GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Telecommuting: Security Policies and Procedures for the "Work-From-Anywhere" Workforce

Jessica L. Hirsch

Introduction

As today's business environment becomes ever more global, companies are faced with an increasing number of non-traditional work schedules. Whether it be a consultant who maintains a home office, or a "road warrior" who gets most of his work done in airports and hotel rooms, employers are recognizing the need for employees to stay connected to the office at all times of day and from all locations. In response to this need, businesses are becoming more interested in telecommuting, which gives employees the flexibility they demand while keeping productivity high.

Remote access and telecommuting, however, are not foolproof, easily implemented solutions. When the corporate network is opened to external access, a number of security risks are introduced, the severity of which are often related to the computer literacy of the employee accessing the network. For example, an intruder may find it simple to attack a less fortified home computer that a user has left logged in to the company LAN, especially when compared with the task of compromising the business network directly. In addition, the territory of an already burdened IT staff is widened, and they find themselves responsible for non-centralized computers that are more difficult to maintain and audit regularly.

Since telecommuting ability is no longer an option in many businesses, both IT and operational managers should take measures to make the process as secure as possible. These measures include, but are not limited to: defining and keeping current a telecommuting policy which clearly addresses security; selecting telecommuters who are computer-literate and responsible; implementing end-user training and awareness education; defining standards for and the means by which employees will purchase or borrow the equipment and software they use; and establishing a maintenance schedule and support network for employees located away from the central office. Each of these measures is discussed at length in the remainder of this essay.

Defining a Telecommuting Security Policy

The first question that should be asked when deciding to formalize and implement telecommuting is, "Does a policy currently exist that addresses telecommuting guidelines and security?" If so, this policy needs to be thoroughly reviewed and updated to account for new corporate guidelines, technology, etc. If not, then a policy needs to be created, so that everyone's expectations are clearly outlined and all are held to the same standard. The security portion of this policy should address, at a minimum:

- Required equipment, operating system, and applications software;
- Guidelines for the physical security of the equipment;
- Measures that must be taken to protect the integrity and security of corporate data

© SANS Institute 2000 - 2005 Author retains full rights.

(backup schedules, secure transmission or VPN access, etc.);
- Employee login and account restrictions, if any;
- Applications and data which may and may not be accessed remotely;
- Disaster recovery, in case of theft, corruption, or destruction of equipment and/or data;
- Support and maintenance guidelines and schedules, whether upgrades and support will be provided by the corporate IT staff or a third party;
- Employee accountability and responsibility for data integrity and confidentiality; and
- "Appropriate personal use" guidelines, if any

All telecommuting personnel should be required to read and understand the policy, and should sign a form for verification after going through any required training. These forms should be kept on file, perhaps with personnel records, for reference and accountability purposes.

Selecting Telecommuters

Oftentimes, a company does not have the luxury of choosing the individuals who will telecommute. These selections may be based on external factors, such as client demands, employee illness or injury, or widening scope of responsibility for an employee. However, with an increasing number of jobs designated for telecommuters, a business has some control over hiring and placement. When selecting the candidates or employees who will take advantage of telecommuting options, two factors should be taken into account: the employee's needs and his/her qualifications as they relate to computer literacy and awareness.

When looking at an employee's need to telecommute, a couple elements need to be evaluated. First, is telecommuting truly necessary? The employee's job function, percentage of travel, and need for constant access to current corporate information will answer this question. Managers who travel overseas extensively, for example, will be more likely to need remote access than salespeople who cover the local area and who are out of the office only two days per week. Second, how often and for how long will the employee need to telecommute? For an employee illness or vacation, a short-term solution, with a user ID that automatically expires once the set time frame has passed, may be an option. For a constant traveler, or an employee who has taken a leave of absence, telecommuting may be a total replacement for an office environment. It is these situations where security and maintenance of the remote computer become paramount.

A telecommuting employee must also meet certain qualifications in order for a remote access solution to work. He or she must have appropriate security clearance for the access level requested, and these access rights should be continually evaluated as the employee's job functions change. In this way, a telecommuter may have access to the materials and applications needed to complete his/her tasks, without being granted excessive permissions that may be taken advantage of, should an intruder compromise the account. Additionally, the telecommuter needs to possess a degree of computer literacy that would enable him/her to perform simple maintenance (backups, for example), to be aware of information security and the risks involved if a compromise does occur, and to know how to explain an issue, should additional support resources need to intervene. These skills may be inherent, or may be gained through a corporate training program, and will make the employee more comfortable with the idea of telecommuting

© SANS Institute 2000 - 2005 Author retains full rights.

and better able to understand the security risks involved with the arrangement.

Education and Training

The purpose of training end-users before they start to telecommute is two-fold: to introduce them to and make them comfortable with the system they will be using, and to raise their awareness of security risks and preventative measures.

If an employee is already familiar with the company's systems and software, then part of the battle is already won. Nevertheless, telecommuting brings additional tools into the picture, such as a personal firewall program, a VPN suite, different or enhanced anti-virus protection, and/or the means to encrypt stored data, all of which may be new to the employee. Therefore, the telecommuter must be trained in the use of these applications. Employees should receive a thorough explanation about what the software does and why it is important, and hands-on training in correct operation and basic troubleshooting of the applications. Educated team members who understand the need for such measures will be more likely to use them, will try to resolve problems or issues quicker, and will be more likely to cooperate with timely installation of upgrades and patches.

