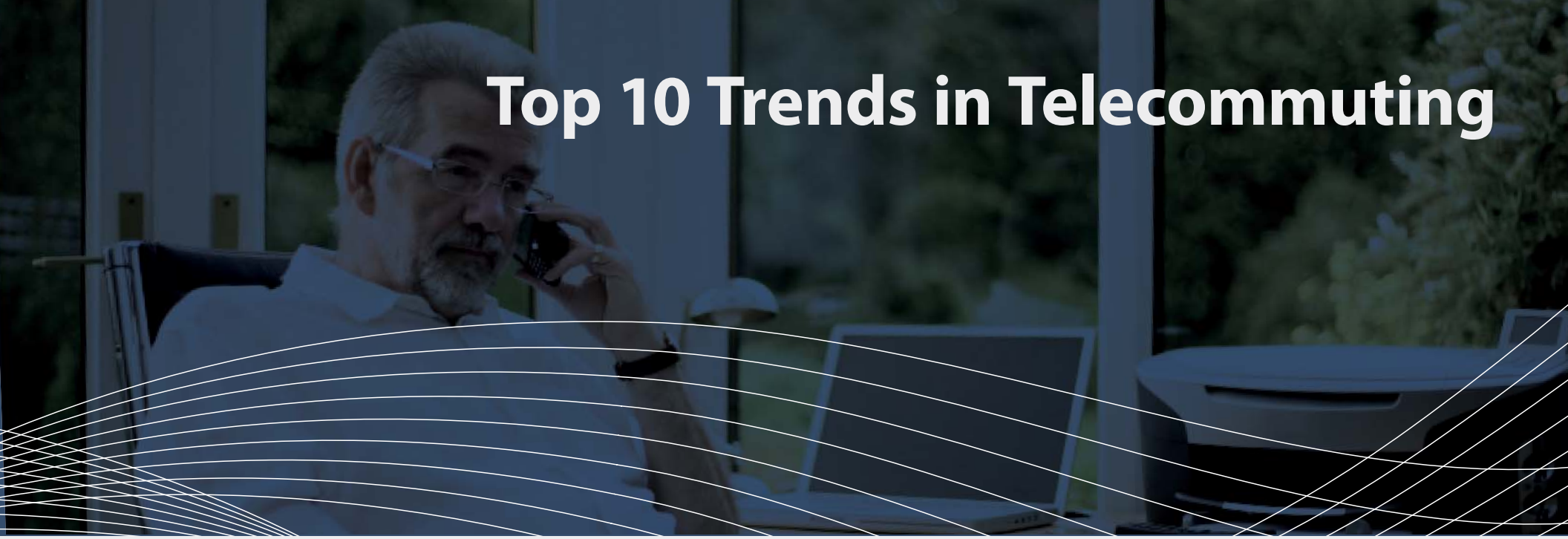


Top 10 Trends in Telecommuting

Business drivers for working remotely, and the technology to make it secure

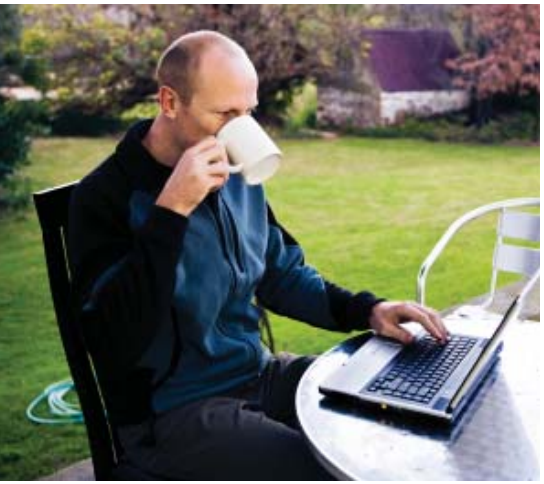
SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS®

Table of Contents

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS®

Introduction



Once, the key drivers for telecommuting were productivity and flexibility—the so-called "work-life balance" that many workers strive for. Those "soft benefits" still exist, but, increasingly, financial considerations such as gas prices, the credit crisis and hard cost savings drive telecommuting programs. Telecommuting programs also help companies strengthen the loyalty of their workers.

Whether driven by hard or soft benefits, telecommuting programs have one core requirement: give telecommuters secure access to corporate networks, applications and data. For workers at remote sites, IT and corporate security managers must select secure remote access technologies to make telecommuting not just viable, but safe. The following pages offer an overview of the top 10 business and technology trends in telecommuting.

