Risk at home:

privacy and security risks in telecommuting

Presented by:

Ernst & Young
Quality In Everything We Do

Center For Democracy & Technology

Contents

Executive summary

It is difficult enough to secure a corporate network with the constant and persistent threat from malicious external parties, from hackers to spammers to viruses.

But for the chief technology officer or chief risk officer of today's organization, perhaps no issue presents more complexity — or more headaches — than the necessity to protect corporate and personal information in an environment where employees travel widely or routinely work at home, using personal computers, laptops, non-corporate owned machines and personal digital assistants (PDAs).

This challenge is only growing, as organizations increasingly offer employees the option of working remotely, from the comfort of their homes or even from the local coffee shop. According to a 2007 Gartner report, the number of individuals worldwide working at least one day a week from home is expected to grow at a compound annual rate of about four percent and will reach over 46 million by the end of 2011.

Developed as a way to manage fixed-asset costs (i.e., to lower the physical office footprint for corporations) and as a means to attract and retain talent by allowing flexible work schedules, corporate work-from-home arrangements can be part of formal telecommuting programs or can emerge ad hoc as employees engage in various activities based on need and opportunity. With the astonishing proliferation of such work arrangements and the portability of technology assets, added to the ease of access to remote or locally hosted memory devices, the result is a business challenge that not only has the CTO awake at night, but has also reached as far as the C-suite and the corporate boardroom.

Privacy and security are the watchwords

Privacy and security risks outside the office are not new. Even before the advent of the Internet, employees routinely took work with them when they went home or on the road. But with the migration to electronically stored information and network computing now almost universal — from *Fortune* 500 businesses to small, family-owned businesses and so-called "virtual organizations" — information management, protection and personal security have become more complex by orders of magnitude. Rapid, easy access to networked information has become an

expectation of employees as they travel; and use of the internet — via a secure connection or not — to transfer data and/or access applications or information on corporate servers has become the norm.

As a consequence, ensuring the privacy and security of not only corporate data but also of personal information — especially the large amounts of data now stored on corporate networks about large groups of individuals — has become paramount. Press reports of information lost in transit — including data tapes, hard drives and laptop devices storing personal information on hundreds of thousands of individuals — have become more frequent. Both private corporations and government entities have come under fire for lax data protection measures.

In short, to protect employees, their customers or constituents and their own reputations, organizations must now focus directly on privacy and security issues. And while protecting data in transit is an issue that can be addressed with some straightforward measures — including increased monitoring, security and improved controls, a challenge more pressing is the protection of personal information, as literally millions of people, daily, weekly or otherwise, are telecommuting to work.

Ernst & Young and the Center for Democracy & Technology survey privacy and security risks

In late 2007, in partnership with Ernst & Young LLP, the Center for Democracy & Technology (CDT) surveyed organizational practices, policies and approaches concerning telecommuting. Mindful that this type of working arrangement is becoming the norm for a growing number of employees, the survey, "The State of Telecommuting: Privacy and Security," was developed to help understand the current state of work-from-home arrangements at a range or organizations, as well as to identify leading practices and areas of weakness.

While different situations present different challenges — for example, an employee who works from home full-time presents different challenges from the distracted business traveler who leaves a laptop unattended in an airport lounge — our survey focused on specific policies, practices, and risks in work-at-home arrangements, which have received comparatively less attention than the well-publicized data losses that have been noted in the media in recent months. Survey questions were designed with both companies and government organizations in mind, ranging from hiring processes for work-from-home employees to the technical and physical controls associated with the work environment and to employers' monitoring of telecommuters activities while online.

A diverse group of 73 organizations from 10 industries in the US, Canada and Europe responded to the joint CDT and Ernst & Young survey by answering close to 60 questions. Each participating organization submitted one completed survey, often developed from responses from multiple respondents within the organization. Approximately half of survey respondents are on the Fortune 1000 list including 20% of the Fortune 100, and company size ranges from over 100,000 to fewer than 20 employees.

Telecommuting risk often ignored, survey shows

One key finding of the survey that should be of concern to the C-suite: survey responses indicate that, while companies are aware that telecommuting is an area of risk, the topic is often sidelined. This suggests that risk issues that evolve over time, such as the growth of the frequency of telecommuting, do not attract the same amount of attention as do more immediate risks and challenges, such as the types of data losses that have recently prompted headlines and regulatory inquiries.

Another concern is the lack of corporate ownership for managing privacy risk. Respondents noted that the practice of telecommuting cuts across departmental boundaries — with varying responsibilities shared by human resources, information technology, security or privacy departments — and respondents suggest that this lack of clear ownership presents an obstacle in assigning responsibility to address what gaps remain in the protection of personal information, especially when employees handle data outside the more controlled environment of the office.

Another surprising finding in the survey was the lack of formal policies, operational procedures or training in place to educate their employees about the risk of data loss or to prevent or mitigate the risk of breaches of privacy or

security regarding personal information. Fully half of organizations surveyed have no such policies or training, even though they allow telecommuters to handle data that includes other people's personal information when working from home.