Raising telecommuters' awareness of general security issues will also aid in keeping remote access and transactions as secure as possible. While many users may understand, for example, the importance of not opening unfamiliar e-mail attachments while at work, they may not be as vigilant on their personal PC, and this behavior may lead to virus infection on the remote computer used to access the corporate network. Preventative measures need to be reinforced and understood, especially as they relate to security issues like viruses, PC configuration changes, physical security of desktops and laptops, intrusion attempts on unwatched-but-connected machines, and appropriate personal use of the equipment typically used for business access.

As part of a comprehensive telecommuting security policy, training such as that outlined above should go hand-in-hand with a business's formal written policy. Once training is complete, the user should sign a form indicating that he/she is aware of and agrees to abide by the rules and guidelines of the company. Also, ongoing "refresher" courses should be required as needed, as well as supplementary training for any new applications or significant upgrades.

Choosing Security Components

Any business with a number of dedicated telecommuters needs to seriously consider purchasing or leasing the equipment for their employees, or sharing the cost of the hardware. An American Management Association survey in November 1999 found that 42% of telecommuters were using personally owned technology to access business networks (3). Generally speaking, these computers are not subject to many of the "appropriate personal use" clauses in telecommuting policies, may contain conflicting or malicious software, are not thoroughly audited on a regular basis, and eliminate much of the control that a company's IT department has over telecommuting and the security thereof. Though the cost of ownership of this hardware may be higher, the trade-off of increased security and control may be worth it.

© SANS Institute 2000 - 2005 Author retains full rights.

At any rate, the software that is run on telecommuters' PCs needs to be standardized throughout the corporation. A multi-layered approach is best, with each layer providing some security from intrusion, malicious software, and other threats. A four-layered approach, for instance, could be comprised of the following:

- Anti-virus software used on the remote PC (regularly updated)
- A personal firewall program active on the remote PC (products are available from many commercial vendors)
- An encrypted connection via VPN to the corporate network
- Regular auditing, both of the remote computer's configuration and of session activity, time, and duration at the central location

Additional measures may include: the use of an e-mail proxy feature available through the corporate firewall, so that telecommuters may check their e-mail without requiring direct access to the corporate LAN (5); one-time passwords, "smart cards," or other alternatives to traditional passwords; or the use of call-back modems if modem access is supported. The type and extent of measures taken depends directly on the confidentiality and importance of the information being accessed remotely, and the company's budget for implementing security solutions.

Maintenance and Support

Once the telecommuter has been presented with the perfectly configured desktop or laptop that he/she will use to access the office, has gone through requisite training, and has signed off on the company policy, what are the corporation's ongoing responsibilities to the telecommuter and to its network? If the employee encounters a problem or suspects tampering, to whom does he or she report it? What happens if a patch is released for the personal firewall software, or when the virus scan libraries are updated? These are questions that must be faced by the IT and operational staff and addressed in the telecommuting policy.

Business leaders may choose to delegate the maintenance and support functions for telecommuters to the in-house IT staff. If this is the case, then timelines must be developed for remote PC auditing and upgrading. On a pre-determined schedule (monthly or quarterly, perhaps), employees may either bring in the system (if it is a portable one) for service, or a technician may be dispatched to the telecommuter's location to ensure that all updates and fixes are in place, that the system conforms to previously mapped out guidelines, and that any configuration changes are investigated and repaired.

Companies without this extensive in-house resource, though, may choose to hand over the maintenance and support functions to a third party, or may contract with an application service provider (ASP) to provide a majority of telecommuting service (one example of this would be www.myCIO.com). This decision would result in decreased liability for the company, since another party is providing the service and therefore the guarantee, but would also decrease the amount of control that the business has over the systems and applications used to access its internal LAN.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Conclusion

Telecommuting is becoming more popular and mainstream, as employers look to maintain productivity and employees demand more schedule flexibility. Businesses that lay the groundwork with a sound security policy and balance financial and security considerations are well ahead of the learning curve as it relates to maintaining data integrity and confidentiality. By creating a telecommuting solution with attention to information security, these companies will be able to meet the challenges of remote access and adapt to the emerging changes in technology and connectivity.

Works Cited

1. Anderson, Rob. "Telecommuting Trend Means Security Concerns." 28 June 2000. URL: http://www.localbusiness.com/Story/Print/0,1197,NOCITY_209401,00.html (10 Dec. 2000).
2. Berinato, Scott. "Do telecommuters invite intrusions?" 19 November 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2655595,00.html (08 Dec. 2000).
3. Goslar, Martin Ph.D. "Telecommuting + Telecomputing = Telechallenging!" 01 May 2000. URL: http:// www.earthweb.com/dlink.resource-jhtml.72.953.| repository| itmanagement|content|article|2000|06|15|EMgoslaresent5|EMgoslaresent5~xml.42.jhtml?cda=true (11 Dec. 2000).
4. Goslar, Martin Ph.D. "The New E-Security Frontier." InformationWeek. 10 July 2000. URL: http://www.techweb.com/internetsecurity/doc/283.html (10 Dec. 2000).
5. "Security Issues for Telecomputing." URL: http://www.nist.gov/itl/lab/bulletns/archives/telecomm.htm (11 Dec. 2000).
6. Wolk, Martin. "Telecommuting—A Security Threat?" 1 November 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2648861,00.html (08 Dec. 2000).
7. Zender, Anne, ed. "Telecommuting Security Checklist." Journal of the American Health Information Management Association. 1999. URL: http://www.ahima.org/journal/pb/99.02.ex6.html (11 Dec. 2000).

© SANS Institute 2000 - 2005 Author retains full rights.