Autodesk University 2007

Enabling a Remote Workforce

Mark Harris – Patton, Harris, Rust and Associates

CM405-1 Supporting employees who want to work from any geographic location is becoming a mission-critical requirement. Accommodating employee relocations, utilizing lower-cost labor markets, supporting production teams in remote locations, tapping talent outside of traditional markets, and satisfying federal and state requirements for telecommuting are all fast becoming high priorities. This session details remote working (telecommuting) issues and identifies solutions that fit different end-user requirements; highlights different technologies that can be utilized; and looks at issues such as security, file management, IT infrastructure, WAN performance, and workload management.

About the Speaker:

Mark currently works as an IT support specialist for Patton, Harris, Rust, and Associates (PHR+A), an engineering firm in the mid-Atlantic region. After more than 8 years of working extensively with CAD applications in land development, he moved into the IT field and has been developing and maintaining infrastructure, messaging, and help-desk solutions, and providing software and hardware management and supplemental CAD training. Mark earned an undergraduate degree in Construction Management from Coventry University in England, and a Masters degree in Information Technology from Virginia Tech. He is also a Microsoft Certified Systems Engineer.

mark.harris@phra.com

Autodesk®

Autodesk
University
2007

Autodesk University 2007

Introduction

Today we are going to look at remote access, the benefits that can be gained from its implementation, issues such as policies and procedures that should be in place before implementation, the technologies used for implementation, and how remote access can be integrated with CAD production. Setting up remote access encompasses many different areas that cannot all be covered in detail during this session. Many of the ideas put forward have accompanying resources that can be found on the Web and also the AU Web site. This document has links to definitions that will help expand on areas that cannot be covered fully during the 90 minutes we have to discuss this topic at AU.

Why Implement a Remote Workforce

The goal of remote access is to make data available to an individual to complete their job from any location. That location may be determined by a more suitable work environment or the need to have the data available in a different location to complete a specific task. With making data available to any location goes the responsibility of being able to manage the data correctly.

The AEC industry has perfect tasks for utilizing mobile data such as uploading and downloading data collectors or machine graders in the field. Through developing technologies such as PDAs, mobile computers, and tablet PCs, mobile data can be used to review plans in the field and to make real-time collaborative changes.

Five common areas that make use of remote access solutions are telework, traveling employees, field crews, data redundancy and disaster protection, and work sharing.

Telework

Some of the benefits of telework include accommodating employee relocations, utilizing cheaper labor markets, increasing productivity, providing an incentive for new hires, reducing greenhouse gasses through reduced transportation needs, allowing for a better quality of life for employees, and reducing real estate overhead.

Traveling Employees

Employees often have to travel away from the office for meetings, field inspections, or collaboration with other employees or partners. Providing remote access to data will improve communications while away from the office.

Field Crews

Most survey crews need to travel to an office to upload and download data. This can increase travel time and fuel costs and make the crews less productive. Making the necessary data available for field crews to complete their jobs from any location eliminates these issues. Quality control can also be improved because data can be transferred to a location where more resources are available to perform cross-checks and quality control.

Redundancy/Fault Tolerance

In the event that a wide area connection fails, remote access solutions can be implemented as a backup system for the primary connection. This can be in the form of a backup router connected to an alternate Internet connection that routes traffic through a VPN.

Having a central data store makes remote access solutions easier to manage. This often means data consolidation considerations in tandem with remote access solutions. Consolidated data lends itself more readily to fault tolerance solutions such as real-time backups.

Remote access solutions can also be used for quick deployments for new and small offices. There are often long lead times for the deployment of WAN circuits that are going to be the primary circuit related to hardware purchases and circuit orders through providers. Temporary WAN links can be established through services and hardware that can be procured more quickly but do not necessarily provide the same fault tolerance or bandwidth of the final solution.

Work Sharing

Infrastructure models for remote access can be used to help work sharing within a company network. This includes data consolidation and remote desktop solutions minimizing the need to move large data sets across slow WAN links where projects teams are located in different geographic areas.