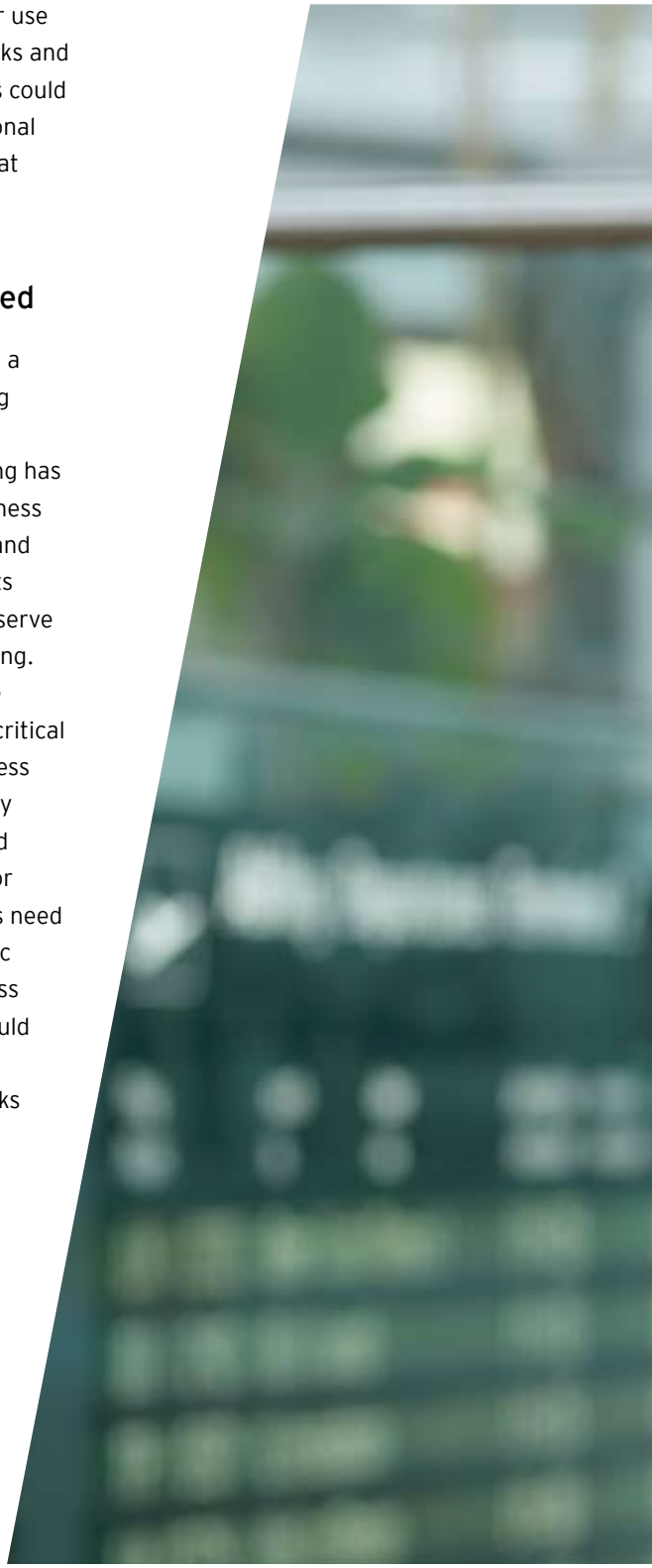
Moreover, there appears a marked lack of consistency in background screening of employees, temporary employees and contractors who telecommute and who are given access to other individuals' personal information. And while organizations consider the physical protection of the computers they provide to their telecommuters, they often neglect to consider how to protect the paper records that telecommuters generate.

The survey also included various questions relating to technology, to learn what software and hardware tools organizations currently deploy and what controls are commonly used to protect information. While many respondents have hundreds or thousands of employees who telecommute and handle personal information, results show the deployment of privacy-enhancing technologies that could be beneficial in the telecommuting setting, especially when dealing with very sensitive information (such as security software for identifying users, biometric controls for login and thin-client terminals) have yet to take hold.

Another finding is the overall weakness in monitoring compliance with key technology-related policies, especially when telecommuters use their own home computers for work purposes. Common privacy and security practices are often lacking with regard to telecommuter use of portable devices, wireless networks and internet downloads; such oversights could lead to the compromise of the personal information that employees handle at home.

Conclusion: privacy and security need to be revisited

Organizations across the board face a dilemma in developing and enforcing controls on the use and security of personal information. Telecommuting has become an inescapable part of business life, but many of the policies, tools and controls that our survey respondents described as in use are intended to serve broader purposes than telecommuting. Such policies, tools and controls are therefore likely to overlook certain critical gaps in how companies should address specific issues, such as those privacy and security risks that are presented by the unique conditions of formal or informal telecommuting. Companies need to develop and communicate specific policies, tools and controls to address the telecommuting process and should implement appropriate methods to monitor the privacy and security risks of these arrangements.



About this survey

Given the widespread adoption of telecommuting by corporations and their employees, and given the continually increasing privacy and security risks that have accompanied the development and dispersion of information technologies worldwide, the benefits and challenges of telecommuting require organizations to address privacy and security directly.

Ernst & Young and the Center for Democracy & Technology (CDT) recognize this risk. In late 2007, CDT and Ernst & Young LLP jointly designed and conducted a survey of corporate practices regarding telecommuting. The survey was publicly announced and made available on the CDT's website from December 2007 to January 2008 to any organization interested in participating; it can be viewed at http://www.cdt.org/privacy/20071206wfhsurvey.doc.

Our joint survey was intended to help identify the current state of work-from-home arrangements, as well as leading practices and areas of weakness. It was designed to identify telecommuting practices at both companies and government organizations, and addressed various aspects related to the work-from-home environment — from the hiring process to the technical and physical controls associated with the work environment to how employers monitor telecommuters' activities. The survey distinguished between employees who predominantly work from home (referred to as "full-time telecommuters"), and employees who only work remotely on occasion (referred to as "occasional telecommuters").

In reporting our results, we divided responses into two broad categories. The first category, ***Process and Risk***, addresses the policies and practices that organizations have developed around telecommuting privacy and security. The second, ***Technology Controls and Solutions***, deals with the technology that telecommuters use at home and how technology is used to secure their work-from-home environments.

About the organizations that responded to the survey

Survey respondents comprised a diverse group of 73 organizations in the US, Canada and Europe. About half of the respondents were representatives from *Fortune* 1000 companies: fifteen were *Fortune* 50 companies, five were *Fortune* 100 companies, twelve were *Fortune* 500 companies, and another five were *Fortune* 1000 companies. The sizes of the organizations ranged from over 100,000 employees to only a handful; the average number of employees at companies in the sample was approximately 50,000 with a median of 4,000.

We identified ten industries among our respondents. Financial services and healthcare were the two industries most represented, comprising 40% of all respondents. Others included business and professional services, government, technology, manufacturing, retail, telecommunication, hospitality and a miscellaneous category for those participants that did not neatly fall within these industries.

