Rise of Telecommuting Poses Unique Privacy and Security Threats to Company Networks

November 26, 2008

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

Telecommuting, a practice increasingly favored by employers and workers alike, has a great deal to recommend it, but it also raises serious new privacy and security threats that must be addressed in order to prevent this generally beneficial practice from leading to serious privacy and security failures. CDT joined Ernst & Young to survey employers about telecommuting and to identify the best practices and areas of weakness.

---

(1) Telecommuting Carves A New Privacy and Security Landscape for Employers

Telecommuting, a practice increasingly favored by employers and workers alike, has a great deal to recommend it, but it also raises serious new privacy and security threats that must be addressed in order to prevent this generally beneficial practice from leading to serious privacy and security failures. CDT joined Ernst & Young to survey employers about telecommuting and to identify the best practices and areas of weakness.

In recent years, telecommuting has been on a steady rise that shows no signs of slowing. According to a recent report more than 46 million people are expected to work at home at least one day a week by the end of 2011. Continuing improvements in mobile computing and broadband availability have virtually eliminated technological barriers that once prevented employees from working effectively outside of the office. For employers, providing the flexibility to telecommute is a low-cost perk that can be a key differentiator in competing for talent. Meanwhile, environmental advocates are urging continued migration to telecommuting to reduce greenhouse emissions and the burning of fossil fuels.

Stacked against these benefits are a host of new privacy and security issues raised by having so many employees that are working outside the controlled environment of the workplace. Companies currently face serious challenges in securing their internal networks and facilities against attacks, failures and unintended data spills. Telecommuting compounds those challenges exponentially.

In too many instances, telecommuting employees:

- Access work networks and data from unsecured personal or home computers;
- Access corporate networks and data from unsecured broadband or wireless networks, including public Wi-Fi hotspots;
- Transport sensitive data on unsecured laptops and storage devices;
- Store unsecured laptops and storage devices containing sensitive data in home offices, cars and other exposed locations; and
- Download programs onto work computers that may include spyware and other malicious code.

These sorts of activities have already led to several high-profile data breaches. Unless they are addressed, such incidents will only increase as telecommuting increases.

The State of Telecommuting: Privacy and Security (July 29, 2008) [1]

---

(2) Emerging Privacy and Security Concerns Are Not Being Consistently Addressed

Although companies are increasingly seeking to accommodate telecommuters, policies designed to address the specific issues associated with telecommuting have lagged far behind, according to the results of the survey. The prevailing theme in the survey was one of systemic inconsistency.

A diverse group of 73 organizations representing 10 industries in the US, Canada, and Europe responded to the survey. Their sizes ranged from over 100,000 to a handful of employees. The average number of employees in the sample was approximately 50,000 with a median of 4,000.

Among the key findings:

- A large majority (84 percent) of respondents allowed employees to handle personal information (generally considered to be data that relates to an identifiable person, such as names, addresses, telephone numbers, or email addresses) at home. Nearly 20 percent of those organizations had no policies addressing hardware and software use by telecommuters.
- Nearly 75 percent of responding organizations 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.
- About 50 percent of respondents indicated that their telecommuting employees, both full-time and occasional, sometime use their own personal computers and PDAs at home for work purposes.
- Fewer than half (49 percent) of the respondents required the use of e-mail encryption software.
- Only 25 percent of respondents said that their organizations have telecommuters store paper records in secured cabinets or other storage systems that the organizations themselves provide.
- A majority (85 percent) of respondents reported using at least one of five key security measures discussed in the survey -- failed login lockout settings on computers, privacy screens, security cables for locking down computers, periodic audits of telecommuter physical working environments, and "clean-desk" policies.
- A majority of organizations (86 percent) indicated that they use encryption to secure telecommuter connections to internal networks such as through a secure virtual private network (VPN). Only 3 percent of organizations prohibit remote access to internal networks altogether.
- About 17 percent of organizations allow telecommuters to download software without any restrictions. Just over half of respondents (including all government respondents) do not permit telecommuters to download software that was not issued by the organization.

Taken together, the results paint a stark picture of a patchwork policy and technical environment for

telecommuters. We have already seen some of the consequences of this uneven policy environment, as several high-profile data breaches in recent years have been traced back to unsecured laptops and home offices. Until employers get serious about addressing these issues, we can expect to see such incidents increase, as more and more workers fill the telecommuting ranks.

---

(3) Companies Must Adopt New Practices to Offset Telecommuting Risks

The good news about the privacy and security challenges associated with telecommuting is that the solutions are not difficult to implement. The key task will be to convince employers to recognize the threat. Once employers are motivated to make comprehensive changes, the path forward is clear.

The CDT-Ernst&Young survey recommends a range of practices for employers to adopt to create a more secure environment for telecommuters. In general these are common sense policies and technical upgrades that should not adversely affect the productivity and ease of telecommuting.

Among other things, the report recommends that employers:

- Develop telecommuting-specific policies and guidance that address specific needs and risks.
- Provide telecommuters with clear guidance on the use and disposal of paper records containing personal information.
- Identify the most relevant physical security requirements for telecommuting employees and provide the tools necessary to meet those requirements.
- Provide "thin" clients and other privacy-enhancing devices to employees that frequently work from home.
- Prohibit employees from using home computers without information security mechanisms installed and before clear policy and guidance are provided to them.
- Require wireless security measures and providing guidance to employees on how to secure their home wireless networks.
- Prohibit telecommuters from using unprotected and unauthorized wireless networks.
- Provide clear guidance on what software may be downloaded on organization-issued devices.

In many cases these recommendations cost employers little or nothing, but return substantial benefits in the form of increased privacy and security. The challenge for policymakers, chief technical officers and all other stakeholders in the security space will be to impress on organizational leaders the very real risks associated with telecommuting and the need for comprehensive internal audits and reform.

Links:
[1] http:/www.cdt.org/privacy/20080729_riskathome.pdf