

REMOТЕLY RISKY?

By: Lori Berhon, Sr. Technical Writer, [Sterling Infosystems Inc.](#)

The vulnerability of mobile devices (laptops, Blackberrys, etc.) to theft and loss has generated many familiar news stories. Consider, for example, the November 2009 incident of the U.S. Army laptop, stolen from the Virginia home of a Family and Morale, Welfare and Recreation Command (MWR) employee and “containing names and personally identifiable information for slightly more than 42,000 individuals”¹ who had used Fort Belvoir MWR facilities. This particular instance was determined to be the result of a random housebreak. Similar news stories from around the country have reported devices stolen from cars or as an adjunct to auto theft, as well as those that were simply lost.

There is a related potential hazard that has received far less attention -- the practice of telecommuting. A 2008 report entitled [Risk At Home](#), authored by the Center for Democracy and Technology in partnership with Ernst and Young and based on their joint 2007 survey “The State of Telecommuting: Privacy and Security,” observes that “while companies are aware that telecommuting is an area of risk, the topic is often sidelined.”²

THE SCOPE OF THE RISK

The limited sense of urgency may be due to an insufficient appreciation of the related exposure.

In 2008, Cisco published an extensive study of [Data Leakage Worldwide: Common Risks and Mistakes Employees Make](#), based on a commissioned analysis performed by InsightExpress. As might be expected, the section of this paper that focuses on remote workers details risks associated with the technology used. As well as the greater potential for the loss of or damage to portable equipment, the study emphasizes that a mobile workforce presents an increased vulnerability related to devices that are “not protected or maintained to IT's standards,”³ including home computers, consumer internet connections, etc.

This study also draws attention to an area companies are less likely to have considered: that working at a remove from the office invites risky behaviors that can open the door to information theft. Even companies that have developed a clear, detailed office security policy and ensured that in-house employees are well trained might not have made specific provision in either the policy or the training plan for telecommuting employees and contractors. Employers need to recognize the inadvertent security spoilers common to “outside” workers, such as “talking about sensitive company matters where others can hear the conversation, and

“In 2003, about 4.4 million Americans were telecommuting, to some extent, instead of showing up at the office. In 2010, that number is expected to surpass 100 million.”

Beyond the 9-to-5: Why Flexible Hours and Telecommuting Are on the Rise.
Joseph Bendar for [BusinessWest Online](#)

¹ “[Laptops Containing Personal Information About MWR Customers Stolen](#)”, by FMWRC Public Affairs, Dec 16, 2009.

[www.army.mil](#) The Official Homepage of the United States Army

² “[Risk At Home: Privacy and Security Risks in Telecommuting](#)”, by The Center for Democracy and Technology, presented by Ernst & Young, 2008

³ “[Data Leakage Worldwide: Common Risks and Mistakes Employees Make](#)”, by Cisco, Inc., 2008

failing to use a laptop privacy guard when working remotely in a public place.”⁴ Carelessness can cause as much harm to a company as malicious incidents of deliberate theft or damage.

Vulnerabilities in the areas of both human capital and technology must be addressed when developing a security policy for telecommuting, just as they are for in-office security policies.

SECURING THE REMOTE WORKFORCE

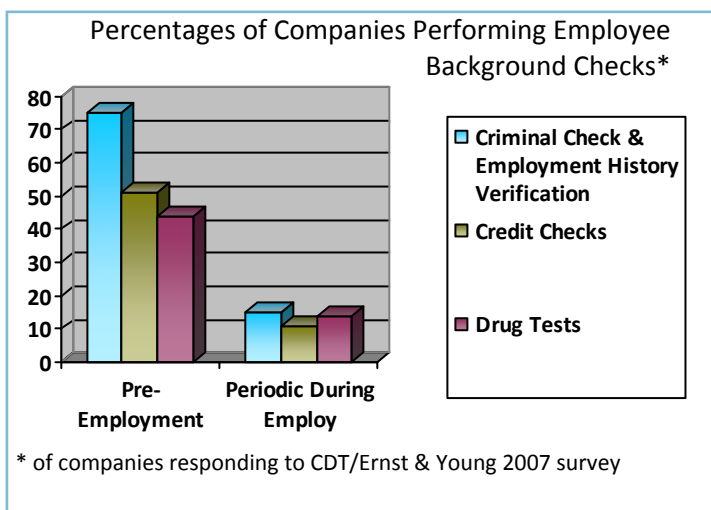
It is suggested that companies utilize a two-pronged approach to managing the human portion of the telecommuting formula: hire the highest quality employees and contractors; and, ensure that each such hire understands his or her responsibilities under the security policy and the gravity of adhering to them.

Background Checks

The importance of employee background checks has often been stressed as factor in ensuring a safe work environment for employees and customers. But what if your employees don’t work in your place of business? Is it still a best practice to run background screenings? The answer should be obvious – an emphatic “yes!”

If anything, considering that the data being accessed remotely by these workers is a valuable commodity, companies should require *additional* reassurance about staff working outside the office. It is surprising that “while telecommuting could provide more opportunities for inappropriate use of personal information,” Risk at Home report observes “it does not seem to be a factor in employee credentialing.”⁵ Even where variations in the approach to employee background investigations do exist within the same company, they don’t seem relate at all to whether or not employees work outside the office.⁶

An employee who handles large sums of money or high-priced hard goods traditionally undergoes a set of screenings that identifies a high level of integrity. A similar level of vetting should be applied to an employee who handles valuable data, and when that employee might



be handling this data in an unsupervised environment, such as a home office, the credentialing required should vary accordingly. The access employees have to sensitive or otherwise valuable information and the organization’s ability to monitor the employee’s activities are of equal concern. To effectively control exposure to risk, both of these should be factors in planning a varied employee credentialing plan.

