



Real Property Policysite



**Right Place,
Right Time,
Right
Solutions.**

*Alternative Workplace
Arrangements and
Asset Management*



5. Security

MEETING SECURITY PERILS OF TELEWORK AND ALTERNATIVE WORK ARRANGEMENTS

(article provided by Brian Bates, PMP and Demi Bekele, PMP, Booz Allen Hamilton; coordinated through Raymond Kent, Booz Allen Hamilton, Associate, CISSP, PMP, and President, Mid-Atlantic Telework Advisory Council - MATAC).

Background

Telework and alternative work arrangements (AWA), also known as flexible work arrangement (FlexWork), are progressively moving in an upward trajectory. This trend has become critical in supporting business continuity and maintaining productivity, retaining a knowledgeable workforce and appealing to a new generation of employees interested in work/life balance, as well as reducing a company's carbon footprint (the total set of GHG (greenhouse gas) emissions caused directly and indirectly by an individual, organization, event or product).

Several factors contribute to this trend, including:

- improvement in technology (such as web meeting and instant messaging, electronic bulletin board and threaded discussion (an electronic discussion), collaborative whiteboard and shared text tool);

- improved telecommunication (such as broadband internet connections and wireless network access);
- government policies supporting and promoting telework;
- employees' increasing interest for flexibility; and
- cost savings through reduced real estate costs.

By recognizing these and other advantages that teleworking offers and setting a culture for measuring performance by results rather than by worker visibility, an organization can create a work environment that is conducive to teleworkers. Adopting a FlexWork policy is one method to help staff balance their professional and personal commitments. As such, managers should be aware of the various telework drivers and benefits and support the career advancement of teleworkers similar to onsite employees.

Secure Telework/ AWA

Security is a topic that often comes up when organizations start discussing telework. The idea of removing data from the four walls of the organization and network firewalls raises concern for potential security leaks. The challenge most organizations face is to give teleworkers sufficient freedom to do

The challenge most organizations face is to give telecommuters sufficient freedom to do their jobs without compromising data security and privacy.

their jobs without compromising data security and privacy. Therefore, it is imperative that sufficient security processes are put in place to protect the data used/accessed by staff that work away from the office and implement the optimum levels of security on the various remote working tools.

Some areas that are instrumental in setting up a successful telework environment include:

- strategy,
- tools,
- data,
- personnel, and
- physical security.

It is important that organizations take a holistic (comprehensive/integrated) approach to teleworking by providing the technology, policy and facilities that enable people to work most effectively. In developing its telework policies, an organization should also look beyond the technology and cover everything from employee eligibility and approval for telework, to training on safety considerations.

The policies, processes and standards driving secure telework/AWA should be well defined, documented and evaluated periodically.

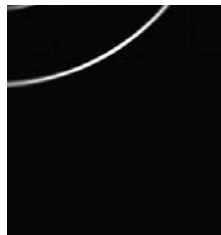
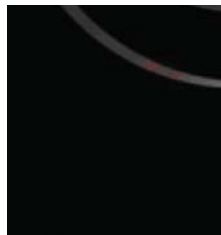
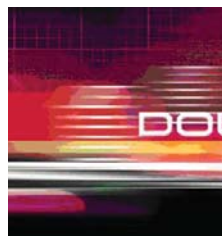
Tools such as secure email, instant messaging, web meeting, intranet web portals and virtual whiteboards allow workers from geographically dispersed locations to work

collaboratively. While these tools provide great convenience for teleworkers, organizations should be cognizant of the security vulnerabilities they pose and take proper precaution to protect their data. The security risks associated with collaboration are not too different from those that IT (information technology) security professionals have been dealing with for years.

However, the real-time nature of collaboration, along with the need to give multiple users in many locations access to applications and content, creates new challenges when it comes to dealing with these risks. As a result, it is necessary to implement a strong security collaboration framework, one that includes both tele- and data communication, to protect sensitive information and data integrity. By creating an "information security services group" to develop a comprehensive

list of technology and process services available to support staff members who work on-site and remotely, this can enhance the security, privacy, and integrity of a firm's and its clients' applications, data, and proprietary information. Securing collaboration through use of encryption is an absolute necessity. Hard drive encryption ensures stored data are only available to authorized users and trusted networks, and unavailable to unauthorized personnel if lost, stolen or otherwise exposed. A secure FTP (File Transfer Protocol) site can also be used to transfer large files internally and externally for a firm, while also allowing clients to upload and access the encrypted files.

Proper authentication provides a degree of assurance to the person's identity. Providing secure remote



access, workstation, and network and application access for authorized employees keeps unauthorized users out of the organization's networks and away from sensitive data. The use of Virtual Private Network (VPN) to access the organization's network, standards-based encryption, and more specifically Public Key Infrastructure (PKI), addresses not only the issue of user authentication but also the protection of data from eavesdropping. By using a Secure Socket Layer Virtual Private Network (SSL VPN), a teleworker can access several internal resources, via any equipment - whether it is a home computer, public terminal, or client-issued equipment. Secure VoIP (Voice over Internet Protocol) is one method that allows employees to use the same phone number at the alternate location as in the office which reduces confusion, such as leaving a phone message regarding the organization's business on the wrong telephone number. The use of VoIP adds the burden of protecting two infrastructures - voice and data. However, with proper application of encryption algorithms and use of VPN, the security risks can be mitigated.

Human capital management is an important component of a secure telework arrangement. Specifically, successful programs must address both top-down (e.g., managerial concerns with strengthening the organization's competences as well as securing its data) and bottom-up demands (e.g., employee needs). This can be achieved through collaborative program planning, careful evaluation, and ongoing program improvement, ultimately

aligning and supporting the organization's strategic and security objectives. Training and education might be the most important aspects of secure telework. Organizations should consider making both remote and on-site training available and making sure that proper access is provided to training and refresher courses to ensure teleworkers follow the remote access policy the organization has put in place, including the handling of sensitive data and secure travel.

To minimize the risks around the physical security of the organization's data and equipment, guidance should be provided on how to properly set up and maintain a home office. The organization should clearly communicate its information security policies about issues such as securing work computers with a locked drawer or cabinet and, using proper protection on PDAs (personal digital assistant), telephones (regular, cell, VoIP), desktop video conferencing, etc., including how to properly manage printouts of work information.

Conclusion

There is no doubt that maintaining a secure telework environment presents many unique challenges. However, it is clear that the perils,



which can be managed, are eclipsed by the benefits. Many public and private organizations (including Booz Allen Hamilton), embrace this environment and have been providing secure telework programs for years.

These organizations have:

- identified program and system level security gaps,
- evaluated, developed and integrated multiple identity and access management solutions,
- implemented industry standard data encryption tools, and
- designed, developed and delivered remote and onsite training and evaluation programs as well as vulnerability and policy management capabilities.

With careful planning and implementation, organizations can protect and secure their information and network resources, anticipate and mitigate strategic risks, and counter threats that impact mission-critical infrastructure and stakeholder value. ■