"It's been a perfect storm. Rising gas prices, leading-edge technology, and the push for work-life flexibility have all come together in the past 12 months to create a pretty dramatic increase in telework across the U.S. and Canada.[1]"

1. Business trend: reigning in operating expenses

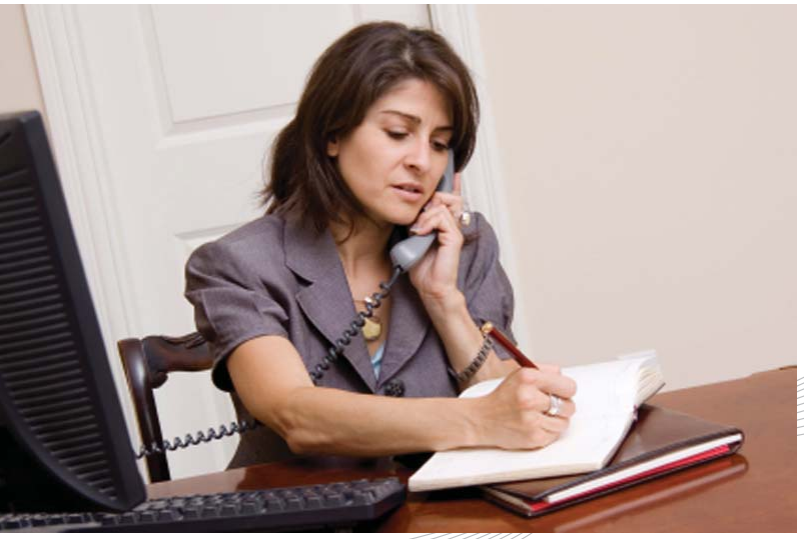
In the big picture, telecommuters help companies lower their operating costs. When telecommuters use their own space, power and cooling to work from home, savvy employers adjust their facilities practices to pocket that savings.

"Hot desking' involves one desk shared between several people who use the desk at different time. A primary motivation for hot desking is cost reduction through space savings—up to 30% in some cases.[2]"

The Canadian Telework Association (CTA) puts some numbers to the "hot desking" phenomena, suggesting that employers need one less office for every three telecommuters or about $2,000 per teleworker per year. AT&T saved $550 million by eliminating or consolidating office space ($3,000 per office) in its telework program, CTA states. About 25% of IBM's 320,000 workers worldwide telecommute from home offices, saving $700 million in real estate costs, per the CTA.

2. Business trend: finding and retaining talent

Economic conditions such as inflation, rising gas prices, military relocations, the housing downturn are affecting many workers and their families. In a May 2008 online survey, the Telework Coalition found that 87% of respondents would limit a job search based on potential commute costs. For businesses, telecommuting breaks barriers to reaching staffing pools in geographic areas with lower salaries or higher talent concentration.



Telecommuting programs can cement employee loyalties. Sun Microsystems says its telecommuters cite the Open Work program as the No. 1 reason they would recommend Sun. By reducing job turnover, employers also eliminate costs of training new hires.

37% of IT workers say they'd accept up to a 10% lower salary to work full-time from home.[3]

3. Business trend: meeting regulatory compliance

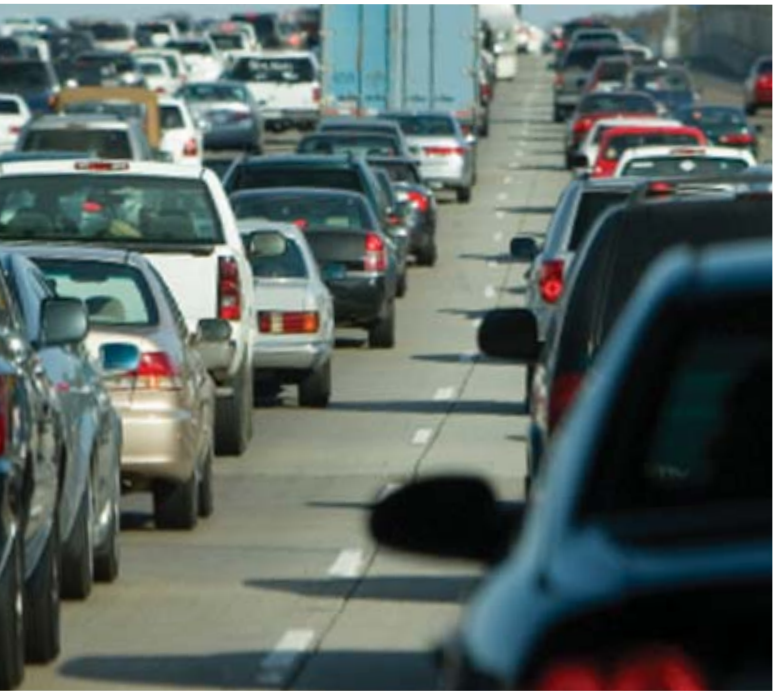
In recent years, businesses have been required to comply with more industry and government regulations, such as Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley and PCI. In general, the goals of such regulations are to protect customer information from unauthorized access, or to safely present corporate information to the public.

