How to Implement a Successful Telecommuting Program
Introduction

This white paper is intended for those companies and CIOs with either an existing telecommuter program or those wishing to launch such a program. In the paper, we will highlight current practices and trends, implementation considerations and technical options. The issue of telecommuting has risen significantly due to the increasing pressure on companies to cut costs and increase employee productivity. Companies are now challenged to initiate more flexible thinking for the new “corporate office.” In addition, the expansion of broadband services to employee’s homes has made telecommuting a viable option – and sometimes a requirement – for medium to large-sized businesses in today’s marketplace.

The benefits of expanding access beyond the corporate walls are compelling:

- Reductions in operating expenses
- Better work-life balance for employees
- Increased employee productivity
- Increased quality contact with customers
- A reduction in air pollution for the community

Some typical telecommuter activities include customer/technical support employees tapping into corporate computing resources for troubleshooting, managers connecting after hours to catch up on email and remote (or traveling) employees linking to the corporate office. Businesses have also implemented “flex time” programs, which permit several telecommuting hours per week.

The popularity of telecommuting and remote access programs has surged recently due to the following drivers:

- Corporate cost reductions and desire to achieve employee productivity gains
- Advances in low-cost, high performance access technologies such as xDSL and DOCSIS Cable
- Improvements in information security such as VPNs, digital certificates, firewalls and data encryption algorithms
- Convergence of voice, video and data on a common IP framework

Background

Until recently, companies wanting to provide telecommuting capabilities to their employees were constrained at the “last mile” access point. Their choices were either slow and difficult to support dial-up modem access, or slow and expensive to install frame relay or dedicated access circuits. The cost and speed limitations of these access methods made full-scale telecommuting a challenging proposition.
In the past few years, however, DSL and cable-based broadband technology have matured dramatically. Managed Service Providers have electronically bonded their provisioning systems directly with the RBOC, ILEC and DLEC internal systems so prequalification is more accurate and installation is more streamlined. Cable companies have brought “business class” cable modem service to market and interconnected their last mile service into fiber backbones for improved speed and reliability. Some of the more forward thinking providers are even offering Service Level Agreement (SLA) commitments to their business customers to address uptime, performance and repair.

A number of market and technology trends have emerged to inspire CIOs to replace their decentralized, unmanaged approach to telecommuting with a formal, well defined policy and technology set. CIOs have been forced to “lock down” and centralize all access into the corporate network due to the ever increasing threat of viruses and security attacks. By publishing a formal telecommuting policy with strict rules for accessing the corporate network, many of these threats can be avoided or dramatically diminished. Laptops running encrypted VPN software with automatically updated virus protection and personal firewalls are a practical way to provide the easy access employees require while maintaining centralized management, control, audit trails and security.

**Implementation Considerations**

**Success Factors**

There are a number of success factors to consider when deploying a telecommuting program. Critical technology issues such as security, access, asset management, reliability and support are vital. “Softer” considerations such as insuring employee fairness, maintaining workplace culture, corporate legal protection and trust must also be considered. Successful telecommuting programs require thorough communication, corporate support, technology standardization, well-defined processes, ongoing training and robust implementation tools. A telecommuting program that is well planned, implemented and managed is an effective work option.

After the policies and scope of the program are established, a large number of technology issues must be addressed.

1. Seamless integration with the existing corporate network must be planned and executed to allow access to computing resources
2. Standardized, scalable and supportable equipment must be selected, tested, staged, configured and deployed
3. Appropriate access partners must be chosen to provide safe and reliable network connectivity
4. Information security and public vs. private transport decisions must be made
5. User enrollment, installation, provisioning and support processes must be defined
6. Decisions around firewall configurations, data encryption ciphers, routing protocols, VPN type and hardware/software interoperability must be thoroughly tested, standardized and deployed

However, the most challenging technical hurdle is multi-vendor integration. There are a daunting number of vendors and access technologies that must seamlessly interoperate to provide secure, reliable remote access to corporate computing resources. The following steps are the major milestones and possible fail points:

1. Integrate customer premise equipment (CPE), network equipment, VPN hardware & software, firewalls, operating systems, telco providers, as well as their corresponding release updates, software patches, bug fixes and firmware upgrades
2. Evaluate and test software applications for remote or mobile users for performance over various connectivity and security methods
3. Analyze the technology outsourcing strategy to determine whether it would be better supported internally, or if an outsourced vendor with telecommuting and VPN expertise would be a better option

How to Begin

Implementing a successful telecommuting program requires much more than simply providing a high speed connection and a laptop. There is an enormous amount of planning that must take place to accommodate policies and procedures, technology selection, training, installation, technical support, cost and budget management and user satisfaction.

