these organizations were contacted, many were very hesitant to detail anything regarding the cost structure of their service, the needs of small business organizations, and what techniques and technology they were currently applying to fulfill their IT support requirements. This hindrance caused the accumulation of relevant data pertaining to this investigation to come far more difficultly, and forced its emphasis to be based on indirect sources of information.

The current speed of the technological market evolution was also extremely surprising. Between the start and completion of this study, the information pertaining to technology shifted, and contact and cite information needed to be changed to match the new structure of the providing organization. This was most apparent in the investigation of the Centerun software deployment technology, which was absorbed by Sun Microsystems and directly incorporated into an existing product when the investigation was only partly completed, leaving no further possible contact with the originating organization.

Lastly, when it was possible to gather cost data directly from IT support organizations, it became very clear that as much value is placed on the cost structure and flexibility of IT support products as in the technology itself. In most circumstances, price structuring was done on a case by case basis, and not on a rigid offering of tools and services. This trend of modeling the product structure around a client's needs demonstrated the change which has occurred in business philosophy over the last decade, shifting from the desire for employees that can provide a specific skill set to be dedicated to specific tasks to that of a broad skill set which can improvise solutions to match unique client environments.

Works Cited

Adams, Igou, and Sillman. "IT Vendors Offer Technology-Enhanced Remote Support Services." Gartner Inc. January 3, 2003.
(Source document provided on attached CD)

AMI Remote Server Management. AMI.2002
<http://www.ami.com/support/doc/AMI-RemoteServerManagementWhitePaper.pdf>

Apicella, Mario. "Extending Support." Infoworld. November 29, 2002. Retrieved March 31, 2003 from www.infoworld.com.
<http://www.infoworld.com/article/02/11/29/021202sewebex_1.html>

Berry and Mok. "Management Update: Highlights From the 2003 IT Market Compensation Study" Gartner Inc. July 16, 2003.
(Source document provided on attached CD)

Blake, Scott. "Protecting the Network Neighborhood." Security Management Online. 2004.
<http://www.securitymanagement.com/library/000833.html>

Brown, Robert H. "Selecting an Outsourcer: Relationships Are Key to SMBs" Gartner Inc. May 6, 2003.
(Source document provided on attached CD)

Brown and Krammer. "SMB IT Utility Wants and Needs". Gartner Inc. 17 January 2003.
(Source document provided on attached CD)

Brown and Young. "SMB's Show Appetite for IT Outsourcing: How Will Outsourcers Respond?." Gartner Inc. February 13, 2003.
(Source document provided on attached CD)

Butorac, John. Telephone Interview. "Priism Deploy Price Quote." 28 September 2003.

Caballero, Albert. "Systems Management vs Remote Control Software". Crosstec Technical Services. Retrieved on December 18, 2004 from www.crosstech.com.
<http://www.crossteccorp.com/support/resources/SMS%20&%20%20Remote%20Control.pdf>

Carincross, Frances. "The Death of Distance." Harvard Business School Press. Boston, Massachusetts. 1992.

Carr, Charles R. "Managed Services Uncovered: North America." Gartner Inc. July 31, 2002.
(Source document provided on attached CD)

Cartright, David. "How to Plan Your Backup Strategy." ComputerWorld Inc. Retrieved on January 5, 2004 from www.computerworld.com.

<http://www.computerworld.com/securitytopics/security/recovery/story/0.10801,83935,00.html>

CenterRun: One Touch Delivery System. CenterRun Inc. 9 September 2003. **<http://www.centerrun.com/>**

Cottrell, Les. "Passive vs. Active Monitoring." Stanford Linear Accelerator Center. March 11, 2001. <http://www.slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html>

Dash, Juliekha. "Help Desk Outsourcing Rises." Computerworld Magazine. June 26, 2000. Retrieved March 31, 2003 from www.computerworld.com. <http://www.computerworld.com/managementtopics/management/outsourcing/story/0.10801,46290,00.html>

Dickerson, Alan. Telephone Interview. "Vantage Console Manager Price Quote." 1 March 2004.