Telecommuters are not excluded from these compliance mandates, so the viability of a telecommuting program requires having technology in place that both monitor telecommuting workers and onsite employees:

- to ensure the identity of who is accessing data.
- appropriately restrict access to sensitive data.
- correctly segregate users, resources and communications.
- verify procedural integrity with effective audit trails.

The total cost of identity theft approaches $50 billion per year.[4]

4. Business trend: preparing for disasters



Disaster recovery has become an increasingly important objective in the era of globalization. An outage at a distant, but strategic, power facility can cripple work, not just locally, but at every other company location. The continuing trend of outsourcing exposes the company to outages that affect their outsource partners.

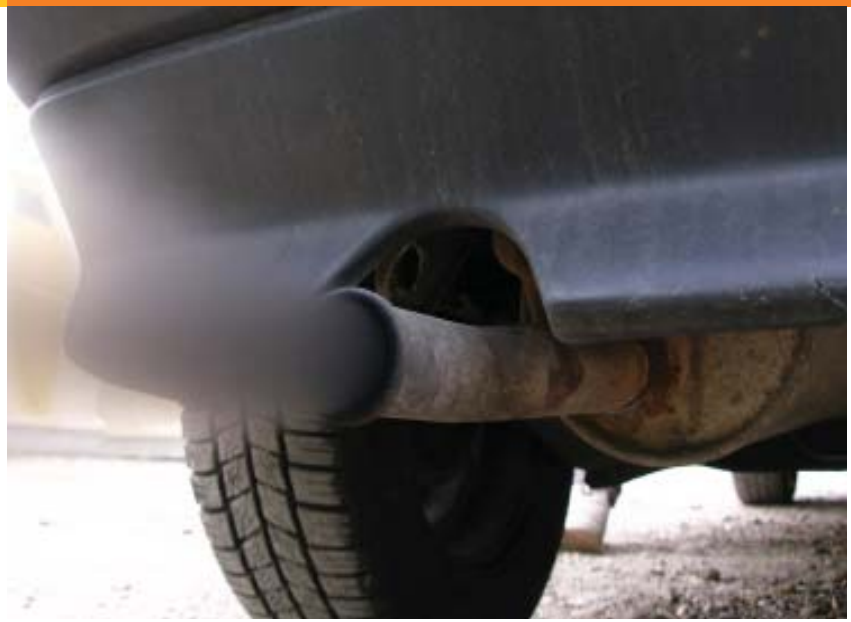
By definition, telecommuting distributes employees away from central offices. Central offices may be knocked out through power outages, weather, traffic jams or localized disturbances. Even a few miles make a difference in those situations, when companies can operate business as usual, maintaining revenue streams and delivering an "always on" image with customers, partners and investors.

"When things get busy, like in a weather event, we can send an e-mail to all [at-home] agents asking them to log in to help. The response is immediate—we don't have to wait for them to come in.[5]"

5. Business trend: working "green"

A company's carbon footprint includes employee business travel by car, airplane, rail and other public transportation. Energy for heating, cooling and electricity also count. Carbon emissions from consuming goods and services also may be included. Fortunately for the environment, going "green" often reduces both carbon footprints and costs.

How does telecommuting affect carbon footprints? In many cases, telecommuters are simply shifting energy consumption from the employer's building to their own homes. However, recent research by Sun reports that its telecommuters use roughly half as much energy at home as they do in the office.



Broadband and collaboration software could could increase the number of telecommuters from 10% to 20% of the U.S. workforce over the next 10 years and reduce carbon emissions in the U.S. by 45 million tons annually.[6]

6. Technology trend: accessing broadband everywhere

As the number of homes with broadband Internet access grows, working from home becomes more viable.

Telecommuters can work more effectively with broadband connections because enterprise applications run closer to real-time when accessed over a fast connection instead of dial-up. Broadband also makes VoIP (Voice over IP, or Internet phone) and other bandwidth-hungry new applications viable when they would not be with a slower connection.

In mid-2008, Gartner Inc. put broadband access from U.S. homes at 54%[7], and even higher in six European Union nations (Netherlands, Switzerland, United Kingdom, France, Sweden, and Belgium) plus South Korea, Hong Kong, Canada, Singapore and Taiwan. By 2012, Gartner sees broadband connections in 77% of U.S. homes.

