



**Missing Link**   
**Security Services**  
Mark Bouchard, Founder

## Tackling the Telecommuting Tsunami—Is Your Organization Ready to Ride the Wave?

### Table of contents

Introduction .....	2
Telecommuting Taking Off.....	2
Tough Times for Everyone .....	2
The Green Machine.....	3
Conventional Wisdom Holds True.....	3
A Strong Foundation Is Now in Place.....	3
Telecommuting Best Practices.....	3
Be Selective .....	3
Empower Users for Success.....	4
Secure the Situation .....	4
The Role of SSL VPN Technology .....	5
Comprehensive Access .....	5
Robust Security .....	5
Comprehensive Applicability .....	6
Summary.....	6
Footnotes/Sources .....	6
About the Author.....	7



## Introduction

Tough economic conditions and heightened environmental awareness are reinforcing an already strong case for telecommuting. Add in the conventional wisdom that a happy worker is a productive worker, along with the growing ubiquity of essential, underlying technologies, and telecommuting is poised to be a major trend, as opposed to the slow-rolling, moss-covered stone that it has been over the past decade or so. In fact, the U.S. Chamber of Commerce is estimating that the number of full and part-time teleworkers in the United States will increase from its current level of 30 million to between 50 and 100 million by 2012.

As attractive as telecommuting may appear, however, achieving meaningful gains is far from guaranteed. To ensure a successful telecommuting program, organizations should ideally pursue the best practices cited herein. Business unit managers need to realize that telecommuting is not appropriate for everyone. They need to manage user expectations and should also work closely with IT to ensure that essential policies, processes, and technologies are put in place. With regard to technology in particular, it is important to recognize the tremendous potential of SSL VPNs. Leading solutions are not only capable of efficiently providing telecommuters with access to all types of centralized applications and data resources, but they also help address a broad range of related security and privacy concerns.

## Telecommuting Taking Off

These days, it seems the terms “telecommuting” and “teleworking” are often used interchangeably. For the record, though, “telecommuting” refers to the specific case where work is done from home, either on a part- or full-time basis. In comparison, “teleworking” refers to the broader scenario where work is done from any place other than a corporate office and includes other locations such as coffee shops, hotel rooms, and facilities belonging to partners or customers. Also for the record, the primary focus of this paper is telecommuting because of the clearer, more direct impact that it has relative to the burning issues of the day: higher fuel costs, a weak and troubled economy, and unsustainably poor treatment of the environment.

Distinctions aside, all signs point to telecommuting/teleworking taking off. For example:

- According to a study conducted by The Polling Company, nearly 25 percent of U.S. workers and 41 percent of small business owners regularly work from home or another offsite location. Furthermore, respondents indicated that the ability to work remotely is valued more than stock options and onsite child care.
- 40 percent more employers are offering telework programs this year than last year<sup>1</sup>.
- 25 percent of the total workforce teleworks at least one day per week, and that number is increasing by 20 to 30 percent per year<sup>2</sup>.

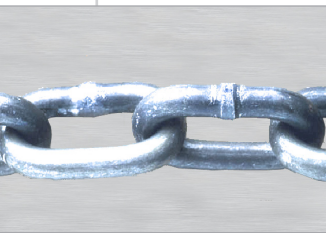
Then there are the efforts and initiatives of major governments worldwide. For instance, in June of 2008, the United States House of Representatives voted to require federal agencies to expand telecommuting. In Japan, companies supporting telecommuting are receiving significant tax breaks. And in Singapore, a fund has been established to help companies implement practices like teleworking that improve work-life balance.

Overall, considering the prevailing economic conditions, environmental concerns, derivative benefits, and ongoing technology trends, it is not difficult to understand why adoption rates for telecommuting are on an upswing and, moreover, are quite possibly primed for a veritable explosion in the near future.

## Tough Times for Everyone

Economists are bound to endlessly debate which segments and geographies of the world economy are “technically” in recession and which are not. But for the majority of organizations and their employees, it is quite clear that they are operating in a period of economic difficulty and uncertainty. Home and business values, retirement funds, and practically all types of investments have been hit hard. Available credit has all but dried up. And the costs for goods and services, especially fuel and energy, continue to climb (despite periodic fluctuations).