Telework

Telework is slightly different from other types of remote access because of the associated policies related to its implementation, possible changes to work methodologies, and choosing suitable employees to undertake telework.

The terms “telework,” “telecommuting,” “flexible workplace,” “remote work,” “virtual work,” and “mobile work” are all used to refer to work done outside of the traditional on-site work environment. These terms are defined in different ways and used in different contexts to refer to anything from jobs that are completely “virtual” or “mobile” to arrangements that enable employees to work from home a few days per week or per month.

Telework is often a situation in which an employee regularly performs officially assigned duties at home or other work sites geographically convenient to the residence of the employee.

Telework arrangements can be broken into three categories:

1. Regular/recurring at least 3 days per week
2. 1 or 2 days per week
3. Less often than once a week, but at least once a month

The following situations are not considered telework:

• Work extension—Employees taking work home with them to work on outside regular work hours.

• Mobile work—Employees who by the general nature of their job travel away from the main work site, possibly working out of their home on occasion.

Benefits of Telework

Following are some of the benefits of implementing a telework program:

- Cost savings: Reduced office space and real estate costs and intangible savings through employee retention or tapping into cheaper labor markets can lead to saving money.
- Increased productivity: Productivity gains of 10%–40% can be realized. Travel time and elimination of office interruptions are factors that boost productivity.

- Employee/skills retention: Employees who may be leaving because of relocation—for example, a change of job by another family member—can remain employed.
- Improved motivation: The extra trust and confidence that is shown toward a telework employee can help motivate and create independent working styles.
- Flexible staffing: Contract workers can be taken on without having to provide office space or hardware.
- Business continuity: Work can continue in the event of external disruptions such as natural disasters, inclement weather conditions, infrastructure disruptions, or terrorist attacks.
- Reduced travel time and costs: This is usually one of the primary motivators to implement a telework plan. Employees' quality of life is improved through reduced travel time, employees are less stressed when they start the work day, and there is the benefit of reduced pollution from vehicle exhaust fumes.
- Social benefits: Employees can spend more time with their families and be involved with community activities.

Other benefits include reduced absence, organizational flexibility, enhanced customer service, extended work hours, and access to work for people with disabilities.

Right-Kind of Business Model

For telework to be viable the business model needs to be able to support the telework environment. Traditional business models tend to rely on managers distributing work on a daily or hourly basis; employees have dedicated work spaces and may be supplied tasks based on hard copy markups. Office resources such as large format printing and copying are used to develop check plots that are routed for checking and further design work.

A business model that relies on independent workers and digital work flows must be adopted to be able to make telework an achievable goal. This usually is not the case with a traditional business model. Using tools such as Design Review help the routing and collaboration of information to remote workers.

Suitable Work for a Teleworker

The type of work that is being undertaken must be suitable for a telework. It is not practical to have a draftsperson working from home full time who needs supervision and works from hard copy markups.

Elimination of hardcopy redlines and markups help accommodate the teleworker. This in turn should improve overall efficiency and effectiveness of other areas such as office-to-office communication and outside collaboration on projects.

To determine if an employee's job can be performed remotely, break their work into tasks with time allocations. Then derive benefits from doing the tasks away from the office or at least identify tasks that can be done away from the office. The data used for this type of analysis can be taken from time sheets and completed tasks lists.

Not all employees are suitable candidates for telework. The following personal characteristics can help you evaluate if an employee is a candidate for telework.

Characteristics of a person suitable for telework include the following:

- Adaptive
- Excellent manager of information
- A team player
- A specialist critical to the organization
- An excellent communicator with managers, co-workers, and customers that will enable a relatively seamless transition from on-site to off-site
- Able to work independently without close supervision
- Comfortable with the technologies
- Has a telework office conducive to a good work environment
- Has dependent care (i.e., child care, elder care, etc.) arrangements in place.
- Flexible about the telework arrangement and can respond to the needs of the manager, the workgroup, and the workload.