As diverse as the group of respondents was, we should also point out that we do not believe that our survey sample is entirely representative of the marketplace as a whole. With the overwhelming majority of participating organizations employing dedicated privacy and security resources and using a data classification policy to guide their data protection operations, our survey respondents appear to be ahead of the curve in their general approach to governance and their awareness of risk. Based on how the state of telecommuting is reflected in this survey, one can reasonably expect "softer" privacy and security practices in organizations where these considerations are not represented in governance and overall awareness.

At the organizations of some respondents, nearly all employees are occasional telecommuters, representing thousands and even tens of thousands of employees. Many respondents found it difficult to estimate the number of their full-time and occasional telecommuters — an interesting finding on its own.

Nonetheless, we did note that the number of full-time telecommuters is significantly smaller than the number of occasional telecommuters. While occasional telecommuters exist at each of the responding organizations, 46 of the 73 respondents employ full-time telecommuters. A total of thirteen respondents were at organizations with 500 or more employees who are full-time telecommuters; at some of these organizations, the number of telecommuters is in the thousands.

Survey highlights

The following key observations are discussed further in this survey report.

Process and risk considerations in telecommuting:

- Most respondents allow employees to handle personal information at home, but only half indicated they have both developed guidelines for telecommuting and provided guidance to their employees on the topic.
- While telecommuting could increase the risk of inappropriate use of personal information, organizations do not typically develop credentialing practices that address varying levels of risk as determined by the employee job function.
- Temporary employees and contractors frequently handle personal information while telecommuting; however, organizations vary widely in how they address this situation.
- Most organizations allow telecommuters to use paper records containing personal information, but the protection of those records is not commonly addressed.
- Security considerations for telecommuter computers used at home are common, but protective policies and mechanisms do not commonly address all prevalent threats.

Technology controls and solutions for telecommuters:

- Telecommuters commonly use their own personal computers and PDAs at home for work purposes. Few organizations have adopted privacy-enhancing devices such as thin-client terminals for employees who commonly telecommute.
- Few organizations limit the use of peripheral devices; even fewer monitor compliance with those requirements.
- File and email encryption tools are commonly used by survey respondents' companies, but still have much lower adoption rates than firewalls and anti-virus software.
- The use of encryption is prevalent when connecting remotely to internal networks, such as through secure virtual private networks (VPNs).
- Hard drive encryption is common, but of little help when employees use their home computers for work.
- Biometric technology has yet to become more than sparsely adopted.
- Most telecommuters connect to the Internet using a consumer-class broadband connection.
- Allowing telecommuters to use wireless Internet connections is a common practice, but requiring that telecommuters use wireless security measures is less common.
- Limitations on downloading software and using peer-to-peer file-sharing applications are common but not prevalent.
- Although personal information can easily leave the organization via email, limitations on telecommuters regarding the use of email and external email services are not common.
- Email encryption solutions are common among our respondents, but telecommuters frequently use home computers on which such solutions are not installed.
- The higher the number of telecommuters in an organization, the more likely the organization monitors those telecommuters' use of tools and technology.

The state of telecommuting: privacy and security survey results

Organizations increasingly offer employees the option of working remotely from the comfort of their homes. Such arrangements can be part of formal telecommuting programs or ad hoc activities that employees engage in based on their individual needs and the opportunity afforded them by their employers. In fact, telecommuting is a category measured by *Fortune* magazine when developing its annual *Best 100 Companies to Work For*[1] list. According to a 2007 Gartner report, the number of individuals working at least one day a week from home is expected to reach 46.6 million by the end of 2011.[2]

Organizations use telecommuting for different purposes. Some require it to maintain and constantly monitor their business continuity plans. Others treat it as a means for retaining and attracting employees. Some organizations have even created customer service positions (once traditionally situated in call centers) to operate out of employee homes. Under some telecommuting models, employees may be hired, trained and begin work without ever stepping in the organization's office or even physically meeting with its representatives.

Privacy and security remain important considerations any time that employees access and use organization data, which includes personal information in their homes or other remote locations. In many ways, privacy and security considerations outside the office are far from new issues. Even before the advent of computers and the internet, employees traveled on business and took work home. Nonetheless, today's work environments — combining both quick access to large amounts of data and the employees' increased expectations of being able to work remotely — bring this topic to the forefront of executive concern.

Privacy and security risks in telecommuting

The risks associated with taking work outside the office are not new. As noted above, even before telecommuting became a topic of discussion in the context of privacy and security, business travelers have been made aware of risks such as:

- Physical loss or theft of information or the devices that contain information
- Inappropriate access by strangers to information that was left unprotected by the employee
- Communicating information through unprotected channels

Telecommuting adds additional considerations to those associated with business travel as employees create for themselves an office away from the office.

Such risks include:

- Printing information without appropriate disposal options
- Accessing or loading information on unprotected home devices
- Allowing non-employees (family members, for example) access to devices for personal use (an increasing area of concern that was confirmed recently by a study conducted by Cisco[3])
- Inappropriate access to information by non-employees residing with the telecommuter who learn to overcome security features (e.g., passwords that are stored in an unsecured manner)
- Lack of privacy and security policies to guide telecommuters
- Lack of compliance with policies and procedures that address telecommuting

Disgruntled employees or those otherwise interested in abusing their ability to access information add yet another layer of risk. Telecommuting provides such employees with an environment more open to destructive actions, such as purposefully extracting and inappropriately sharing information, and/or changing and manipulating hardware and software to overcome security controls.

[1] In 2007, 84 of the Best Companies to Work For allowed employees to telecommute at least 20% of the time.
[2] Gartner, Inc. "Dataquest Insight: Teleworking, The Quiet Revolution (2007 Update)" by Caroline Jones, May 14, 2007.
[3] "How Remote Workers Heighten Security Risks for Businesses, IT Organizations, and Themselves," Cisco Systems, 2007.