Begin by carefully planning and documenting the key phases of the project. Build a policies and procedures manual that includes:

- Selection criteria for participation
- Participation requirements & enrollment procedures
- Telecommuter agreement & contract
- Office supply policy
- Home office setup guide
- Administrative support policy
- Mail and overnight package procedures
- Program termination policy
- Training program outline (technology usage, time management, decentralized meetings, cultural issues, etc.)
Planning

Detailed technical and operational planning is critical to the success of any telecommuter program. Poor planning can not only result in frustrated users, but could also compromise business computing resources. The “technology bundle” that telecommuters will use to work remotely includes hardware such as computers, phones, modems and printers as well as software such as operating systems, applications, firewalls, security keys, backup software and diagnosis tools. The heart of the telecommuting technology “bundle” is the VPN or Virtual Private Network. The VPN is comprised of all the hardware and software required to gain authorized access to the corporate network. It can include security tokens, phonebook/dialer software, hardware or software-based data encryption, shared authentication keys and preconfigured “tunnel” paths to authorization servers. Careful consideration must be given to architecting security, designing access methods, establishing hardware and software standards and planning for ongoing upgrades/patches/bug fixes. Companies may seek outsourced vendors and technology partners to assist with the planning, deployment and operation of the project. Select a partner that has a track record of implementing a successful telecommuting program and has outlined best practices procedures to help navigate the myriad of challenges.

Telecommuting technologies are largely transparent to the user, so the ultimate gauge of each telecommuter’s satisfaction is the user experience. Plan for a single, integrated VPN and Dialer graphical user interface (GUI) that makes establishing a secure connection seamless. Maintain the same front end whether the telecommuter is using dial-up, broadband, the office LAN, etc. Be sure the front end is smart enough to present the same look and feel irrespective of access method. It should also include all the firewall, digital certificate, virus protection and other embedded software in the background so the telecommuter does not have to manually launch or configure each individually.

The challenge of balancing supportability and standardization with the economics of leveraging existing equipment is a difficult one. Some sample considerations are:

- Issuing new preconfigured PCs for maximum standardization and minimum support costs vs. reloading existing PCs with new VPN and application software to minimize capital expenditures
- Distributing VPN and application software on CDs or via email for telecommuters to self-install on their existing computers vs. having the IS or help desk staff install all of the software

Successful planning will make provisions to accommodate all of these situations and work to find the proper balance between “standardization & control” and “user satisfaction and budget.”
Implementation & Deployment

The most difficult task of any telecommuting initiative is the implementation and deployment of the solution to the workforce. Typically, one of the most difficult processes is selecting and ordering the appropriate access connection for each telecommuter and managing the installation. After insuring that the telecommuter candidate is approved for the program, the next step involves assessing which technologies are available in the user’s geography, which of those can actually reach the telecommuters home and what bandwidth options are available. Most companies will probably select DSL or cable modem service because of the attractive speed/price offer. However, the actual ordering and installation of the service can be time consuming. Typically, finding the right access method involves searching each phone company, cable company, or other telecommunications provider in each telecommuter’s coverage area to determine availability of service. It becomes quickly apparent that there is not a single source broadband provider that can reach all of the telecommuter locations. The task of matching service providers to telecommuter area and then managing the ordering and installation process can quickly become an unwieldy multi-vendor challenge.

Once the telecommuters have been prequalified for the appropriate type/speed of access, then the next challenge is to coordinate the installation with the telecommuter’s schedule and track its progress (i.e. install dates, circuit install dates, hardware configuration and setup, inside wiring). Some VPN service providers have developed web-based implementation tools to greatly ease the process of finding and “pre-qualifying” broadband access and managing installation and activation.