Not surprisingly, telecommuting is attractive in this kind of economic environment because of the financial relief that it can provide—which, it should be noted, is applicable regardless of the state of the economy. For employees, this takes the form of cutting commuting costs and related expenses for vehicle maintenance. Even for individuals that work from home only a couple of days per week, the savings can easily reach several thousand dollars per year.



On the other hand, employers can cut costs literally by millions as a result of having to buy, heat, power, and furnish less real estate. For example, an organization that manages to eliminate one office space for every three of its 3000 telecommuters can save approximately \$3 million per year (assuming a very conservative annual cost of \$3000 per office).

Employers also stand to gain from the greater operational flexibility and resiliency that telecommuting affords. Talented individuals can be recruited, vetted, and employed despite their being “geographically undesirable”—all without having to incur the expenses, distractions, and disruptions associated with relocation. In addition, having a telecommuting program in place inherently, and therefore inexpensively, helps organizations address another high-level business objective: maintaining continuity of operations during disruptive events such as storms, natural disasters, or acts of terrorism.

## The Green Machine

Growing public concern with global warming and other environmental issues is spilling over into the business world. As a result, companies are increasingly looking to make their operations “greener” by minimizing their environmental impact. Telecommuting dovetails nicely with this objective because it decreases commute-related emissions, wear and tear on public infrastructure, and consumption of scarce resources such as fuel and land. Furthermore, it can help organizations:

- Achieve compliance with related regulations such as state-instituted traffic restrictions, and federal or global limits on carbon emissions;
- Qualify for available tax incentives associated with “being green”; and
- Establish a green corporate image, thereby accruing customer goodwill.

## Conventional Wisdom Holds True

Another factor contributing to the interest in telecommuting is that many of its softer benefits have proven to be very real. Based on years of real-world experience, it is now generally acknowledged that higher productivity and increased job satisfaction do, in fact, result from telecommuters having fewer distractions, lower stress, and a better work-life balance. Indeed, for well-managed telecommuters, it is not uncommon to obtain productivity gains of 30+ percent, as outfits such as British Telecom (31 percent), Dow Chemical (32.5 percent) and American Express (43 percent) have demonstrated<sup>3</sup>.

## A Strong Foundation Is Now in Place

Finally, telecommuting is also poised to take off due to the relatively recent emergence of a strong technology foundation. There is little doubt that the implementation of telecommuting programs and their potential for success is facilitated by elements such as:

- The ubiquity of broadband Internet services;
- The proliferation of relatively inexpensive and/or user-owned client devices; and,
- The widespread adoption of collaborative solutions and other enabling technologies such as presence software, Web 2.0 applications, and VoIP.

## Telecommuting Best Practices

Just because the benefits of telecommuting are ripe for the taking, however, does not mean they can automatically be achieved or, for that matter, maximized. To get the most out of a telecommuting program, organizations will need to carefully control who is allowed to participate. Management, along with IT, will then need to provide these employees with the guidance and tools required to enable them to operate both successfully and securely.



## Be Selective

Telecommuting is by no means appropriate for all of an organization's employees. Unless there's a good fit, expected benefits will be minimized and can even turn into negatives. This is precisely what happened at Hewlett-Packard and Intel, each of which decided to scale back its telecommuting program in response to unacceptable fall-offs in employee productivity and collaboration<sup>4</sup>. To avoid having a similar experience, it is recommended that organizations evaluate a range of factors when considering whether to pursue the use of telecommuting in a given scenario. These include:

- The nature of the work. Best results are obtained when the jobs being performed are task oriented and require little communication or interaction with others.
- The nature of the employee. The best candidates are self-motivated staffers with a minimum of several years experience.
- The nature of the telecommuter's direct manager. Supervisors without the skills or temperament to manage employees remotely can quickly erode the success of a telecommuting initiative.

Ideally, supervisors should also be assessing the productivity of their telecommuters on a fairly regular basis, so that any corrective actions that are required can be taken as early in the process as possible.

