Top 10 trends in telecommuting

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

DELL Software

Table of contents

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.

IT has traditionally had the option to lock down laptop operating systems to prevent the installation of potentially insecure or non-approved applications. Today, though, employees demand the same freedom-of-technology at work as they have in their personal lives. This consumerization of IT (as well as the budgetary incentive of offsetting inventory costs) has led companies to establish "bring your own device"

(BYOD) policies that enable employees to select their own personal mobile devices for use at work. The phenomenal popularity of consumer smartphones and tablets—most notably iOS and Google® Android™ devices—has positioned these devices as powerful platforms for mobile business and academic computing.

Whether driven by hard or soft benefits, telecommuting programs have one core requirement: give mobile employees 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.

> About one in five workers around the globe, particularly employees in the Middle East, Latin America and Asia, telecommute frequently, and nearly 10 percent work from home every day.[1]

1. Business trend: Reining 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.

The Canadian Telework Association (CTA) puts some numbers to the "hot desking" phenomenon, 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) through 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.

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

2. Business trend: Finding and retaining talent

Economic conditions such as inflation, rising gas prices, military relocations, and the housing downturn are affecting many workers and their families. According to a study by the Bureau of Labor Statistics in 2010, over 5 million individuals worked at home at least twice per month[3]. 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. A 2011 study on Canadian employees by the Telework Research Network found that telecommuting enhances attraction and retention, and is among the top non-financial benefits desired by employees[4]. By reducing job turnover, employers also eliminate costs of training new hires.

One organization found annual attrition rates drop 3 percent among teleworkers, with 90 percent of respondents indicating the telework program had influenced them to stay.[5]

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.

The mobile workforce is not excluded from these compliance mandates, so the viability of a telecommuting program requires having technology in place that monitors both 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

$37,000,000,000

Approximately 8.1 million Americans learned that they were victims of identity fraud in 2010, at a cost of $37 billion.[6]

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 companies to outages that affect their outsource partners.

By definition, telecommuting distributes employees away from central offices that 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.

During February 2010 snowstorms, teleworkers at the U.S. Patent Trademark Office attained higher performance rates than in the previous quarter, and kept up 85 percent productivity while other government departments had to shut down.[7]

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. A 2011 Telework Research Network study reports that twice-weekly telework by Canadian workers could save 5.2 million barrels of oil[8].

Studies have estimated a ten year savings of 312.4 million tons of greenhouse gas emissions.[9]

6. Technology trend: Accessing broadband everywhere

As the number of homes with broadband Internet access grows, working from home has become 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.
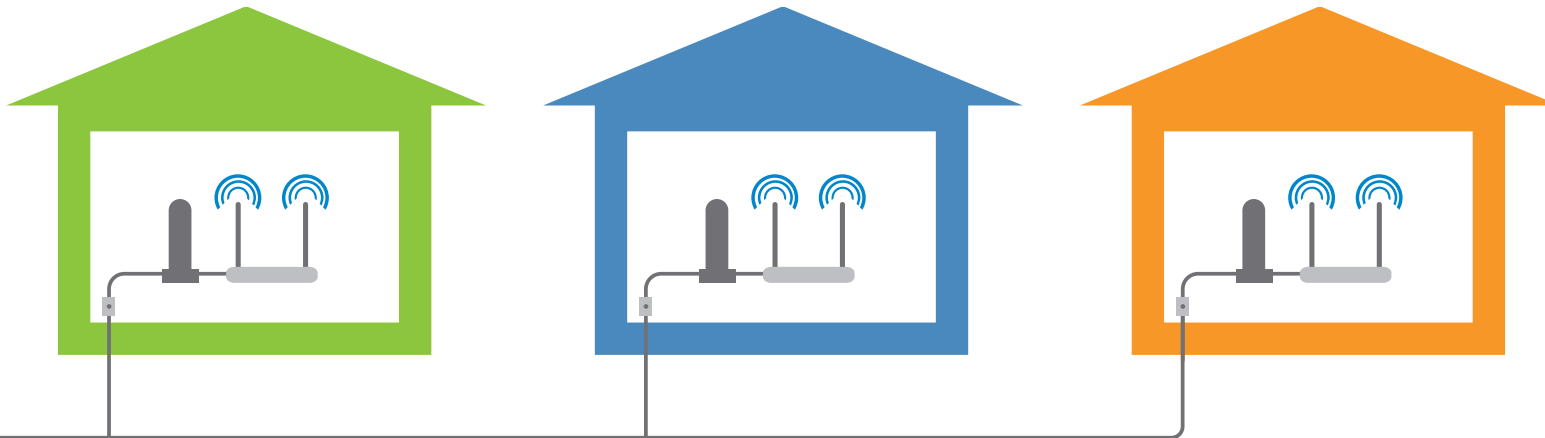
7. Technology trend: Collaborating via Web 2.0

