Executive Summary

Implementing a telecommuting program can be a major commitment, but it can also a major reward as companies save on such budget drains as real estate, recruiting, and disaster recovery, not to mention the increased employee satisfaction and retention benefits as well. Unfortunately companies can make a mistake by focusing so much on the potential rewards that they rush to put a program in place without considering all of the angles.

One of the biggest questions a company may have about telecommuting is remote access. How can management be certain that employees are using e-mail and Internet access properly and that security breaches and viruses can be guarded against? Overall, a company needs to assess the level of risk it is willing to take, because there is no 100 percent guaranteed safe process. Telecommuting inherently requires a level of trust between the telecommuter and the company, which is why choosing which employees will telecommute is the most important part of the process because even with careful planning, they can make or break the program. Nevertheless, there are measures that a company can take to secure its system and bind its telecommuters to an agreement about how, when, and why e-mail and
Issues to Consider

Before an organization allows an employee to work from home, even on a part-time basis, it should consider the following issues in regard to remote access.

Company Costs Versus Employee Costs

An organization can basically handle telecommuting in one of two ways. The first option is to allow employees to work from home, using their own computers and other equipment as well as their own Internet connection. Predominantly, a telecommuter will need a broadband connection, so in this case, employees would need to already have or install this type of connection, at their own expense, before telecommuting. The company then typically provides the software needed to access the company's VPN or LAN, if that is even necessary. In the most basic scenarios, a telecommuter simply uses tools--such as software and home e-mail accounts--and then sends files via e-mail attachments or via a company FTP site. Overall, a company may provide a list of essential equipment and specifications that employees must have at their home offices in order to be able to telecommute, but it is up to the employees to pay for this equipment.

The second option is for an organization to purchase all of the equipment necessary for the telecommuter, such as PC, Internet connection, fax, printer, second phone line, and software. As a result, the company would manage and control use and security features of the equipment, instead of being at the mercy of the telecommuter's existing equipment.

Although the second option is more expensive upfront for the company, it can provide better security measures and reduce headaches later on. Nevertheless, most companies deploy some type of combination of the two options. Perhaps an employee has certain equipment, meeting certain specifications, already. The company will then simply purchase for the employee the remaining equipment or software that is needed. Then, the employee owns part, and the company owns part.

Security

One of the biggest technology issues with telecommuting is security. Essentially, hackers are much more of a possibility, as they attempt to steal corporate information through electronic access. Transmitted data via e-mail, FTP, or VPN can be read and perhaps modified while it is in transit between the telecommuter and the office.

Within the confines of a traditional office setting, a company can adequately prevent a stranger from walking into the building, sitting down at a terminal, and using a company PC. Building security personnel, video cameras, attentive staff members, and other various security measures can prevent this from happening. When an employee is working outside of the home, however, this is much harder to prevent. For instance, an employee’s spouse, child, roommate can easily sit down and start using file-sharing programs or install beta copies of video games. Either of these actions could easily lead to a virus, which will infect the company's entire LAN.

Employee Compliance

Perhaps the toughest issue with telecommuting in general, but certainly with remote access in particular, is simply finding ways to make sure that telecommuters are adhering to policies and procedures. Even with detailed security measures in place, a company cannot always be certain that a telecommuter is properly taking care of or using e-mail or Internet access properly. It can also not be certain that a
telecommuter is not allowing other household members to see private company information or use company resources.

**Analysis**

[return to top of this report]

There are some steps that an organization can take to protect itself and to ensure that it is doing its best to implement solid policies and procedures for its telecommuters.

**Company Costs Versus Telecommuter Costs**

It is better for employers to provide telecommuting employees with the equipment necessary for them to participate in the program, rather than having the employees use their home computers. It is easier to maintain security, and it there will be less headaches when an employee's equipment breaks down. This also ensures that there are no compatibility issues. When an employer is providing the equipment, software, and broadband connection, the company knows—at least from the start—that the telecommuter has the proper specifications to carry out job responsibilities remotely. It can also place stricter restrictions on the telecommuter for monitoring and for following procedures.