Furthermore, it's important to realize that telecommuting is by no means appropriate for all organizations. In other words, another significant consideration will be the nature of the company itself. If the organization as a whole is not particularly receptive to having employees work from home, if there is an inclination to treat telecommuters as "less than equal" to their in-office counterparts, or if the corporate culture places a premium on team concepts and contributions, then it will probably be best to use the practice of telecommuting rather sparingly—at least until these conditions change or, better yet given the benefits at stake, are proactively addressed.

## Empower Users for Success

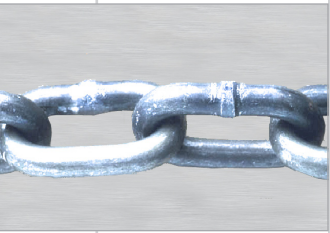
The magnitude of the gains derived from a telecommuting program will depend as well on the extent to which users are empowered to succeed. Unless telecommuters are given sufficient guidance and have access to an appropriate set of tools, the results will inevitably be poor. To avoid this outcome, organizations should consider instituting related best practices, including the following:

- Creating a telecommuting policy and/or agreement that clearly spells out management's expectations and user responsibilities (relative to work schedules, output, meeting attendance, qualifying expenses, and so forth);
- Providing advice and possibly assistance for setting up a proper workspace;
- Taking extra measures to keep telecommuters "in the loop" (such as issuing a specially prepared newsletter or requiring regular interactions with co-workers);
- Provisioning "enabling" and cost-saving technologies such as virtual/hosted PBX services and collaboration software; and,
- Implementing a solution to ensure that users can easily and seamlessly access all of the applications and related computing resources required to get their jobs done.

This last item, in particular, is absolutely crucial. The productivity of telecommuters will undoubtedly be impacted unfavorably if they are unable to access applications and systems in a manner and to an extent comparable to that available when operating from a corporate office.

## Secure the Situation

Intentionally left out of the previous section in order to emphasize its importance, security is another ingredient critical to the success of any telecommuting initiative. Enabling remote access to data and applications obviously exposes those resources to greater risk. This is doubly true if the client device being used is one that is not owned, or more importantly managed, by the organization—a condition which currently applies for approximately 50 percent of telecommuters and is likely to become even more prevalent going forward.



A fundamental prerequisite of any telecommuting program, therefore, is the need to mitigate these risks. Steps that organizations should consider to help meet this objective include the following:

- Establishing detailed policies and procedures for telecommuting security that cover items such as usage, storage, and disposal of sensitive data;
- Ensuring awareness of and performing training on the aforementioned policies and procedures;
- Provisioning telecommuters with physical security equipment and essential endpoint security tools such as shredders, cable locks, secure storage containers, antivirus software, and a file/disk encryption solution;
- Conducting periodic audits of telecommuter work environments;
- Controlling the telecommuter's ability to access, download, and locally operate on sensitive data by implementing a wide range of technical countermeasures such as identity-based access control, host integrity checking, transport encryption, information usage controls, secure virtual workspaces, content filtering, and terminal services (for view-only access); and,
- Defending the corporate environment from potentially compromised telecommuters by implementing "backstop" countermeasures such as network isolation tools and techniques, and network and host intrusion prevention systems.

Pursuing each of the sets of best practices outlined above has one other important advantage as well. Specifically, it puts a framework in place that defines "how to do telecommuting the right way" for a given organization. With any luck, this should reduce the likelihood of having individual, well-meaning business units do it some other way—a way that is inevitably not as effective and less secure.

## The Role of SSL VPN Technology

Considering the requirements that need to be met to ensure a successful program, SSL VPN technology definitely has a role to play when it comes to telecommuting. Indeed, a leading SSL VPN solution could very well be characterized as an ideal fit. This is based on being able to provide comprehensive access to centralized resources, the breadth and depth of security capabilities it delivers, and the ability to address all of an organization's other remote access needs as well.

### Comprehensive Access

A major strength for top-tier SSL VPNs is the capability to provide any user, operating in any location and with practically any client device, access to any type of application they need. In other words, with little more than a Web browser, telecommuters can access whatever resources they need to get their jobs done, be they basic Web-based applications, or ones that are a bit more complex (for example, involving XML, JavaScript, Flash, or requiring a socket connection), telnet/SSH-hosted applications, terminal services applications, custom-built client/server applications, or even just simple Windows and Unix file shares.