Managing the uniqueness of home electrical and wiring conditions can impact a successful install. Care must be taken not to damage carpet, wallpaper and furniture while appropriately positioning routers or other hardware.

Maintenance

Supporting and maintaining a group of telecommuters, even with the best training and planning, can be difficult. Questions which would normally arise in the office and would probably be handled by asking a co-worker are now the sole responsibility of technical support. Since telecommuters are usually physically isolated from other workers, their workflow is very dependent on the proper functioning of their “technology bundle,” and responsive technical support. Studies show that telecommuters tend to work longer hours, usually well into the evening when most traditional office workers have gone home. CIOs have the challenge of deciding the window for technical support (i.e. limit to normal business hours or extend the hours). Most telecommuters prefer a centralized, single point of contact support model. Telecommuters then articulate the problem once to a sole contact who then either remedies the issue or draws from additional resources.

A hardware failure can cause a telecommuter to become completely inoperable until a repair can be accommodated. For speed to repair, consider instituting a mandatory data backup policy and if possible, install
automated, unattended backup software on the telecommuter’s PC. Consider keeping a minimum level of “hot spares” (including PCs, cable/DSL modems, routers, VPN appliances, etc.) preconfigured and kept on hand at the help desk for fast shipment to the telecommuter or choose a service provider that offers this type of CPE maintenance. The volume of calls and occasional need to make an “onsite visit” to assist a telecommuter has inspired many companies to outsource this function to either their telecommuting service provider or to a technical support company who has remote field agents. Whether choosing to insource or outsource the support function, it is important to implement adequate troubleshooting tools and repair processes to keep telecommuters productive. Technical support experts should be maintained in the following categories: hardware repair, application software support, telecom & network support and provisioning/install–deinstall. In addition, a well defined escalation path within the in-house IT department and outsourced partners should be provided for a seamless customer service experience.

In addition to “reactive” support to address telecommuter requests for assistance, many CIOs are embracing a proactive management and monitoring philosophy for the VPN network (similar to the way corporate LAN and WAN networks are managed.) To minimize outages and telecommuter problems, plan to extend WAN management tools to monitor the endpoints of the telecommuter broadband connections and measure uptime and performance. Some VPN service providers offer portals into their management systems so the VPN endpoints (and corresponding SLAs) can be monitored. Deploying the VPN service to the telecommuter community is just part of the process. Depending on the complexity of the VPN, there are numerous hardware, software and firmware components provided by vendors that continually release upgrades, patches, fixes and enhancements. Each discrete vendor upgrade/patch release must be evaluated on its own merits and then evaluated within the interoperability context of the “technology bundle.” This is the only way to insure that the telecommuter will successfully connect to the resources he or she requires. VPN Service Providers that offer CPE Management will maintain records of each user’s hardware, firmware and configuration. They will automatically provide these upgrades/patches transparent to the end-user.

**Technical Considerations**

A comprehensive telecommuting program strategy includes a technical architecture that is well planned and evaluated within the context of a company’s existing LAN and WAN environment. The goal is to create the optimum technical design that:

- Leverages the existing network infrastructure
- Creates a seamless “extension of the LAN” to telecommuters
- Minimizes security risks
- Establishes a framework for adding additional services like voice over IP and video
- Maximizes supportability via use of industry standards
Network Design

One of the first considerations is to select the type of remote access technology. The choices range from slow, cumbersome dial-up to expensive dedicated private circuits. For most telecommuting programs however, the best choice is a VPN which uses fast, inexpensive broadband over the public Internet. This is often supplemented with dial-up VPNs over the public Internet for those times when the telecommuter is “mobile.” Alternatively, for extremely sensitive data, a network provider that can offer a “private” IP environment may be considered. Typically these providers have interconnected their backbone privately with “last mile” broadband providers and can keep the telecommuting traffic off the public Internet and on their private links. This is generally more expensive than using data encryption and the public Internet for transport.