**Security**

There are several different options for maintaining security. These options may require a fair amount of upfront investment on the part of the company, depending on the number of telecommuters, but it can definitely be worth the cost to ensure proper security measures are in place.

**Firewalls.** Companies must take steps to ensure that only authorized users can get to the internal, corporate network. Employers also must ensure that firewalls work properly and must decide what types of resources can be made available to telecommuting employees. Some employees working from home may only need access to corporate e-mail, while others may need access to files or programs. There are several firewall implementations, for example, that use an email proxy to allow access to files on a protected system without having to directly access that system.

When a telecommuter needs to use internal resources, access to a LAN, mainframe applications, or VPN, running client software, and TCP/IP may be required. In this case, a firewall or series of firewalls can be used to divide internal resources based on need of the telecommuter. Computers with high-risk data or proprietary information can be separated by a firewall from systems with a lower level of risk. In some cases, current firewall technology can give virtual access by using proxies.

A personal firewall, which is located on the telecommuter’s desktop, will help protect open ports and Internet programs as well as let administrators know if a PC is a vulnerable to a security breach. This can be centrally managed or non-manageable. In the case of the non-manageable firewall, administrators will not be able to know whether a telecommuter is running the personal firewall, or if it has been turned off. Furthermore, a telecommuter could adjust the safety parameters too low.

In the case of the centrally managed firewall, administrators can dictate the policy file and can prevent telecommuters from disabling the firewall or from changing the safety parameters. Administrators can also push out new policy files without user intervention and receive trouble reports.

**Robust Authentication.** Robust authentication is required if access is needed to internal systems, but it should also be used for e-mail, particularly if e-mail will be used to discuss business decisions. Robust authentication requires the user to possess a token as well as a password or PIN number. It can also create one-time passwords to provide a different password each time a user logs in. Most commercial robust authentication systems use smart tokens. The user provides a PIN that unlocks the token and then
uses the token to create a one-time password.

Telecommuters should use robust authentication in combination with routing to specific computer systems. This combination increases security significantly and reduces costs associated with robust authentication by limiting it to employees with the greatest access. If material is considered highly classified, cryptography is needed. Other methods, such as applying a digital signature to every packet, are currently being developed.

**Port Protection Devices (PPDs).** This option is fitted to a communications port of a host PC and authorizes access to the port before and independent of the computer’s own access control functions. A PPD can be either a separate device in the communications system or incorporated into a communications device, such as a modem. Usually, a PPD works in conjunction with an authenticator, such as a password.

The dial-back modem is one example of a PPD. A user calls the dial-back modem and enters a password. The modem hangs up on the user and then looks for the password using a table lookup. Once the password is found, the modem calls the user back to initiate the session. Nevertheless, hackers have been known to use call forwarding to reroute calls and intercept the session.

**VPN Client Software.** A telecommuter’s desktop should be loaded with VPN client software, and all policy files should be monitored from the corporate LAN.

**SOHO Router.** Multiple business PCs can be hidden behind one IP address by using a SOHO router, like those made by Linksys or Nexland. If a company only has one telecommuting PC, a SOHO router is not necessary but it does provide further security. Not all SOHO routers support IPsec traffic. So if a VPN solution can encapsulate IPsec with UDP, it is worthwhile.

**Separate Computers.** Some companies may require telecommuters to only use company equipment for company use, not personal. Personal e-mails, Internet access, and so on must take place on a personal PC in the telecommuter’s home. The policy can be difficult to enforce and requires diligence on the part of the company to monitor and inspect usage.

**Separate IP Addresses.** Some companies have started requiring that employees purchase a separate broadband connection for personal use in an effort to completely separate corporate transfer of data and personal. Furthermore, the business machines can be put behind a NAT box, and telecommuters can be told not to share data between the two devices.

**Employee Compliance**

There is no full-proof method for ensuring that telecommuters follow procedures, but companies can incorporate several different safeguards that will at least signal to the employee the severity of following protocols and provide accountability to the process. Each of these safeguards will require planning and devoted resources to implement, which could mean increased cost and management time.