Process and risk considerations in telecommuting

Organizations institute a variety of policies and procedures to address and mitigate the risks presented by telecommuting. This section examines our survey findings relating to those policies and procedures.

Respondents indicated that, while organizations are aware that telecommuting is an area of risk, the topic has often been sidelined for different reasons. Based on survey responses, it would appear that business risks which evolve gradually over time, including the privacy and security risks related to telecommuting, do not always get the same level of attention that new, more pressing challenges do. In other cases, respondents noted that the multidisciplinary nature of telecommuting oversight within the organization — a task which could be assigned to the HR, IT, security or privacy departments — proved to be an obstacle in assigning responsibility to address it.

Survey respondents confirmed these challenges even further. While we found that many organizations allow telecommuters to handle personal information at home, only half of the respondents seek to address the risk entailed by such practices with formal policies and training. Background screening of employees, temporary employees and contractors who handle personal information while telecommuting also lacks consistency. Furthermore, while organizations consider the physical protection of the computers they provide to their telecommuters, they often neglect to consider how to protect the paper records that telecommuters generate.

Standards and guidance

Most respondents allow employees to handle personal information at home, but only half indicated they have both developed guidelines for telecommuting and provided guidance to their employees on the topic.

Survey participants were asked about the standard policies, procedures and guidelines that their organizations have developed to address telecommuting. While two-thirds of the respondents indicated that they have such standards, in some cases that response referred to general policies for computer use that cover mobile devices for all employees, not specifically for telecommuters. The protection of mobile devices is relevant not only to telecommuters but also to business travelers, and even to those working in the office.

However, these policies do not commonly tackle many risks specific to telecommuting, such as loading and/or transferring data onto home devices and access to information by non-employees in the household who have access to such equipment. Furthermore, while 84% of respondents indicated that they allow employees to handle personal information at home, close to 20% of these organizations do not have policies or procedures in place that address telecommuter hardware and software use. In other cases, telecommuting-specific standards address full-time telecommuters only.

Even when organizations have telecommuting privacy and security policies in place, they face challenges in raising employee awareness of the policies. Survey comments indicate that it is not out of the ordinary for organizations to develop telecommuting policies and post them on their intranets without doing anything else to effectively alert employees of their existence.

One goal of the survey was to ascertain whether organizations have been providing guidance (e.g., awareness programs, training) to their employees about privacy and security when telecommuting. A recent study by Bentley College of over 1,000 US employees affirms the importance of training. In the Bentley survey, employees who had undergone security training were significantly more aware of computer security threats and more confident in their abilities to secure their home computing environments.[4]

When it comes to providing such guidance to employees, more effort has been focused on full-time telecommuters than on occasional telecommuters or business travelers. However, even with the broader population of employees, over half of survey respondents (60%) indicated that some guidance (e.g., general privacy and security training) is provided to employees who telecommute at least occasionally. Of the 61 respondents that allow their employees to handle personal information at home, more than 20% do not provide any guidance on maintaining security or privacy of personal information when telecommuting.

[4] Culnan, Professor Mary J., Bentley College; Foxman, Ellen R., Bentley College; and Ray, Professor Amy, Bentley College, "Locking the Barn Door after the Data are Gone: The Role for the IT Executive in Employee Home Computer Security," MIS Quarterly Executive, January 2008.

Practices to adopt	Practices to avoid
▸ Developing telecommuting-specific policies and guidance that address the organization's specific needs and risks ▸ Identifying those employees who should become aware of telecommuting policies and providing them with relevant guidance	▸ Guiding and training only full-time telecommuters, or not providing guidance at all ▸ Using general acceptable-use policies in place of telecommuting policies ▸ Training that only broadly addresses working from home and that does not delve into specific risks and practices that apply to both occasional and full-time telecommuters ▸ Developing policies, but not communicating them effectively to the relevant employees

Employee credentialing

While telecommuting could increase the risk for inappropriate use of personal information, organizations do not typically develop credentialing practices that address varying levels of risk as determined by the employee job function.

Employee credentialing questions were included in the survey to assess the "insider threat" – that is, employees' abuse of their familiarity with the business and access to systems for unauthorized and inappropriate actions. A common approach to addressing the insider threat is to conduct criminal background reviews and to confirm employees' representations of themselves, such as on job applications and in resumes.

While telecommuting could provide more opportunities for inappropriate use of personal information, it does not seem to be a factor in employee credentialing. We noted variations across responses and found some trends, but they do not relate to whether employees work outside the office. In fact, credentialing of employees appears to vary even within an organization based on business unit and geography, including state-level differences.

Employee credentialing is predominantly done prior to employment. Verification of employment history and criminal background checks are the most common. In both cases more than 75% of respondents perform these activities prior to employment, but only 15% continue to perform them periodically during employment. Credit checks are less common, with only about 51% of respondents performing them prior to employment and only 11% performing them periodically during employment. In the financial industry, more respondents use credit checks than do companies in the other industries. Drug tests are the least common, with about 44% of respondents conducting them prior to employment, but only 14% of those respondents conduct them prior to and periodically during employment. The financial and healthcare industries also have the highest percentage of organizations, together over 50%, that repeat some of the credentialing procedures used to pre-screen employees after they are employed.

Practices to adopt	Practices to avoid
▸ Credentialing employees based on risk, including employee access to information and the organization's ability to monitor the employee activities	▸ Following a cookie-cutter approach to employee credentialing that does not consider risk to the organization based on employee access to information
▸ Repeating the credentialing to identify possible changes in background or changes in the employee position	▸ Applying inconsistent credentialing across business units without having a privacy or security rationale for doing so

Temporary employees and contractors

Temporary employees and contractors frequently handle personal information while telecommuting; however, organizations vary widely in how they address this situation.

Our survey questions regarding temporary employees and contractors focused on whether the organizations allow these groups to telecommute with the organization's data, and with personal information in particular, as well as whether these groups undergo background checks similar to those for employees.

The answers we received to these questions varied widely. The majority of respondents allow either of these groups to telecommute with organization data, and about half allow one of these groups to do so with personal information. Similarly, about half of the respondents require temporary employees and/or contractors to undergo similar background checks as employees do.