Eagle, Liam. "Remote Management Places Customers in Control". TheWhir.com. Retrrieved April 2, 2003 from theWhir.com. <http://thewhir.com/features/remote.cfm>

Ecora Reporter. Knowledgestorm. 2004. <http://www.knowledgestorm.com/ActivityServlet?ksAction=optInRes&pos=6&Referer=http%3A%2F%2Fwww.knowledgestorm.com%2Fsearch%2Fbrowse%2F227%2F227.jsp&solId=57561&opt_in_type=I&submit.x=51&submit.y=4&Referer=null>

"Empirix Test Suite." Gartner Inc. Retrieved on May 17, 2003 from www.gartner.com <http://www.gartner.com/gc/webletter/empirix/issue4/index.html>

Empirix Web Application Performance Overview. Empirix. 2004. <http://www.empirix.com/Empirix/Web+Test+Monitoring/Web+Test+Monitor+Overview.html>

Enterprise Backup Solutions. Arkeia. 2004. <http://www.arkeia.com/why.html>

Ethereal. Network Integration Services Inc. February 19, 2004. <http://www.ethereal.com/>

Frisch, Aeleen. "Essential System Administration." O'Reilly and Associates Inc. United States of America. 1995.

Greenhill, Graeme. "Five Steps for Developing a Software Deployment and Management Strategy." NASPA. Retrieved on 12/18/2004 from www.naspa.com. <http://www.naspa.com/PDF/2001/0901%20PDF/T0109004.pdf>

Goodness, Parveen, Kavanaagh, and Phua. "Network and Security Services Generate Revenue Growth in 2002." Gartner Inc. March 21, 2003.
(Source document provided on attached CD)

Houweling, Douglas E. Van. "Support for Decentralized Computers." ACM Press. New York, NY. 1979.

Hyder, Edward. Logical Solutions. "Current Uses of Remote Technology." 5 June 2003.

Info Security. Smartline Inc. 2004.
<http://www.protect-me.com/>

IPSentry Network Monitoring and Alert Software. RGE Inc. 2003.
<http://www.ipsentry.com/>

Jungo: WinDriver Product Line. Jungo Ltd. 2004.
<http://www.jungo.com/windriver.html>

Kempf and Krammer. "Small Business IT Spending and Staffing." Gartner Inc. 11 October 2002.
(Source document provided on attached CD)

LANDesk Client Manager. Network America. Inc. 2004.
<http://www.ldms.com/landesk/mgmtsuite.htm>

Leong, Lydia. "The Battle for the Middle Ground: Low-End Dedicated Web Hosting." Gartner Inc. May 7, 2002.
(Source document provided on attached CD)

Lipkind, Harry. Telephone Interview. "WildPackets Price Quote." November, 3 2003.

McLellan, Laura. "Customer Buying Trends for IT Services in 2002." Gartner Inc. 14 February 2003.
(Source document provided on attached CD)

Middleton, Bruce. "Mapping a Network Security Strategy." ." Security Management Online. 2004.
<http://www.securitymanagement.com/library/000619.html>

Morrison and Slywotzky. "How Digital is your Business." Mercer Management Consulting Inc. New York, New York. 2000.

Managesoft Software Deployment. Managesoft.Corp. 2004
<http://www.managesoft.co.uk/solution/distribution/index.xml>

NetOp Remote Control. CrossTec Corporation. 2003.
<http://www.crossteccorp.com/netopremote/features>

New Boundary Technologies Prism and Radiem Solutions. New Boundary Technologies. 2004.
<http://www.lanovation.com/products/prismdeploy/prismdeploy_info.htm>

"A New Model for Low-Cost, High-Satisfaction End-User Problem Resolution." Intel Networking. Retrieved March 31, 2003 from http://207.36.127.62. <http://207.36.127.62/production/bocacomm/bctchelpdesk-integrated.html>

NetReach Remote Network Management for Wide Area Networks. Western Telematic Inc. 2004. <http://www.wti.com/netreach.htm>