Characteristics of a person not suitable for telework include:

- Not trustworthy
- Takes advantage of privilege
- Excessive Web surfing
- Bad home environment
- Motivation through watching/competing with colleagues
- Poor communicator
- Not a technologist
- Cannot balance work and play

Usually telework is seen as a privilege. It requires the employee to have a strict job description, tenure, and performance criteria.

Home Safety

Ergonomically Correct Workstation

An ergonomically correct working area is important no matter where work is being conducted. Good ergonomics help reduce the risk of both short- and long-term injuries.

Home Free of Hazardous Materials and Is a Safe Work Environment

A home office should follow the same safety standards as a business office. Guidelines by OSHA for home office environments can be found on the OSHA Web site.

Report Work-Related Incidents

Any work-related injuries should be reported to human resources, even if they occur in a home office.

Requirements for Federal Agencies

In 2000 a legislative mandate was established for telework within federal agencies. Further legislation regarding telework was passed in January 2004 and December 2004. The implementation of telework in the federal sector also ties into the requirement for the continuity of operations required by federal agencies, which requires the government to provide support in the event of events such as natural disaster, terrorist attack, or pandemic health crisis.

Telework Policies

Policies and agreements need to be established for remote users. Policies should outline work hours, eligibility, resources, workspace requirements, office supplies, liability, and methods of coordination and communication. An agreement should be signed by the supervisor and employee agreeing to the policy and outlining items, such as the following:

- Location of the telework office (e.g., home, telework center, other)
- Equipment inventory—what the employee is supplying; what the organization is providing; and, if applicable, what the telework center is providing
- In general, the job tasks to be performed while teleworking
- Telework schedule
- Telework contact information (e.g., the phone number to use on the telework day)
- Safety checklist—certifying the home office meets certain standards
- Technical support hours and who provides technical support
- Responsibilities for replacing broken equipment

Scale of Implementation

Identifying the scale of a solution will help determine the right type of solution. The scale of implementation can be broken into three different categories: single user/mobile user, small office, and failover for larger offices.

Single User/Mobile User

Single user/mobile user refers to one person making a dedicated connection to the network. The connection point and technology will vary greatly and may include connections from homes, hotel rooms, public kiosks, telework centers, or laptops with dialup broadband connections. The bandwidth is usually variable and unknown. The connection may be unreliable and the access point may be unsecured. These are usually the most difficult type of connections to support because there are so many variables involved. There is also the "user factor" involved, where you may not have access to the remote hardware and have to troubleshoot issues with someone with limited or no technical knowledge.

Small Office

The small office connection is a point-to-point connection setup to allow one or more users to access data between two networks. The connection will usually be created with either a hardware or software VPN tunnel. The connection technology used at the remote site may be unreliable and may not have any service level agreements. Both end points can usually be secured and once set up are usually stable and easy to troubleshoot.

Failover for Larger Offices

A failover for larger offices is a similar setup to small offices but is only used as a backup in the event that the main WAN link fails. The connection usually will run over a cheaper circuit or a service that can brought online quickly and easily.

Scope of Implementation

When looking at accessing data or being able to work remotely it is important to look at the scope of the type of data or work that is required. This will determine the type of solution that will meet your needs. Outlined below are common scopes.

Communication Only

Communication via email, instant messaging, FTP, or phone may be all that is required for someone to complete the majority of their work or help keep them in the informed while away from the office.

Administration/Management

Tasks such as basic word processing or spreadsheet manipulation may be all that is required in addition to the communication methods outlined above. This usually means small file sizes with low bandwidth requirements for data transfer. Work can be performed on a mid-range workstation.