Based on the comments provided by respondents, it is evident that many organizations have yet to thoroughly consider this issue; several indicated that they are only now starting to address it. While some apply requirements to temporary employees and contractors based on the task and risk, other responses showed an overall lack of clarity on the issue, reliance on agencies or the contractor companies to apply reasonable requirements or variations in approaches across business units.

Practices to adopt	Practices to avoid
▸ Applying and ensuring that the credentialing requirements for telecommuting temporary employees and contractors are risk-based and aligned with those applied to telecommuting employees of the organization	▸ Allowing temporary employees and contractors to telecommute with personal information without aligning their credentialing to the organization requirements

Paper records management

Most organizations allow telecommuters to use paper records containing personal information, but the protection of those records is not commonly addressed.

Nearly 75% of organizations say that they allow telecommuters to generate paper records containing personal information. This includes transcribing personal information onto notepads or forms, printing or faxing personal information and bringing paper records containing personal information home from the office.

However, when it comes to the protection of these records, survey comments suggest that paper records management is not a common component of privacy and security policies. Only 25% of respondents said their organizations have telecommuters store paper records in secured cabinets or other storage systems that the organizations themselves provide. A slightly larger percentage indicated that they require telecommuters to store records in secure cabinets, but the employees must arrange for the cabinets themselves. One quarter of respondents told us that telecommuters are required to send paper records back to the organization. And 15% of the organizations said they have no requirements in place regarding storage of paper records.

There also appeared to be no single common disposal method used across organizations for telecommuters' paper records. One-third of organizations surveyed said they provide telecommuters with shredders for disposal. Roughly the same percentage said they have telecommuters shred paper records, but the employees must arrange their own shredders. And 17% of the organizations indicated that they have no disposal requirement for paper records.

Practices to adopt	Practices to avoid
▸ Providing telecommuters with clear guidance on the use and disposal of paper records containing personal information ▸ Providing full-time telecommuters with cabinets and shredders before allowing them to handle paper records with personal information ▸ Minimizing the use of paper records in general and the amount of personal information in such records in particular	▸ Relying on telecommuters to figure out on their own what the appropriate practices are when it comes to creating, handling and disposing of paper records with personal information at home

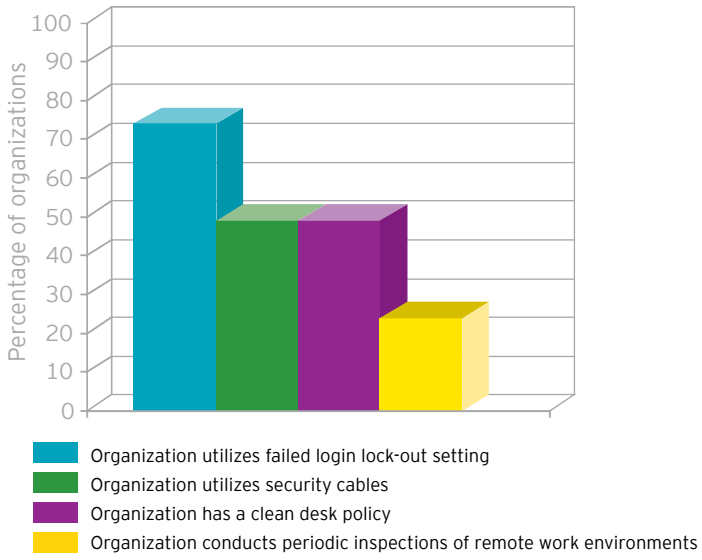
Securing hardware

Security considerations for telecommuter computers used at home are common, but protective policies and mechanisms do not commonly address all prevalent threats.

We asked respondents about the use of five different security measures: failed login lockout settings on computers, privacy screens, security cables for locking down computers, periodic audits of telecommuter physical working environments and whether the organizations have a clean desk policy for telecommuters.

About 85% of organizations indicated they implement at least one of these measures. Failed login lockout settings are the most common, particularly among government respondents. Slightly less than half of respondents use security cables and apply clean desk policies.

Approximately 20% of organizations said they conduct periodic inspections of telecommuter remote work environments. Survey results show the rate of these periodic inspections is correlated to the number of telecommuters. The higher the number of telecommuters, the more likely the organization is to conduct such inspections.



Practices to adopt	Practices to avoid
▸ Identifying the most relevant physical security requirements for your telecommuting employees, providing them with the tools and monitoring compliance with the requirements ▸ Conducting house visits to ensure full-time telecommuters who handle personal information are meeting the requirements	▸ Requiring security measures to be applied, but relying on telecommuters to purchase the items themselves ▸ Relying on telecommuters to figure out on their own what the necessary security mechanisms are

Technology controls and solutions for telecommuters

Respondents were asked a variety of technology-related questions in an attempt to understand the software and hardware tools that organizations deploy and the controls that organizations commonly apply to protect information. Data shows that, while many respondents have hundreds or thousands of employees who telecommute and handle personal information, deployment of privacy-enhancing technologies that are especially beneficial in the telecommuting setting, such as biometric controls and thin-client terminals, has yet to take hold. The survey also reveals common challenges related to telecommuter use of home computers for work purposes and an overall lack of monitoring of telecommuter compliance with key technology-related policies.

On a more positive note, the use of encryption, while not yet prevalent, is common on hard drives, in securing network connections and even in protecting email messages. With regard to telecommuter use of portable devices, wireless networks and internet downloads, common practices are often lacking and could lead to the compromise of the personal information that employees handle at home.

Devices used by telecommuters

Telecommuters commonly use their own personal computers and PDAs at home for work purposes. Few organizations have adopted privacy-enhancing devices such as thin-client terminals for employees who commonly telecommute.

Organization-issued devices that telecommuters use are mainly laptops (74%) and PDAs (60%) for both full-time and occasional telecommuters. Issuing desktops to full-time telecommuters is less common (16%), and only 8% of organizations issue thin clients (computer terminals with no memory or disk), mainly to full-time telecommuters.