For telecommuters, there are two main VPN technology models to choose from regardless of whether using the public Internet or private transport for connectivity: IP-Security (“IPSec”) or Secure Socket Layer (“SSL”). In an IPSec model, a secure, encrypted datapath is set up between the user and the host server, typically a VPN concentrator. In an SSL model, the security and encryption is incorporated into the web browser, such as Microsoft Internet Explorer or Netscape Navigator. Therefore SSL-based VPNs only provide access to web-enabled applications such as email or file sharing. Applications that require client software, such as ERP or CRM systems, are therefore relegated to IPSec VPNs. In recent months, however, some vendors have released “client-based” versions of their SSL VPN offering, in which users launch an “application window” to run non-web-enabled applications. In either model, the telecommuter’s traffic is “encrypted and tunneled” to a corporate security device (VPN concentrator) where it is validated and “de-crypted” through the corporate firewall into the corporate network.

For IPSec VPNs, the next decision is to determine how the VPN sessions will originate. Specifically, the decision must be made between software-based VPN technology and a hardware-based VPN appliance. In the software-based model, only the traffic coming to and from the telecommuter’s PC is encrypted in VPN tunnels, while in the hardware-based model all traffic going through the appliance is encrypted. An important factor in determining the best model is understanding and accommodating other Internet traffic from inside the telecommuter’s residence. If the telecommuter has other PCs that access the Internet from the broadband connection or lives with another telecommuter working for a different company, then the best course is to utilize a software-based VPN loaded on the telecommuter’s “business PC.” While hardware VPN devices can be configured to only tunnel traffic originating from specific PCs on the telecommuter’s “home network” and user authentication is required to access corporate resources, many companies feel more comfortable establishing the VPN session directly from the telecommuter’s PC. If firewall or antivirus software is tampered with, the session will automatically be disconnected.
**Hardware Requirements**

Regardless of which VPN model is chosen, hardware exists to be managed. In addition to the hardware PC, there must be CPE equipment to terminate the DSL, cable, ISDN, or other broadband connection. In some cases, this is simply a modem that connects the broadband service to the telecommuter’s PC, while in other cases it could be a combination of equipment including a router, hub, wireless access point, firewall, or VPN appliance. Like most large scale technology deployments, standardization is critical to maintaining adequate support levels. Driving standardization becomes a difficult challenge, because typically, each of the disparate “last mile providers” will have their own CPE standards which may or may not match others. In the DSL or cable provider world, each provider (BellSouth, Verizon, Cox, RoadRunner, et al) has deployed their own broadband network equipment and selected CPE that is compatible with them. From a support perspective, managing all the different CPE devices and understanding their configuration utilities to set up filters, firewalls, access lists and provide upgrades can be a challenging proposition. Moreover, if VPN appliances, wireless access points, or hubs to connect multiple PCs are deployed, the telecommuter can quickly amass a stack of equipment complete with patch cords, power supplies, etc. that could result in an unsafe, unreliable, or overheated environment.

**Options for Internet Access**

*Dial-up Access:*
Although dial does not provide much bandwidth; it is widely available and very straightforward. Dial can provide centralized network access to the corporate LAN or WAN via internally managed modem banks or RAS servers. However, it can have expensive per minute charges for users outside the local calling area. Alternately, purchase plans are available from a National Dial Provider with thousands of local numbers.

*xDSL Access:*
(Digital Subscriber Line) is a proven technology utilizing existing telephone lines to provide high bandwidth access. DSL is a distance sensitive service with speeds relative to endpoint distance from the central office housing the DSLAM. Not every local phone company’s central office has the proper equipment, so the service is not universally accessible. However, DSL is widely available in larger cities. Generally DSL can provide speeds equal or better than traditional 1.5mb T1 service when the telecommuter’s home is within a mile or so of the central office. This speed drops proportionally as distance from the central office increases. Generally access becomes unavailable beyond 18 to 20 thousand feet. There are multiple types of DSL, with the three most common being Asymmetrical (ADSL) which provides fast download speed and slower upload speed and is generally priced below $100/mo. Symmetrical (SDSL) provides equal upload and download speeds. IDSL can run greater distances than ADSL or SDSL, but it only has a maximum speed of 144k. Generally, less expensive ADSL is most suited for telecommuters while higher performance SDSL is better suited for small office and multi-user VPNs. There are other, far less available forms of DSL including G.Line, S/HDSL and
VDSL that promise faster speeds and greater distances. These technologies have not yet been embraced by the market and are not generally available.