CAD Production

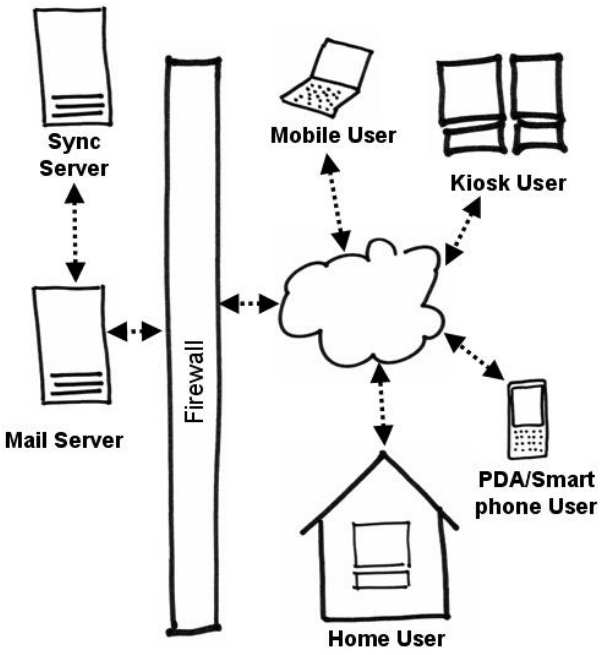
Large file sizes and data transfers may be required for CAD production. A high-end workstation set up either locally or at the remote site with adequate RAM and processing power is needed to manipulate data.

Employees requesting any type of remote access should be required to complete a questionnaire outlining their needs. This will determine the scope of the individual deployment.

Solutions

Communication

Email access, text messaging, and instant messaging can be accessed through a mobile device such as a Blackberry or smart phone. Additional features can be added such as calendar and contacts synchronization. This can be done through services such as Wireless Sync or BB Enterprise Server. Web access to company mail systems provide remote access to messages, contacts, and schedules. An example is Outlook Web Access. Smaller companies may also use free services such as Gmail for messaging which also has the advantage of access from anywhere or any computer. Remote users should also have access to voice communication, which can be provided through landline phones, mobile phones, or IP telephones.



Communication connections

Access to Files and Network Resources

Some applications and data can be published to the Internet and then accessed securely through a Web browser. An example is a Web-based accounting system. Not all applications will work this way, so

access to the network or the network files must be allowed by some means. This can be done by either allowing access into the network through the firewall or placing the required resources outside the network.

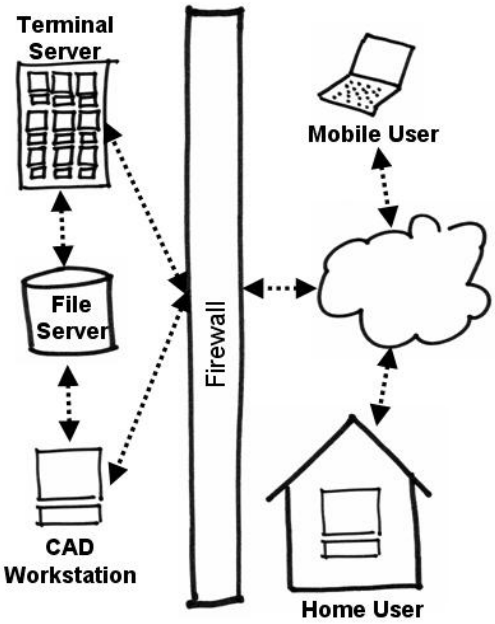
The most common way of allowing access into the network is through a Virtual Private Network (VPN). A VPN creates a secure virtual tunnel over an untrusted network such as the Internet, allowing a connection into a secure network to access data, connect to a mail server, or connect to a remote workstation. When files are small, they can be opened directly from a remote workstation.

Data can also be stored outside of a network for external access. For example, project files can be posted to a third-party project collaboration site like Buzzsaw so outside parties can download, review, and collaborate on projects. FTP sites are also an easy way to make data available outside the network. User login credentials can be established making specific data available for certain users. Logins can be protected with passwords. One issue with posting data to an outside location is that information is being duplicated, leading to multiple file versions that become difficult to consolidate and track. When possible, having a single data source is the best approach.