And unlike IPsec VPN solutions, there is no need for a pre-installed client. Administrative effort is reduced considerably and support can easily be extended to a wide range of both corporate and user-owned devices. As a result, organizations effectively have a choice: they can reduce program costs either by allowing telecommuters to use their own client platforms or by provisioning low cost alternatives to conventional laptops and desktops; they can stick with whatever computing device is the corporate standard; or they can choose to mix and match based on whatever criteria best meet the needs of the business.

Moreover, the experience for the user is completely straightforward. The only choices that have to be made are which resources to access. In fact, in many instances the solution can be configured so that users are able to access resources in a manner and with a look and feel identical to that applicable when operating locally.

### Robust Security

Beyond enabling access to centralized resources, SSL VPNs also provide a wealth of capabilities to help "secure the situation," as discussed earlier. One of the most important of these, particularly given the goal of supporting user-owned and managed endpoints, is host integrity checking. Host integrity checking enables organizations to have access to resources be conditional based on the outcome of an inspection of the user's device. For example, client platforms that are found to be "clean" can be granted full/normal access. In contrast, those discovered to be missing patches or essential security software can be restricted in some manner, or even completely blocked until discrepancies have been remedied.



In addition to host integrity checking and, of course, transport encryption for all user sessions, other commonly available security capabilities include the following:

- Multiple options, including strong, multi-factor methods, for user authentication;
- User/application single sign-on (SSO);
- Granular authorization/access control that can be dynamically adjusted based on a wide variety of attributes (user role and location, strength of authentication, and ownership or security posture of the client device);
- Cache cleaning, which removes information remnants from browser and application-specific caches upon completion of an access session;
- Secure virtual workspaces, which refers to the ability to create an encrypted workspace on the client device to help prevent data leakage;
- Information control, which involves limiting the functions that users can apply to accessed data (copy/paste, save, print);
- Gateway-based features such as embedded firewalling and mechanisms to thwart denial-of-service (DoS) attacks; and
- Detailed activity logging for both user and administrator sessions to enable monitoring, facilitate troubleshooting, and help demonstrate compliance with policies and any applicable regulations.

## Comprehensive Applicability

Last but not least, another compelling benefit of SSL VPN technology is that it is applicable to much more than just telecommuting. Most organizations today have come to realize that one of the keys to achieving greater operational efficiencies, raising the level of service to their constituents, and remaining competitive in general is increasing the accessibility of select business data, services, and systems. This means having to steadily increase support not just for telecommuters but for all types of teleworkers—so road warriors, occasional travelers, and day extenders as well—in addition to a broad array of guest users, partners, service providers, and potentially even customers. The good news is that because of the breadth and depth of their capabilities, top-tier SSL VPNs can efficiently and effectively support all of an organization's secure access use cases, both now and as they continue to emerge in the future.

## Summary

Telecommuting is poised to take off. A strong technology foundation is now in place and the advantages it provides are simply too hard to ignore, especially in times of economic turmoil. Employees that telecommute can save a small bundle on commuting costs, reduce their stress levels, and achieve a better work-life balance. In turn, their employers stand to gain in terms of increased productivity, higher retention rates, a better ability to attract and take advantage of far-flung talent, lower facilities costs, and an improved posture when it comes to maintaining continuity of operations.

To ensure and hopefully maximize these gains, however, organizations need to be selective. Telecommuting is not a good fit for all employees and situations. In addition, organizations will need to provide their telecommuters with the guidance and tools required to operate both successfully and securely. In this regard, one solution that makes particularly good sense is an SSL VPN. Leading SSL VPN products efficiently enable comprehensive access to centralized resources, provide a wealth of essential security capabilities, and can simultaneously address practically all of an organization's other secure access scenarios as well.

## Footnotes/Sources

1. WorldatWork
2. The Telework Coalition
3. The Telework Coalition
4. Computerworld, "The trouble with telecommuting", October 13, 2008



## About the Author

---

Mark Bouchard, CISSP, is the founder of Missing Link Security Services LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of networking and information security topics for over 10 years. He is passionate about helping enterprises address their information security challenges. During his career he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and overall architectures to the justification, selection, acquisition, implementation and operation of security and networking solutions.

2000293-001 Nov 2008