Applications such as Microsoft Sharepoint and Live Meeting 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, despite bandwidth and time-based restrictions.[10]"

8. Technology trend: Consumerization of IT

The consumerization of IT means that most new technologies enterprises currently adopt for their information systems have roots in consumer applications. Falling prices and greater horsepower of consumer smartphones (e.g., Apple® iPhone®, Google Android and Windows® Phone 7), and tablets as well as laptop computers, have put the technology of telecommuting within the reach of many organizations and their workers.

ZDNet reports that one survey found that 24 percent of employees now use a personal smartphone, and 10 percent a tablet, to access or store corporate data, but that data is encrypted for only one third of these devices. Smartphones and tablets issued by corporate IT typically are more likely to be configured to access the corporate network securely. However, most of these devices are typically owned by the employee and then used to access the company network for work. Consumer devices open corporate networks to new threats, not the least of which is that small devices are easier to lose than larger ones. Moreover, applications on these devices can act as a conduit for threats, sap productivity and consume available bandwidth, and so they must be controlled. Plus, IT departments are responsible for smartphones and tablets despite not having control over them.

One study found 51 percent of organizations had experienced data loss due to poorly secured mobile devices.[11]

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 Dell SonicWALL Clean VPN

A Clean VPN approach establishes intelligent layers of secure remote access, gateway firewall, and policy control by integrating SSL VPN and Next-Generation Firewalls. 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.

Dell™ 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, Next-Generation Firewall and Global Management System product lines. Dell SonicWALL Clean VPN™ delivers the critical dual protection of SSL VPN and high-performance

Next-Generation Firewall necessary to secure both VPN access and traffic. The multi-layered protection of Clean VPN enables organizations to decrypt and scan for malware on all authorized SSL VPN traffic before it enters the network environment. Dell SonicWALL Clean VPN supports Apple Mac OS®, iOS, Linux®, Google Android, Microsoft Windows, Windows Phone 7 and Windows Mobile platforms.

Conclusions

The technology enablers of telecommuting include reliable secure remote access, wider access to high-speed broadband Internet, new collaborative applications, and the popularity of smartphones and tablets, as well as escalating gas prices 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.

How can I learn more?
• Download the Whitepaper "Controlling Laptop and Smartphone Access to Corporate Networks"
• Opt-in to receive Dell SonicWALL newsletters

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

Forward to a friend

About Dell SonicWALL
Dell™ SonicWALL™ provides intelligent network security and data protection solutions that enable customers and partners to dynamically secure, control, and scale their global networks. Securing any organization with multi-threat scanning based on global input at wire speed, Dell SonicWALL is recognized as an industry leader by Gartner and NSS Labs. For more information, visit the web site at **www.sonicwall.com**.

[1] Ipsos/Reuters poll, Jan. 2012
[2] "Hot desking," Wikipedia, (http://en.wikipedia.org/wiki/Hot_desking).
[3] Source: http://www.mobilitychoice.org/MCtelecommuting.pdf (pg. 3, Fig. 1)
[4] Source: http://www.teleworkresearchnetwork.com/wp-content/uploads/2011/04/Telework-Canada-Final5.pdf (pg. 12)
[5] 2011 Identity Fraud Survey Report, Javelin Strategy & Research
[6] Federal Trade Commission - Identify Theft Survey Report (September 2003)
[7] "2012 Status of Telework in the Federal Government," Kate Lister & Tom Harnish, June 2011
[8] Source: http://www.teleworkresearchnetwork.com/wp-content/uploads/2011/04/Telework-Canada-Final5.pdf (pg. 20)
[9] "Broadband and telecommuting: Helping the U.S. environment and the economy," Fuhr & Pociask, 2011
[10] Mark Bouchard, Missing Link Security Services
[11] "BYOD: How to avoid Bring Your Own Danger," ZDNet, May 31, 2012

DELL Software