Access to Applications and Large Data Sets

When files get large (more than 3 MB) it becomes impractical to open or copy files over a relatively slow connection. To work around this issue a remote session that controls either a terminal session or a computer that is local to the network, allowing files to remain on the local network, can be utilized. Small amounts of screen refresh data are then passed over the connection back to the remote user. Application maintenance, licensing restrictions, and workstation processing power may also be contributing factors that require resources to be kept on the local network and be accessed remotely.

Other technologies such as data replication and application streaming such as Microsoft's Softgrid can also be solutions to the small pipe issue. However, these usually lead to higher maintenance overhead, especially if they are being used for individual remote connections.



Remote Desktop Connection via VPN

Scale and Complexity

The scale and complexity of a remote access implementation will depend on the following factors:

- Number of users: Small numbers of remote users are easier to manage from an IT standpoint, but economies of scale may not be realized if expensive equipment is required. Supporting large numbers of users may require dedicated staff to manage and assist the remote user pool.
- Budget: Initial investment and ongoing support costs may limit the scale of remote user deployments
- Method of communication
- Required scope
    - Communications only

    - Administration/management tasks
    - CAD production
- Mobile or immobile connections

Data Management

Data management becomes paramount with a remote workforce. Instead of having a single location for data storage, you introduce the potential of hundreds of locations where data can be stored. This can lead to problems with duplicate data, file security, and backups. If possible, having a central file store that users can access and work on files in a single location rather than copy or move to an alternate location will help alleviate these problems. If data has to be moved or copied to alternate locations, a check in/check out system can be implemented. Features such as Windows Offline Files utility can also be used to help synchronize files.

In some situations unsynchronized data transfers are acceptable and FTP and email attachments can be used. This is useful for data that is not used concurrently with other employees.

Data consolidation can be achieved by having a large WAN pipe with local area network speeds, WAN acceleration, or data replication and synchronization. At this time having a WAN with local area speeds, if it is even available, it usually cost prohibitive. Emerging technologies such as WiMAX and fiber connections will make this an affordable reality in the future. WAN acceleration takes existing bandwidth and uses caching through some kind of appliance at ether end of the connection to reduce the amount of data that is required to be passed over the pipe. An example of this would be a Riverbed appliance. Data replication ensures that local copies of data are identical throughout the network. Bit-level replication helps reduce bandwidth consumption. Examples of this include Availl and Microsoft DFS.

All these technologies can either help consolidate data to a single location where remote users can access or can be used to share data with a remote site.

Implementation Costs

Implementation costs can be analyzed by breaking down cost per user. In some cases a per-user cost will be lower the more users you have working remotely. Cost for enabling remote users can be summarized as follows:

Initial Setup

Initial setup costs include the initial hardware and software. In some cases initial per user cost becomes lower as more users take part in remote access. For example, distributing the cost of a router across more users provides a better ROI. Other costs, such as personal equipment for each user, do not realize any economies of scale.

Maintenance

Ongoing maintenance and technical support need to be considered when looking at the cost of implementing a remote workforce. On average you can expect 2–5 hours per month of support time per user depending on the type of remote access that is implemented after the initial set up period.

Depending on the model used two sets of hardware, one at the remote site and one at the local site, need to be maintained. Maintenance includes patching, updating, and resolving hardware issues.

Overhead

Overhead costs include the following:

- Additional bandwidth required at the host site for remote access connections.
- Service provider fees if you are using a third-party solution for remote connections.
- Broadband connection fees for remote site if this is part of your policy.
- Additional data and hardware maintenance plans with wireless carriers.

Hardware Resources

To ensure that the correct hardware is supplied, a scope needs to be established. This will determine the required resources to meet the required objective.

Remote Hardware

Hardware for the remote user will need to be supplied or you will need to make use of equipment that the home user already has. It is important to establish a policy for who is responsible for the equipment that is located off site and how it will be serviced. If personal equipment is used, then it will need to meet the minimal hardware requirements for the connection being used. Utilizing personal home PCs for remote work is only recommended if the system will not be connecting directly into the main network. Personal PCs should be considered untrusted and should be kept off any internal networks. In the event that personal PCs are used, customized setup and configuration should be kept to a minimum. Web services for mail and external file sharing such as FTP should be utilized as much as possible. Be aware that some home use license agreements do not allow business licensed software to be installed on personal PCs.

