

Opinion: 8 Growing Risks of Employee Home Offices

Jay Cline

January 30, 2008 ([Computerworld](#))

When a [Pfizer](#) employee last June exposed sensitive data on 15,700 fellow employees from his home computer — where his spouse had enabled peer-to-peer connectivity — little did he know that he was adding a new item to the 2008 agendas of CPOs and CISOs across the country.

Employee home offices had long been a concern for data-protection leaders, but murky legal considerations stymied any initiatives to address this risk. With security-breach notification now a \$100 million cost and brand liability, it's only a matter of time before corporate-compliance programs bring employee homes within their purview. (See Table 1 for seven other publicized home-office breaches.)

The focus on the home office couldn't have come sooner. With the economy apparently slowing down, security officers are sitting up and taking notice. It's not only because otherwise good employees might be tempted by hard times to abuse their access privileges. The real problem is more widespread: employees and contractors in all positions, fearing layoffs, taking more and more work home to unsecured computing environments.

Two remarkable innovations — the [BlackBerry](#) and the USB drive — have rapidly accelerated this bleeding of the workplace into every corner of American life. Add in portable Internet cards, and you have large amounts of Internet-accessible data following employees and contractors wherever they are. And where are they most of the time, besides work?

Burglars and hackers have caused a number of highly publicized home-office incidents, raising the question for CPOs of how to bring employee homes within the purview of corporate compliance initiatives.

Employers, happy to cut the overhead of office space and take credit for offering flexible work arrangements, have gladly let employees turn their homes into de facto field offices.

But has corporate America written a check it can't cash? With the cost of the [Department of Veterans Affairs](#) and TJX breaches each expected to reach \$500 million, can companies really afford to take these risks?

Table 1: Selected Home-Office Privacy Breaches

Date	Organization breached	Nature of breach	Impact
December 2007	Forrester Research (Massachusetts)	Burglar stole laptop from employee's home	Personal data, including Social Security numbers, of an undisclosed number of current and former employees exposed
December 2007	West Penn Allegheny Health System (Pennsylvania)	Burglar stole laptop from employee's home	Personal and clinical information on 42,000 patients exposed
November 2007	Provincial Public Health Laboratory (Canada)	Hacker extracted patient data from consultant's computer via an unsecured home Internet connection	Names, medical ID numbers, and test results for infectious diseases, including HIV and hepatitis, exposed for an indeterminate number of citizens; health minister forced to explain
May 2007	Pfizer (New York)	A third party copied employee	Names, SSNs and in some cases

Date	Organization breached	Nature of breach	Impact
February 2007	Nationwide Building Society (U.K.)	information from the computer of an employee whose spouse had installed peer-to-peer software on it while that computer was connected to the Internet at home	addresses and bonus information on 15,700 employees exposed
May 2006	Department of Veterans Affairs (District of Columbia)	Burglar stole laptop from employee's home	11 million customers' information exposed; company fined £1.4 million by U.K. government; CEO forced to explain
May 2006	Department of Veterans Affairs (District of Columbia)	Burglar stole laptop from employee's home	25 million veterans' information exposed; department expects to incur \$100 million to \$500 million in costs related to the breach
May 2006	Nationwide Agribusiness (Ohio)	Burglar stole laptop from employee's home	306 employee names, addresses, and SSNs exposed
September 2004	Brazos Higher Education	Burglar stole laptop from	Brazos could not determine

Date	Organization breached	Nature of breach	Impact
	Service Corporation (Texas)	employee's home	which customers' information may have been exposed, so notified all customers of the breach; unsuccessful lawsuit brought by one customer

Eight Risks

There are at least eight cracks in the armor that have just gotten wider with the growing surge of home work:

1. Corporate laptops in transit home. Read the crime section of your local paper, and what do you see these days? Line after line of laptops and GPS devices stolen from vehicles. Despite a wave of laptop-encryption initiatives over the past two years, many employees are still taking home unencrypted laptops containing sensitive personal information.
2. USB drives in transit home. With the decreasing sizes and increasing speeds of these devices, expect to see more lost flash drives prompting security-breach notifications in the near future.
3. Lost personal BlackBerries and Treos. People have put great trust in the security of how their handheld e-mail messages are transmitted and stored. Find somebody's BlackBerry, and you have access to his deals, contacts, calendar and e-mail attachments.
4. Unprotected home computers. Twenty dollars to the first person who can name a Fortune 1,000 company that has assured that even 10% of its employees' home computers meet corporate policies for antivirus, spyware, personal firewall and peer-to-peer settings.
5. Unprotected home networks. Ditto for employees' home wireless network settings.
6. Unprotected files in home e-mail accounts. Which companies store sensitive information from every large company on earth? Yahoo,

Google, [Microsoft](#) and AOL. But would these e-mail programs meet your company's password, encryption and retention standards?

7. Unsecured documents in home offices. Employees have locking cabinets at work for storing sensitive documents and shred bins for discarding them, but how many of your employees lock away and shred at home?
8. Uninventoried data in home offices. More data at home means more surprises and costs — and now, potential fines – for corporate attorneys trying to conduct e-discovery.

If you take these risks and put them into a traditional threat-vulnerability matrix, you may reach an unexpected conclusion: that the home office ranks ahead of other key storage zones of corporate data. (See Table 2 for a sample matrix.)

Table 2: Threat-Vulnerability Matrix for Key Corporate Data Zones

Data-Storage Zone	Level of Threat to this Zone	Level of Vulnerability of this Zone	Risk of Breach of this Zone (Threat and Vulnerability)
Production applications and databases	HIGH	LOW	MEDIUM / HIGH
Home offices	LOW	HIGH	MEDIUM / HIGH
Vendors	MEDIU M	MEDIUM	MEDIUM
Informal data stores (Access databases and spreadsheets)	MEDIU M	MEDIUM	MEDIUM

Risk-Mitigation Options

Alan Charles Raul, a partner at the privacy practice of [Sidley Austin](#), recently addressed this topic at a privacy conference in St. Paul, Minn.

"Working at home offers tremendous productivity and convenience benefits to both employers and employees," Raul told me afterward. "But while being work-accessible 24/7 has efficiency advantages, it presents delicate privacy risks for workers and security challenges for bosses. Dealing effectively with these challenges requires identifying both sets of risks and dealing with them concretely," he added.

What were Raul's top recommendations?

1. Update your policies to include standards for home-office work and home-compliance assessments.
2. Get employee consent with these policies if they want to continue working from home.
3. Properly equip and train employees to comply with the policies.
4. Inventory data in home offices.
5. Conduct spot checks where legally permissible.

If the only thing your company is doing about these risks is waving a policy in the air prohibiting employees from taking confidential data home, I've got some subprime mortgages in Detroit to sell you. The risk tolerance is about the same.

Jay Cline is a former chief privacy officer of a Fortune 500 company and now president of [Minnesota Privacy Consultants](#). You can reach him at cwprivacy@computerworld.com.