About 50% of respondents indicated that telecommuting employees, both full-time and occasional, sometimes use their own personal computers and PDAs at home for work purposes. While some respondents indicated that such a practice is clearly prohibited in their organization, others indicated that their organization is looking to ease this limitation and allow it.

While many organizations encrypt the hard drives of organization-issued devices (as discussed below in a subsequent section), no similar requirements or considerations apply to the use of employees' own devices. In fact, responses to the different parts of the survey show us that organizations allow the handling of personal information at home, are aware and in some cases allow telecommuters to use their own computers, but apply practices such as hard drive encryption only to organization-issued devices.

Practices to adopt	Practices to avoid
▸ Providing thin clients or other privacy-enhancing devices to employees who frequently work from home ▸ Prohibiting employees from using home computers without having installed information security mechanisms stipulated by the organization, and before clear policy and guidance are provided to them ▸ Providing employees with the necessary security mechanisms to be installed on home computers ▸ Prohibiting processing and storing the organization's personal information on home computers	▸ Allowing the use of peripheral devices for the processing and transfer of personal information without clear guidance and effective information security

Peripheral device management

Few organizations limit the use of peripheral devices; even fewer monitor compliance with those requirements.

Respondents were asked whether their organization prohibits telecommuters from using nine different kinds of peripheral devices: USB drives, other portable storage devices (like external hard drives), printers, scanners, fax machines, removable disks (like DVD-RW and CD-RW), web cameras, microphones and media players. Although many of these devices can store personal information digitally, only 25% of organizations prohibit them altogether or require that the data they contain be encrypted. Such requirements typically apply only to USB drives, other portable storage devices and removable drives.

Only half of the organizations that said they prohibit some type of peripheral device also indicated that they conduct monitoring that would allow them to verify that such devices are not in use. These types of monitoring include remote access into employee computers and visits to the home worksite.

Practices to adopt	Practices to avoid
▸ Providing security tools such as encryption when allowing the use of peripheral devices for the transfer of personal information ▸ Monitoring compliance with peripheral device policies	▸ Allowing the use of peripheral devices for the processing and transfer of personal information without clear guidance and effective information security

Encryption technology

File and email encryption tools are commonly used by survey respondents' companies, but still have much lower adoption rates than firewalls and anti-virus software.

The security features that are installed on the computers used for working from home do not differ between full-time and occasional telecommuters. Most common are firewalls (91%) and anti-virus applications (95%). Following these are anti-spyware programs (78%), file encryption software (63%) and email encryption software (49%).

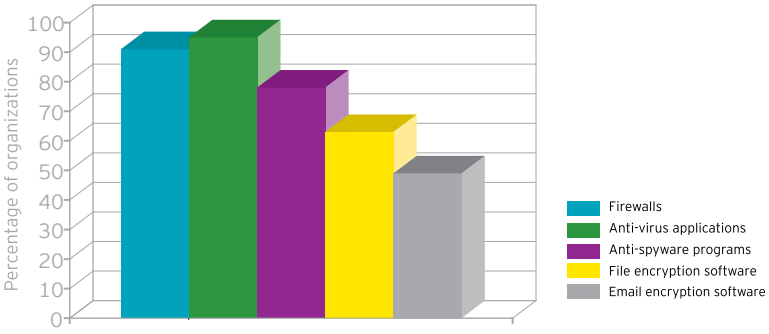
For the 49% of companies that use email encryption software (either computer or network-based options), there seems little distinction between the use of these tools by full-time and occasional telecommuters, and there is no indication that the number of telecommuters an organization employs affects the use of these tools. Of note, however, is that close to 70% of the companies with a Fortune designation have implemented these tools. The importance of file and email encryption is further compounded by the risks of using unsecured wireless networks, as noted in a later section.

The use of encryption is prevalent when connecting remotely to internal networks, such as through secure virtual private networks (VPNs).

A majority of organizations (86%) indicated they use encryption to secure telecommuter connections to internal networks, such as through a secure virtual private network (VPN). Only 3% of organizations prohibit remote access to internal networks altogether. More interestingly, while the use of encryption is common for remote networking, only 36 organizations (about half) require that their employees use some form of wireless security measure when connecting wirelessly at home (see the Internet Connectivity section of this report).

Hard drive encryption is common, but of little help when employees use their home computers for work.

Just over half of the respondents indicated that their organizations require hard drive encryption on organization-issued devices. However, telecommuters at about half of the responding organizations are allowed to use their home computers for work, where similar encryption requirements may not apply. Further, the processes that organizations follow to identify the devices to encrypt vary widely. Some encrypt all laptops and apply encryption to desktops that contain information they define as sensitive. Others limit hard drive encryption only to the devices that employees identify as containing the information designated for that level of protection. A third group avoids full drive encryption altogether and provides file or folder encryption tools to employees who use certain information categories.



Practices to adopt	Practices to avoid
▸ Providing telecommuters with file and email encryption tools and instructing them on the proper use of the tools ▸ Applying encryption on all devices used by telecommuters that may contain personal information ▸ Using encryption to secure remote connections to the organization network	▸ Expecting employees to identify whether they need to use encryption tools ▸ Providing folder or file-based encryption in lieu of full drive encryption without guiding and training employees on the proper use of those tools or monitoring their compliance with related requirements