Supplying a remote worker with a virtualized workstation is also an option if the employee's personal hardware is to be used. Virtual workstations can be run from DVDs, solid state memory, or external hard drives. By using a virtual workstation, untrusted hardware can be made trusted.

Providing hardware to remote users is often the best solution. A feeling of separation between personal and business use is created. Systems can be configured so that minimal personal activities can be performed on the system. Locking the system down with permissions, policies, and security applications will deter non-business use. Hardware supplied to a remote location not set up by a qualified IT support person should be accompanied with detailed setup instructions.

Depending on the remote access model being implemented hardware may vary.

Downstreamed older system can be used as remote terminals connecting back into the main network at minimal cost. A downstreamed system can be defined as workstation that is no longer considered production class and will be relegated to administrative tasks.

Additional home hardware may include routers/firewalls, modems, cables, keyboards, mice, printers, backup power supplies, and CD/DVD writers.

Any equipment installed outside of the office should have property labels and should be inventoried.

Employees who travel away from the office for mobile work may require a laptop that is capable of either administrative tasks or CAD tasks, depending on the role of the employee.

Local Hardware

In addition to remote resources, local hardware may also need to be procured. This may include routers, servers, an upgraded firewall, additional bandwidth, and hardware and software for data consolidation.

Remote Desktop Solutions

Two different options are available for connecting your remote users to your network for accessing remote desktop sessions: third party applications and in-house solutions.

Third-Party Applications

A number of third-party solutions will allow connections to a desktop inside a company's network from the Internet. The technology relies on a client being installed on the host PC that then connects to a third-party server outside the corporate network. A client PC is then routed through the third-party Web site to the host workstation. Two of the many companies who supply these third-party solutions are Symantec(PC Anywhere), and Citrix (GoToMyPC). Drawbacks of third-party solutions include data being passed through someone else's network, possible buyout or merger issues that may orphan the application, ongoing subscription fees, and possible security issues from poorly developed or unpatched software. Benefits of third-party solutions include easy deployment, multiple levels of administrator management, access to host workstations from any computer with Web access, and the ability to lock down file access to the internal network.

In-House Solutions

In-house solutions comprise creating a connection to internal workstation via a VPN tunnel. Once the VPN connection is established host computers can be accessed using applications such as Remote Desktop, Net Meeting, or VNC. Drawbacks of in-house solutions include higher administration time, more help desk support needed, connections from secure workstations only, and possible higher initial equipment costs for providing home PCs. Advantages include custom security, solution is owned wholly by the organization, and data are kept 100% in house.

Broadband Technologies

There are a range of different technologies available to connected remote users to your network. The availability of the different services and the types of technology are changing rapidly. The type of broadband connection used may be determined by the service availability. Service reliability, customer support, and pricing plans also need to be taken into consideration. Other requirements such as the availability of fixed IP addresses and connection mobility may determine the technology used. Broadband connections are the biggest bottleneck for remote access. Speeds in the United States are still too slow, limited, and costly to allow for direct access to network resources and have LAN speed performance. Following is a summary of the most common technologies that are available and their connection speeds.

Technology	Connection Speed (Download/Upload)
FiOS	2–50 Mbps/2–5 Mbps
DSL	256 Kbps/128 Kbps
VDSL	1.5 Mbps–6 Mbps/1 Mbps–1.5 Mbps
Cable	2 Mbps–16 Mbps/384 Kbps–2 Mbps
EDVO(Rev A)	1 Mbps
WiMAX	10–100 Mbps
Satellite	10 Mbps
ISDN	128 Kbps
POTS modems	28–56 Kbps

Actual speeds can be tested using online tools such as ones provided by DSLReports.

