



State of Colorado Monthly Cyber Security Tips

July 2007

Volume 2, Issue 7

Telecommuting Security Risks

Telecommuting is being used by some State agencies and considered by others as part of a workforce cost savings or environmental strategy. The issue of telecommuting is increasingly popular due in part to the potential of improved workforce capabilities. This edition of Cyber Security Tips is not advocating for or against telecommuting; however, if a State agency decides to implement telecommuting, there are specific steps that should be considered to address security.

Security Issues/Risks

Telecommuting can consist of the employee connecting to their office network via their own home computer, or from a State-issued machine. Because the State has less control over the security of the employee's home computing environment than it does the office environment, there are specific risks that must be addressed. The user may not have installed the necessary components to keep software up to date and may not be checking the home computer regularly for viruses, trojans, adware or spyware. Individuals in the household other than the employee may access the computer and download or install software, unintentionally infecting it, including installing malware, such as keylogging utilities that can track sensitive information, such as user IDs and passwords. Other computers on the home network can become infected and potentially spread the infection to the telecommuting computer on the home network. In addition, users may have a wireless network at home that isn't adequately secured, thus making all other computers and devices on the wireless network open to intruders.

Another important security concern that should be addressed is the physical protection of the telecommuting computer or home computer and the data on the computer or on other storage media, such as CDs, DVDs, and USB flash drives. The computer and the devices may be stolen if a break-in occurs at the employee's house or vehicle. We've had this

happen several times in Colorado over the past couple of years and it creates a tremendous liability for the State due to the possible exposure of sensitive data.

Steps to Making Telecommuting Secure

Before allowing telecommuting, ensure that your agency has a telecommuting policy that addresses cyber security issues. The policy should define requirements for both State agency and employee including a defined environment to work within. The Office of Cyber Security has established general policies including P-CCSP-002, Incident Response, P-CCSP-008, Access Control, P-CCSP-013, System Access and Acceptable Use, and P-CCSP-018, Mobile Computing that should be considered when designing a telecommuting policy. These policies are available at www.colorado.gov/cybersecurity/resources. You can contact my office if you need assistance crafting a policy.

1. Each individual agency needs to decide whether to provide a computer to the employee. By providing the computer, the State agency can control what is installed and what activities are allowed or not allowed (such as instant messaging or peer-to-peer applications).
2. The telecommuting policy must state what security features must be installed and maintained on the computer. Best practice security features include the following:
 - a. Firewalls (software and/or hardware)
 - b. Anti-virus software
 - c. Anti-adware / anti-spyware software
 - d. Encryption software
3. The policy should state what software is needed for the employee to work remotely, as well as what types of software will not be allowed on the computer.
4. The policy should identify to whom the user should report suspicious activity to. See P-CCSP-002, Incident Response. IT support staff should be ready to advise the employee on how to configure the computer and the employee's home networks for maximum security.
5. If the network connections are not properly secured, valuable data can be intercepted during the data transmission between the home and the agency network. Virtual Private Networks (VPNs) are a best practice for securing communications to the State agency's internal network. When connected to the agency's network, all transmissions should be encrypted, both coming from and going to the home. Every time a telecommuting device establishes a connection to the State agency network, it should be checked to ensure that all security software is active and up-to-date before being allowed access.
6. State agencies must assess the risk of allowing a telecommuter to directly access the State network versus taking copies of the data home. If the data being taken home is personal, private or sensitive data, it should be encrypted.
7. If a State agency has determined it will allow encrypted data to be removed from the network, they should limit the data being removed only to that which is absolutely necessary. In other words, don't download the entire file to bring home; only take that data which is absolutely necessary to complete the task.

8. When data is accessed from the State agency network by the telecommuting employee, the agency system should automatically log the time, date, user, computer or workstation, files, and the records they are accessing.
9. A two-factor method of authentication should be considered by the agency if the telecommuter accesses the State network from home.
10. The operating system and all applications should be up-to-date or at the most secure version available. File sharing should be turned off so no other computer can access data located on the telecommuting device.
11. Employees should be trained on security procedures.

Telecommuting Security Tips for Users

1. Follow your State agency's telecommuting policy.
2. Keep your anti-virus and anti-spyware/anti-adware software up to date and running real time protection.
 - a. Once a week, run a full scan on your computer – both anti-virus and anti-spyware.
3. Install a firewall and keep it up to date and configured securely.
4. Talk with your agency IT support personnel on how to configure it properly.
5. Report any suspicious activity on your computer such as:
 - a. Unexplained slow-down in performance
 - b. Ads popping up in windows
 - c. Hard drive activity when you aren't running any applications
6. If your telecommuting computer was assigned to you by your State agency, don't allow anyone else to access it.
7. If you have a wireless network at home, enable all security settings and change the default passwords.

Summary

Telecommuting is increasingly being discussed in today's work environment as organizations analyze remote workforce options. While security risks can never be eliminated completely, by taking precautions and enforcing a secure telecommuting environment, they can certainly be minimized.

For more information:

<http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf>

<http://www.itl.nist.gov/lab/bulletns/archives/telecomm.htm>

http://www.fedtechmagazine.com/pf.asp?item_id=190

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1147286,00.html?bucket=ETA

For previous issues of the Monthly Cyber Security Tips Newsletter go to

www.msisac.org/awareness/news/

Brought to you by:



<http://www.colorado.gov/cybersecurity>



<http://www.msisac.org>



<http://www.us-cert.gov/>