7. Technology trend: collaborating via Web 2.0

New applications such as wikis and VoIP are key enablers of online collaboration so that employees don't have to be in the same location to work together. For telecommuters, remote collaboration is a huge productivity gain, as proven by the growth of Web conferencing for meetings. Today Web meetings have become commonplace within companies that have distributed workforces, whether in remote offices or home offices. Web meetings not only boost collaboration but keep remote workers from feeling isolated from central office contact.

In terms of office culture, outsourcing and extended supply chains have given many organizations new lessons in real-time collaboration—online or by phone—with suppliers, partners and outsourcers. Now employees can apply those skills to collaborate with each other remotely.

"Web 2.0 applications are already present on the majority of corporate networks, whether they've been formally or centrally-approved or not, through bandwidth and time-based restrictions.[8]"

8. Technology trend: mobilizing communications

Falling prices and greater horsepower of smartphones, PDAs, other handheld (Blackberry, Symbian) devices, as well as laptop computers, have put the technology of telecommuting within the reach of many organizations and their workers.

In one poll[9], however, 70% of respondents admitted to accessing corporate data over wireless—posing a great concern for network security. In corporations, PDAs tend to be managed (even issued) by corporate IT, so they are more likely to be configured to access the corporate network securely. Smartphones are most often owned by the employee and then used to access the company network for work. Both types of devices open corporate networks to new threats, not the least of which is that small devices are easier to lose than larger ones. Plus IT departments are responsible for smartphones without controlling them.

"82% of smartphone owners said they use their devices to read business e-mail, 80% surfed corporate Web sites, and 61% accessed enterprise data.[10]"

9. Technology trend: protecting against more sophisticated threats

No longer are culprits simply brilliant teens or other amateurs. Organized crime has moved into the Internet age. To growing hacker sophistication, add the reality that tough economic times force companies to cut their work forces, potentially creating a new class of security threats: disgruntled ex-employees. What if those unhappy ex-employees become potential partners to professional hackers?

Secure Sockets Layer virtual private networks (SSL VPNs) form the basic security requirement for secure telecommuting, and also address the growing sophistication of hacker attacks and the organizations behind them. Telecommuting, which on the surface might seem to open new security vulnerabilities, should not, if enterprises insist on secure remote access technology.

Not only are attacks on networks growing more sophisticated, but the cyber-criminals are become more sophisticated in organizing themselves.

10. Technology trend: establishing a SonicWALL® Clean VPN™

A "clean VPN" approach establishes intelligent layers of secure remote access, gateway firewall, and policy control by integrating SSL VPN and Unified Threat Management (UTM). To be practically effective, a clean VPN must be able to:

Detect the integrity of users, endpoints and traffic from beyond the traditional network perimeter.

Protect applications and resources against unauthorized access and malware attacks.

Connect authorized users with appropriate resources seamlessly and easily in real time.

SonicWALL® has strategically positioned itself as an industry leader in pioneering clean VPN technology solutions for organizations of all sizes by enabling the managed integration of its award-winning Secure Remote Access, Network Security Appliance and Global Management System product lines. The SonicWALL Clean VPN™ solution unites next-generation SSL VPN and UTM technologies to enforce granular application-layer access policies while comprehensively inspecting all traffic at the gateway, while simultaneously correlating event information to streamline and enhance security efficiencies.

Conclusion

The technology enablers of telecommuting include reliable secure remote access, wider access to broadband Internet, new collaborative applications, and the popularity of PDAs and smartphones, as well as heightened public awareness of global warming and the original push from employees seeking better balance between their work and family lives. Trends in both business and technology are increasingly making telecommuting a reality.

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS®

How Can I Learn More?

- Download the Whitepaper "10 Telecommuting Trends"
- Download the Whitepaper "Teleworking and the New Economy"
- Opt-in to receive SonicWALL Newsletters

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an e-mail to **feedback@sonicwall.com.**

Forward to a Friend

About SonicWALL

SonicWALL® is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high-performance business network. For more information, visit the company Web site at **www.sonicwall.com**.

[1] Anne C. Ruddy, president, WorldatWork (August 2008)
[2] "Hot desking," Wikipedia, (http://en.wikipedia.org/wiki/Hot_desking).
[3] The Dice Report, June 2008.
[4] Federal Trade Commission - Identify Theft Survey Report (September 2003)
[5] "Call Centers Come Home," HR Magazine, January 2007.
[6] Broadband Services: Economic and Environmental Benefits, American Consumer Institute, 2007.
[7] Gartner press release, July 24, 2008. Leichtman Research Group puts U.S. penetration at 53%, Leichtman, press release June 25, 2008.
[8] Mark Bouchard, Missing Link Security Services
[9] Information Week (July 2007)
[10] Information Week (February 2008)