General Technology Issues

Ongoing support and maintenance will always be a factor no matter what technology is employed for remote access solutions. Software will need to be patched and upgraded, remote workstations will fail, and smart phones will lock up and loose data. As with all technologies, especially emerging ones, bugs and instability can be expected. Technologies are also changing continuously and solutions that are deployed today may not be right for an organization in 18 months. R&D should be the first step taken when deploying a new technology solution. Thorough testing through beta deployments and rollouts should be conducted. Realistic milestone should be established and followed for R&D of new technologies and solutions.

Remote access solutions rely on many different technologies. Different pieces of the remote access solution puzzle evolve at different rates. Weeding out fads and spotting disruptive technologies will help develop better long-term and sustainable solutions. Reducing the number of components will help reduce points of failure. Potential bottlenecks and points of failure need to be identified before they become an issue. Technology used for remote access needs to be as seamless and transparent as possible to the end user.

Troubleshooting

Outlined below are areas that can cause issues when connecting. Each item should be checked when trouble shooting a connection issue.

- Routing
- Name resolution
- Security settings (e.g., group policies and membership)
- Firewall settings
- Physical hardware setup (e.g., cables into the wrong ports)
- Internet connectivity
- Proxy servers
- Expired certificates
- Other security measure such as RSA, group memberships, and account permissions

Security

Security is an extremely important topic when dealing with remote access to a network. Opening up a network to outside communication increases the risk of virus attacks, data theft, data loss, unauthorized access, DOS attacks, infiltration by malware, and other attacks.

A good resource for security issues related to remote access and telework is the Security for Telecommuting and Broadband Communications, Recommendations of the National Institute of Standards and Technology, Special Publication 800-46. The document "assists organizations in addressing security issues by providing recommendations on securing a variety of applications, protocols, and networking architectures."

The main recommendations for securing networks include the following:

- All home networks connected to the Internet via a broadband connection should have some firewall device installed.
- Web browsers should be configured to limit vulnerability to intrusion.
- Operating system configuration options should be selected to increase security.
- Selection of wireless and other home networking technologies should be in accordance with security goals.
- Telecommuting users should be guided on selecting appropriate technologies, software, and tools that are consistent with network and security policies.

An organization should have a security policy in place that outlines data ownership, expectations of privacy, monitoring, messaging restrictions, acceptable uses of email and the Internet, and software and hardware restrictions.

Protecting Remote Systems

Steps need to be taken to ensure that remote system are maintained. These include:

Backups

If data are being moved off site, then there must be a method to provide backups. This can be done with DVDs or CDs or USB mass storage, either solid state or hard drive.

UPS

A backup power supply to prevent data loss in the event of a power failure should be installed. This also protects equipment for power surges and brown outs.

Software

Patches and software updates need to be applied to remote systems. Virus definitions need to be updated, and firewalls may need to be reconfigured. Using WSUS in a Microsoft environment is a simple way to ensure Windows updates are applied.

Hardware

Hardware needs to be located where it will not be damaged or tampered with. Home environment conditions should be equal or better than office environments. Contact with dust, extreme temperatures, pets, and children should be avoided. Mobile hardware such as laptops are more susceptible to damage and theft.

Redundant Connections

Redundant connections must be compatible with the gateway. If you use dialup for backup connections, a RAS server with dialup capabilities must be available. Redundancy must enable a remote user to still be able to communicate effectively if the primary method of

connection/communication fails. This can be as simple as ensuring that a remote user has a cell phone in addition to a landline.

Guidelines need to be established for who is responsible for protecting the system. Hardware, software, and broadband connections provided by the company remain the responsibility of the company. Systems owned by the end user may lead to ownership issues. This should be addressed with policies and guidelines that are developed for remote workers. A good philosophy is that work for the company should be performed on a system owned and maintained by the organization.