Authentication

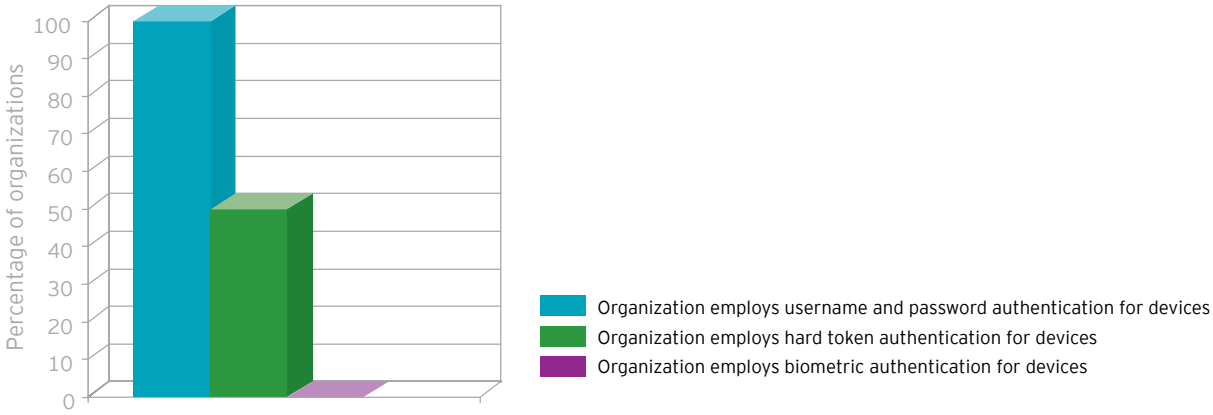
Biometric technology has yet to become more than sparsely adopted.

Respondents were asked how telecommuters authenticate themselves to access their computers and other devices, organization intranets and applications accessed locally rather than on an organization's internal network.

Survey responses demonstrate that username and password authentication is ubiquitous. This form of authentication is by far the most common choice for accessing all three. Hard tokens (such as smart cards or one-time password generators) are used by half of the organizations to access their devices and networks and by 25% of respondents for accessing applications locally on their devices.

On the other hand, biometric authentication remains rare. Almost no respondents say they use biometric technology. While some respondents indicate they are considering implementing it, financial costs and technical implementation complexities were cited as common obstacles.[5]

Putting this information in the context of the data gleaned from the previous section, Encryption technology, we find that close to half of respondents do not employ hard drive encryption when allowing telecommuters to handle personal information at home and only require a username and password for device authentication. This suggests a fairly relaxed approach to the protection of personal information, despite the fact that respondents acknowledge the privacy and security risks in the telecommuting setting.



Practices to adopt	Practices to avoid
▸ Utilizing hard token authentication for access to devices, networks or applications where merited by the sensitivity of the information and according to a risk-based approach ▸ Start assessing the adoption of biometric technology for local authentication[5] to high-risk devices, networks and applications	▸ Relying only on username and password as a method of authentication for access to devices, networks and applications without a current risk assessment

Internet connectivity

Most telecommuters connect to the Internet using a consumer-class broadband connection.

Most telecommuters connect to the Internet using a consumer-class broadband connection, with the overwhelming majority of organizations indicating their telecommuters connect over a DSL or cable broadband line.

Dial up internet access is also still a common choice; more than half of organizations say that they use it as a connection mechanism for telecommuters. Over half of the organizations also indicate that they use more than one type of internet connection for telecommuters. Dedicated circuits (e.g., T1 lines) are less common, but still available in almost half of the organizations surveyed.

Allowing telecommuters to use wireless internet connections is a common practice, but requiring that telecommuters use wireless security measures is less common.

Over three-quarters of organizations indicate that their telecommuters connect to the internet via a wireless network. Of these, only 36 organizations said they require some form of wireless security measure, including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) or MAC address filtering. Among those choices, WPA and WEP are the most common.

A recent Cisco study reported that 12% of remote workers worldwide admit to accessing a neighbor's wireless connection when working at home, with steady increases year over year in many countries.[6] Our survey results indicate that over half of organizations with wireless security requirements allow employees to use their own computers and devices for remote work. These two factors combine to create the probability that telecommuters who use easily available and unprotected wireless networks for personal use may not apply wireless security procedures when they switch to work use – a significant business risk for corporations that are focused on security for any and all data and privacy protections.

Practices to adopt	Practices to avoid
▸ Requiring wireless security measures and providing guidance to employees on how to secure their home wireless networks ▸ Prohibiting telecommuters from using unprotected and unauthorized wireless networks ▸ Considering disabling wireless networking features in devices provided to full-time telecommuters, where practical	▸ Ignoring information security risks in wireless networking when guiding telecommuters on the proper communication mechanisms for working from home

[5] The benefits of biometric authentication should be weighed against the privacy risks of storing and sending the highly sensitive information that biometrics contain. Thus, we recommend that organizations begin to explore how biometrics might be used for local authentication – where biometric information is only communicated and stored on a device or token in the telecommuter's possession – as opposed to systems that require biometric data to be sent to a remote server. For more information on this distinction, see National Research Council of the National Academy of Sciences, "Who Goes There? Authentication Through the Lens of Privacy," 2003.

[6] "How Remote Workers Heighten Security Risks for Businesses, IT Organizations, and Themselves," Cisco Systems, 2007.

Software downloads and web usage

Limitations on downloading software and using peer-to-peer file-sharing applications are common but not prevalent.

More than half of respondents, including all participating government organizations, prohibit telecommuters from downloading to their organization-provided device software that was not issued by the organization. However, many respondents noted they have no technical controls in place to enforce these policies. Also, 17% of organizations indicated they allow telecommuters to download any software they want.

Close to half of organizations surveyed say that they prohibit telecommuters from using peer-to-peer file-sharing applications and employ technical controls to prevent their use. One-third of respondents indicated that they block telecommuters from using instant messaging applications.

Furthermore, nearly three-quarters of organizations indicated that they use filtering software that blocks employees from visiting certain websites. However, these technical limitations on website access are commonly applied only when telecommuters are connected through the internal network. Less than one-quarter said they have no restrictions in place, either through technology or policy, on the websites that employees visit.

Practices to adopt	Practices to avoid
▸ Providing clear guidance on what software may be downloaded on organization-issued devices, if any ▸ Prohibiting most types of file-sharing applications on organization-issued devices; if allowing telecommuters to use home computers, prohibiting the use of such applications on those devices as well ▸ Monitoring for compliance with communicated requirements	▸ Allowing unauthorized software to be used on organization-issued devices ▸ Not communicating guidance about unsafe software on home computers

Using email

Although personal information can easily leave the organization via email, limitations on telecommuters regarding the use of email and external email services are not common.