**Monitoring.** Telecommuting employees may not realize the extent of security threats and disable desktop firewalls, turn off virus protection software, and disregard admonitions concerning downloading shareware files for personal use. Products are available to centrally manage firewalls and to monitor Internet and e-mail usage. Employers should have measures in place to punish these types of infractions, up to and including termination.

**Home Inspections.** If a telecommuter is housing company equipment in a home office, then it is a good practice for the company to do home inspections. This way, a company can ensure that a telecommuter is taking care of the equipment, monitor the type of environment the equipment is placed in, and see how the equipment is being used. This can be time consuming and difficult if a telecommuter is out of state or even the country, but where possible, it is a good policy to follow and signals to the telecommuter that the company is serious about following rules.
Telecommuting Agreements. Every company who works with telecommuters should have a telecommuting agreement in place. Along with regulatory, insurance-related, and administrative issues, the telecommuting agreement should also include the procedures that the telecommuter is to follow in regard to Internet access, e-mail, equipment ownership, and personal use of company equipment. It should outline security measures that the telecommuter is expected to uphold, and it should dictate what expenses will be incurred by the telecommuter and by the company. The telecommuting agreement should also outline what actions will be taken for breach of contract. Both parties should sign and date the agreement, and it should be reviewed and updated yearly.

Recommendations

[return to top of this report]

Overall, telecommuting can be a great option for both a company and its employees. Even though there are many concerns in regard to remote access, most companies believe it is worth the risk. Measures should be taken along with careful planning to ensure that the safest possible process is in place and that telecommuters adhere to it.

A step-by-step outline for organizations to follow when making decisions regarding e-mail and Internet use for telecommuters follows. This guideline is based on the recommendation made there that a company put together a team of cross-department personnel who focus on designing a comprehensive program, called here the "Implementation Team":

1. The Implementation Team, which comprises at least one member from IT, senior-level staff, HR representative, legal counsel, and department representatives from affected departments, assesses what needs are necessary in regard to remote access: equipment, software, what the company will pay for versus what the employee will pay for, type of Internet connection, and what information employee will need access to. This may need to be done a department-by-department basis if more than one department is involved and needs vary.

2. Once needs have been properly assessed, the Team should consider the ramifications of this setup. For instance, if the company is buying the equipment, how is it to be handled, who will support it, what happens if it breaks down, what happens if any employee or someone in the employee’s household breaks it? If the employee is responsible for incurring some of the cost, what restrictions does that place on the setup?

3. The Implementation Team next needs to look at security issues in regard to e-mail and Internet access. What type of data will be transmitted? How can it be secured? The Team should be looking at some of the options listed above. Which ones can the company implement?

4. The Implementation Team should now put together a cost assessment based on their findings. How much will it cost to set up each telecommuter for remote access? Once that is done, is this cost reasonable and still worth doing?

5. Now the Team is ready to run a test of the setup. Put together a system from a remote site and do conduct a trial run-through. This should allow room for adjustments as needed.

6. Then the Team will need to set guidelines that outline how various issues related to remote access will need to be followed. For example, what are the security procedures that need to be followed? What is absolutely forbidden? What is allowed?

7. Now the Team needs to think about how these guidelines will be enforced. What type of central monitoring can and will be done? How about home inspections, are they reasonable to do?

8. The Team should add the decisions made to these issues in the telecommuting services agreement. It is also wise to put together an equipment checklist as well as written procedures and rules that the telecommuter must follow in regard to personal use, security, etc. The employee must also have in writing what the consequences are to failure to comply.

9. All parties need to sign the agreement.
About the Author

Sheree Van Vreede is an independent consultant who has worked with the IEEE in the fields of telecommunications, information technology, and various scientific- and engineering-related issues. She works with the IEEE Standards as well, helping to publish guidelines for various technological processes. Sheree is a regular contributor to Faulkner Information Services for the past three years and is a member of Faulkner’s Advisory Panel.

Web Links

AT&T Telework Webguide: http://www.att.com/telework/
International Telecommuting Association and Council: http://www.telecommute.org/
June Langhoff’s Telecommuting Resource Center: http://www.langhoff.com/