Remote Access and CAD

Licensing

The Autodesk EULA allows for the installation of a second seat of AutoCAD to be installed on a second computer for use while working away from usual work locations. Use of the second seat cannot be concurrent. The installation must also be on a system owned or leased by the license owner and so cannot be installed on an employee's personally owned computer. Network licenses can be pulled over a VPN tunnel to the remote workstation. Licenses can be checked out if the remote connection is unreliable.

Because there are licensing limitations to running Autodesk products on a terminal server (only two sessions can be run at one time) an alternate solution is required to allow remote users to connect to a network and access a copy of an Autodesk product. This can be done by either having a physical workstation located in the office the remote user can connect to or a virtualized system using products such as VMWare or Microsoft Virtual PC. Virtualized products can be then run inside a terminal server. Licensing for the operating system also needs to be taken into consideration to ensure that there is a similar home use agreement. If not, additional licenses will need to be acquired.

File Size and Data Management Issues

Autodesk project files can be complex, with cross-referenced drawings, embedded images, associated project files and databases. Moving all project data back and forth between two systems is usually impractical and leads to file version issues. Keeping the data in a single location is always preferred. Tunneling into the network and working on the data using local resources through a remote terminal session is the best approach for remote users. Data transfers across the WAN are minimized, the ability to work in real time with other team members is possible, and duplicate files and versioning issues are avoided.

Remote Connection and Screen Lag

One of the drawbacks with using AutoCAD through a remote session is that there is a screen lag in the main drawing area. This is caused by the screen image being converted to bitmap data and then transferred across the network. Screen lag can be diminished by using good practices such as minimizing panning and zooming by utilizing saved views and good layer management and only displaying data that are relevant to the current work session.

Summary

There are many benefits to implementing access for remote users. Implementations should take into consideration the scale and scope of the deployment so that the correct resources can be procured and

rolled out. Data management is an important issue and methods of data consolidation or replication should be explored. These solutions will also aid the coordination of data for non-remote users and users dispersed across multiple office locations. Remote desktop solutions help keep data local and reduce the amount of traffic on WAN links. There are many different broadband solutions for connecting remote users with varying costs and availability. Security is an important part of remote access deployments to ensure that networks do not become infected, data theft does not occur, and policies are not violated. Off-site workstation should have the same level of maintenance if not higher than on-site systems to ensure data are properly backed up and remote users do not experience any down time as a result of a hardware or software issue.

CAD applications lend themselves to remote desktop connections because of the large data sets and coordinated files that are usually involved. Optimization techniques within CAD applications can be used to ensure a good user experience within the application.

Web Resources

General Telecommuting

http://www.commuterchoice.com/ - *Provides an open service to employers, commuters, and Commuter Choice service providers throughout the United States*

http://www.telework.gov/ - *GSA Telework Homepage*

http://www.telecommutect.com/homeplate/home.php - *State of Connecticut telecommuting resources*

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=DIRECTIVES&p_id=2254 - *OSHA – Worksite in an employees home*

http://www.telework.gov/twlaws.asp - *Federal agency telecommuting laws*

http://www.telcoa.org/index.htm - *The Telework Coalition*

http://www.gilgordon.com/ - *General Teleworking resources*

Broadband

http://www.fcc.gov/cgb/broadband.html - *FCC Broadband explanations*

http://www.dslreports.com/tools - *Broadband speed tools, reviews and more*

http://pcworld.about.com/od/dslcablesatellite/The-Best-and-Worst-ISPs.htm - *ISP Reviews*

http://www.itif.org/files/BroadbandRankings.pdf - *Worldwide broadband rankings*

CWA survey: average broadband speed in US is 1.9Mbps - *Worldwide broadband rankings*

Security

http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf - *Security for Telecommunication and Broadband connections by the NIST*

AU Online Resources

- SampleRemoteUserQuestionnaire.doc
- SampleChecklistForPersonalTeleworkSuitability.doc
- SampleTeleworkPolicy.doc
- SampleSupervisorChecklist.doc
- SampleTeleworkAgreement.doc
- SampleHomeNetworkSetupInstructions.doc