Our survey asked about the restrictions imposed on telecommuters regarding their sending email external to the organization, including to their personal email accounts. Slightly more than 10% of respondents indicated that they restrict telecommuters from sending email to their personal email accounts with or without attachments. In addition, slightly less than 10% of the organizations restrict any external emailing of emails with or without attachments. Also, approximately 30% of respondents prohibit telecommuters from accessing external email services, but only 20% use filtering tools on their network to block employees from accessing websites that offer such services.

Email encryption solutions are common among our respondents, but telecommuters frequently use home computers where these solutions are not installed.

Close to half of respondents indicated that they encrypt their email messages, while others have indicated their approach to protecting email is to require that any attachments containing personal information be encrypted (e.g., with file encryption). While a significant number of organizations make email encryption tools available to employees, such tools are of little help if they are device-based and employees use their home computers.

Practices to adopt	Practices to avoid
▸ Communicating clear limitations to telecommuters on the use of personal information in email and providing them with tools to protect it ▸ Providing network-based email encryption solutions when allowing telecommuters to use their home computers for work ▸ Prohibiting processing of personal information on home computers and sending it to personal email accounts ▸ Monitoring what and how personal information is leaving the organization via email	▸ Allowing the use of external email accounts or ignoring its risks in policy and guidance to telecommuters ▸ Allowing the use of personal information without providing the security tools to protect it ▸ Preventing the use of personal information in email without monitoring and enforcement

Monitoring the use of technology

The higher the number of telecommuters in an organization, the more likely the organization monitors those telecommuters' use of tools and technology.

Our survey presented various monitoring options and asked respondents to indicate which of them they deploy. Over 70% indicated that their organizations do some monitoring of telecommuters, most commonly by network monitoring of telecommuter email and internet use (close to 60% of the organizations), review of access logs to applications and databases containing personal data (almost 50% of organizations) and monitoring of internal organization resources, such as file shares (nearly 40% of organizations).

More targeted monitoring may be done based on a client request or when investigating a complaint. Visits to the homes of telecommuters do not appear to be common practice and telephone monitoring is only common when the telecommuting employee serves in a call-center capacity.

Practices to adopt	Practices to avoid
▸ Identifying practical and effective means to monitor the use of technology by occasional and full-time telecommuters ▸ Identifying practical and effective means to monitor the use of technology within organizations that only have a relatively small number of telecommuters ▸ Notifying employees of the fact that the organization may monitor their actions ▸ Conducting house visits to ensure that full-time telecommuters who handle personal information are meeting the organization requirements	▸ Providing telecommuters with broad access to resources with no effective monitoring of their actions

Conclusion

Based on the results of this survey, many organizations today are not effectively managing the risks to personal information presented by the telecommuting workforce. When employees leave the office with the personal information of employees, customers or anyone else affiliated with the business organization, significant privacy and security gaps remain.

Correspondingly, organizations can and should improve their approaches to managing these privacy and security exposures. Not doing so invites unnecessary risk, ranging from data corruption and/or data loss to fraudulent use of data, regulatory non-compliance and loss of corporate reputation.

Many of the policies, tools and controls that our respondents reported on with reference to telecommuting serve broader purposes than telecommuting. This is an important distinction to make, since policies, tools and controls implemented to address multiple purposes are likely to leave gaps in how they address specific issues. This applies to computer use policies that only broadly address telecommuting; general privacy and security training that only briefly touches on the subject of telecommuting and using the same considerations in credentialing employees temporary employees; and contractors who telecommute as well as those who do not. The ubiquitous use of failed login lockouts, security cables and clean desk policies, when compared to the lackluster adoption of solutions and controls that are significantly more effective in addressing telecommuting-specific risks, is further evidence of this trend.

Effective controls and considerations specific to telecommuting, although present, appear to have lower adoption rates. Such controls include providing telecommuters with shredders and locked cabinets to use at home, inspections of remote work environments and limitations on the use of external memory devices. Monitoring telecommuters' use of certain technologies and using encryption to connect to internal networks is more common and can serve as a foundation for developing a robust, risk-based response to the privacy and security challenges of telecommuting.

Organizations should address the privacy and security risks presented by telecommuters by clearly differentiating them from risks that may arise in other operating environments. An employee who works from home full-time presents different challenges from the absent-minded business traveler. Organizations must develop and communicate specific policies, tools and other internal controls to address the telecommuting process; for example, installing email encryption tools on the organization-issued devices is of little help when employees use their home computers. Last but not least, organizations should monitor the privacy and security of their telecommuting arrangements.

Work-from-home arrangements are the next frontier for many companies, and the challenges they pose to privacy and security should be approached with appropriate rigor and resources. Based on the results of the CDT and Ernst & Young's joint survey, it is critical that organizations assess their current telecommuting arrangements and address the needs of their overall workforce when it comes to matters of privacy and security.

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 130,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve potential.

For more information, please visit www.ey.com.

About Ernst & Young's Technology Risk and Security Services
Information technology is one of the key enablers for modern organizations to compete. Effective information technology risk management helps you to improve the competitive advantage of your information technology operations, to make these operations more cost efficient and to manage down the risks related to running your systems. Our 6,000 information technology risk professionals work with you to develop an integrated, holistic approach to your information technology risk or to deal with a specific risk and security issue – wherever you are in the world. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

About CDT
The Center for Democracy and Technology (CDT) is a 501(c)(3) non-profit public policy organization dedicated to promoting the democratic potential of today's open, decentralized global Internet. CDT's mission is to conceptualize, develop, and implement public policies to preserve and enhance free expression, privacy, open access and other democratic values in the new and increasingly integrated communications environment. CDT pursues its mission through research and public policy development in a consensus-building process based on convening and operating broad-based working groups composed of public interest and commercial representatives of divergent views to explore solutions to critical policy issues.

www.ey.com/us/privacy

EYG No. BG0026