The Risk at Home report also observes that the majority of those survey respondents who perform background checks do so only on a pre-employment basis.⁷ Should there be a change in an

⁴ Ibid

⁵ “Risk At Home”, Op Cit.

⁶ Ibid

⁷ Ibid

employee's status or responsibilities, the potential for risk might increase without the employer's awareness. The prudent employer will repeat credentialing on a periodic basis, to limit this vulnerability.

Education

"Another surprising finding in the [Risk At Home] 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."⁸

Even companies that feel confident of their employee security policy training program often fail to recognize that employees working outside the office, even if they only do so occasionally, require additional education.

In the controlled environment of the office, where those who are present can be assumed to have undergone appropriate credentialing and everyone is "on the same team," there are nonetheless safeguards around the use and sharing of data. Once the employee – and the information -- leaves those walls, no such assumptions can be made.

Increased vigilance is called for on the outside, and yet this is exactly where work discipline is likely to relax and the safeguards drop. On the phones or at the computer, people often lose track of their environment and assume a level of privacy that is at odds with reality.

In developing a risk-abatement strategy for a telecommuting workforce, companies would do well to consider the special situations that arise when working outside the office and elaborate on behavioral "do's and don'ts." The employee who thinks a street corner is a phone booth needs to understand that anytime people can hear even half a conversation, it's reasonable to expect that some of them may also be listening and taking note of what is said. Employees who work at coffee shops, on airplanes, or even in a quasi-office situation such as a kiosk in a convention center must learn to consider that the person retrieving the discarded page from the floor or leaning in to get a look at the laptop monitor may not be a casual bystander.

When telecommuting involves portable electronic devices, the company should emphasize that there is greater value on the data they contain than in the resale value of the equipment. The cost of a business laptop stolen from an unlocked car isn't \$2000 for replacing the hardware, but a possibly incalculable amount in lost data, lost confidentiality and related legal costs. Even if the computer is recovered, the broken custody "makes the integrity of the data stored on the disk suspect."⁹ As well as encouraging a heightened safety, companies should equip laptops with locking devices that prevent unauthorized use of the keyboard and reinforce the habit of logging off whenever employees are not actively working. Security experts, such as the various computer security incident response teams (CSIRTS) that are allied with the CERT® (Computer Emergency Readiness Team) Coordination Center at Carnegie Mellon University's Software

- 46 % of remote employees admit to transferring files between work & personal computers
- 75%+ of employees do not use a privacy guard when working remotely in a public place
- 68% of people do not consider whether they can be overheard when speaking on the phone in public places
- 13% of those working from home send business emails via their personal email

Data Leakage Worldwide

⁸ Ibid

⁹ Website of the CERT® Coordination Center at Carnegie Mellon University's Software Engineering Institute http://www.cert.org/tech_tips/home_networks.html#III-C-3; also posted on the US-CERT website http://www.us-cert.gov/reading_room/home-network-security/

Engineering Institute, also encourage companies to use tools “that can encrypt data stored on a computer’s hard disk....if the computer contains sensitive data or is at high risk of theft.”¹⁰

OUTSIDE THE OFFICE NETWORK

When utilizing a remote workforce, companies must address the security risks posed by the electronic devices and consumer internet connections that individuals use to access data. Whether working via laptop, desktop, smart phone, etc., telecommuters access and often transfer sensitive data from a carefully protected network to an environment that may have no, or at best limited, security.

All the safeguards surrounding the VPN that connects the remote worker to the office will not apply if the worker needs to download a copy of a file to a local hard drive and possibly email it. If this seems an unlikely possibility, note that the Data Leakage study found that “46 percent of employees admitted to transferring files between work and personal computers when working from home”¹¹ Even when data is not actively transferred, data files are open while the telecommuter is working and therefore are subject to damage should the connection be severed by disk or power failure.

CERT® and US-CERT devote an entire website section to Home Network Security. A quick skim of the topic outline¹² reminds us of how vulnerable the average network can be. Before dismissing the importance of this, consider a few key questions: How robust – and how up to date – is the virus protection software on your own home computer? Is your home network protected by a firewall as impermeable as the one used by your company? What protection do you have against IP address spoofing, Trojan horse programs and other hidden threats? Now multiply your response by the number of people who work remotely for your company and ask yourself if this is an acceptable risk.

Companies are advised to create a security policy surrounding the use of home and consumer networks, and to ensure that all employees are educated in that policy and in the risks that have inspired it.

TAKING THE FIRST STEP

In order for policies and procedures to protect data, they must be executed by dependable people. Any initiative to improve security must begin by ensuring that employees and contractors work remotely are individuals of the highest integrity.

When designing a credentialing regimen for telecommuters, companies should always recognize that data-related vulnerabilities will vary based on whether files are being accessed within or from outside of the office environment. As with any special purpose background screening initiative, companies can benefit from the expertise of their chosen background checking professionals.

¹⁰ Ibid

¹¹ “Data Leakage Worldwide”, Op Cit.

¹² CERT Website, Op Cit.