*Cable Modem:*
In the past few years, cable companies have spent millions upgrading the high-speed access services to be more “business class.” They have laid fiber and optimized routing and network technologies so that individual user speeds are not as impacted by other users like they once were.

**Security**
In addition to IPSec and SSL-based VPN encryption, there are additional security considerations to evaluate when deploying a telecommuter program. Review internal security policies to insure that they extend to the telecommuting workforce. Realize there are multiple levels of a sound security methodology including physical security, access security and data security.

**Value-added Applications**
When deploying a telecommuting program it is important to plan ahead and attempt to “future-proof” the investment. Select standards-based technologies and build an open framework to support additional IP services and tools as they become relevant. Consider an inexpensive dial backup strategy for those rare times when the broadband connection is unavailable. This could be an automated “dial failover” that initiates a dial VPN session from the CPE if the primary link goes down, or it could be a simple process of training users to use their manual dial-up VPN capabilities if the broadband becomes unavailable.

Over time, telecommuters will request enhancements and productivity tools, such as voice/video/data convergence and unified data communications. They will inevitably begin to use tools such as Instant Messaging. CIOs will need to make decisions regarding the safety and security of using these applications. To improve communications with other telecommuter and employees in traditional offices, consider online collaboration tools, web-based “presentation rooms,” and even desktop video conferencing. IP Telephony can be an extremely effective means of eliminating long distance phone calls between the telecommuter and headquarters and extending office PBX functionality to the home. High-speed broadband connections and secured VPNs make webcams and online meetings a viable option. Telecommuters are going to request these value-added applications, so CIOs must think ahead and communicate a technology roadmap. By articulating the plans for improved and expanded services, telecommuters will be less inclined to “do it themselves” and increase the support burden. Moreover, a well articulated plan will make for more satisfied telecommuters and create volunteers to help pilot new and innovative ideas.
Buy vs. Build

As with most IT projects, a telecommuting initiative should go through a build vs. buy analysis to determine the best course of action. Key to this decision is the CIO’s methodology for using internal staff. Often, CIOs prefer to utilize their internal resources to deliver applications and technologies that create a competitive advantage. They may select to outsource infrastructure and communication services to providers who can offer best practices, economies of scale and a track record of success. Managing the myriad of last mile vendors, coordinating circuit installation, configuring and deploying equipment, maintaining CPE replacement inventories, deploying performance monitoring tools, managing security, fielding user support calls and creating associated training can be daunting tasks. Partnering with a provider who has successfully implemented other telecommuter programs and has existing relationships with last mile providers, equipment vendors and field service resources can often reduce project risks and speed deployment. Working with a provider can also help quantify and guarantee service levels and deployment costs. Often, providers can help CIOs better manage costs by reducing the upfront capital expenditure costs and integrating all elements into a user-based, variable cost model for more control.

A decision to engage a VPN Service Provider should be made with care. Interview multiple providers and their existing accounts. Make sure that the provider can provide an automated broadband VPN provisioning, monitoring and management. Be sure the provider is more than a broadband aggregator and actually operates an IP Backbone and a 24x7 Network Operation Center. They should also offer flexible options for growth, including site-to-site VPNs, Internet access and security services. Be sure that the provider has strong SLAs with clear metrics and financial penalties. These SLAs should cover more than simply network availability, but should also address individual customer circuit performance, provisioning times, problem notification/resolution and web-based reporting.

Conclusion

Regardless of whether implementing a telecommuting initiative with internal resources or an outsourced partner, the core components of a successful project remain the same. Clear communication and training, proper expectation setting, reliable technology and passionate project leaders are paramount to achieving the mission. With the right planning and consideration of the issues outlined above, you can ensure that your telecommuting program is a success.