Net Support Manager. NetSupport Limited. 2003. <http://www.netsupportsoftware.com/nsm/netsupport_manager_overview.htm>

Network Administration in the Distributed Enterprise. WildPackets. 2004. <http://www.wildpackets.com/solutions/distributed>

Networking: Wake on LAN Technology. IBM. 2003. <http://www.networking.ibm.com/eji/ejiwake.html>

New Remote Hardware Access and Development Tool. Jungo. April 25 2000. <http://www.jungo.com/ra_news.html>

NovaStor Online Remote Backup Solutions. NovaStor Corporation. 2004. <http://www.online-backup.com/index.asp>

"An Overview of SNMP". Diversified Data Resources Inc. Retrieved on November 12, 2003 from http://web.archive.org <http://web.archive.org/web/20010813014724/www.ddri.com/Doc/SNMP_Overview.html>

"Planning a Remote Backup Solution for your Enterprise." Sun Microsystems. Retrieved December 15, 2003 from www.sun.com. <http://www.sun.com/storage/white-papers/backup-checklist.html>

Quircach, John. Telephone Interview. "Empirix Price Quote." 14 July 2003.

Radview Products and Services. Radview. 2001 <http://www.radview.com/products/Index.asp>

Ranum, Marcus J. "Put your Money Where Your Net Is." Security Management Online. 2004. <http://www.securitymanagement.com/library/000431.html>

R*emote Backup Solutions for Subscription-Based Remote Backup Service Providers.* Remote Backup Systems. 2003. <http://remote-backup.com/>

"Remote PC Wake-Up." IBM. 2003. <http://www.madge.com/_assets/downloads/lsshelp8.0/LSSHelp/AdvFeat/WonLAN/WonLAN2.htm

Remote Support Buyers Guide. IBM. 2003.
<http://www-1.ibm.com/services/its/us/remotebguide.html>

SiteScope. Mercury Interactive Corporation. 2004
<http://www.mercuryinteractive.com/products/sitescope/>

SSH. SSH Communications Security. 2004.
<http://www.ssh.com/company/sales/store/>

"Sun Microsystems Completes Acquisition of Centerrun Inc". Sun News. Retrieved 12/20/03 from www.sun.com.
<http://www.sun.com/smi/Press/sunflash/2003-08/sunflash.20030821.1.html?redirect=false&refurl=http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=centerrun+sun>

Sun Network Management. Sun Microsystems. 2004.
<http://wwws.sun.com/software/product_categories/network_mgmt.html>

Symantec pcAnywhere. Symantec. 2004.
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=2>

"To Host or Not To Host." Resource Index Online. Retrieved November 12, 2003 from http://webhosting.resourceindex.com.
<http://webhosting.resourceindex.com/articles/000017.html>

Underwood, Kim S. "Web Hosting: An Overview." Gartner Inc. November 19, 2002. (Source document provided on attached CD)

Vantage Console Access Technology. Asp Technologies Inc. 2004.
<http://www.asptech.com/>

"Web Hosting for Small Business." Resource Index Online. Retrieved November 12, 2003 from http://webhosting.resourceindex.com.
<http://webhosting.resourceindex.com/articles/000014.html>

Web Performance Testing Tools. Web Performance Inc. 2004
<http://www.webperformanceinc.com/>

Who/What is Sandra? SiSoftware. 2004.
<http://www.sisoftware.net/index.html?dir=&location=pinformation&langx=en&a>

Windows 2000 Terminal Services. Microsoft Corporation. 2004.
<http://www.microsoft.com/windows2000/technologies/terminal/default.asp>

ZDNet: 10/100 PCI ENET ADAPTER WAKE ON LAN. CNET Networks Inc. 2004.
<http://shopper-zdnet.com.com/10_100_PCI_ENET_ADAPTER_WAKE_ON_LAN/4014-3251_15-6704702.html?tag=pl&q=>

ZipToNetX Remote Automatic Backup Software. ZipToNet Ltd. 2004.
<http://ziptonet.com/ziptonetx.html>