New Study Identifies Snooping as Growing Threat for Corporate Data Breaches

Two-Thirds of Employees Put Sensitive Information At Risk for a Visual Data Breach When Working Outside the Workplace

A new study conducted by People Security and commissioned by 3M, the maker of privacy filters for computers and mobile devices, reveals two-thirds of employees expose sensitive data outside the workplace – some even exposing highly regulated and confidential information such as customer credit card and social security numbers. TheVisual Data Breach Risk Assessment Study also found the majority of companies do not have policies or measures in place to protect sensitive information from computer screen snooping when employees are working in public places.

“With the rise in mobile workers carrying confidential data with them outside the office, snooping is no longer a harmless hobby and may represent a weak link in corporate data security practices,” says Dr. Hugh Thompson, Chief Security Strategist of People Security. “Today’s latest smart phones now make it possible for a data thief to take a high-resolution picture of confidential information on a computer screen and retrieve readable data without any hacking necessary. Information revealed on mobile devices outside the workplace now creates a window into a corporation’s most confidential data – whether it is regulated or simply company secrets – and significantly raises the threat level of visual data breaches.”

The study included a survey of 800 working professionals1 and an experiment at a large IT conference where attendee computer usage habits and data security choices were observed2.

According to the Privacy Rights Clearinghouse’s Chronology of Data Breaches, more than a half billion sensitive records have been breached since 2005, leaving Americans vulnerable to identity theft. While this number does not include visual privacy breaches, 71 percent of working professionals surveyed admitted to glancing at another person’s computer screen where they saw such things as corporate emails (26%), presentations (20%), documents (18%), spreadsheets (29%) or other corporate sensitive information (11%). While most surveyed said the reason for glancing at another person’s screen was unintentional, 15 percent were interested in what was on the screen and 2 percent even admitted they were trying to obtain information.

“Companies know they need to protect confidential information, but the threat of a visual data breach has historically been low on the priority list,” said John Stoxen, 3M Director of Business Conduct and Compliance. “This study should convince companies to reassess their data security policies and tools to determine how to better protect against visual data breaches when employees are working outside the office. At 3M, we address the risk of visual privacy in our Electronic Resources policy by requiring employees to take appropriate measures to protect 3M confidential information in public places by using privacy filters.”

The study also examined how privacy concerns affect employee productivity while working outside the office. Fifty-seven percent of working professionals surveyed said they have stopped working on their laptops because of privacy concerns in a public place and 80 percent thought that “prying eyes” posed at least some risk to their organization.

For more information or to downloadable the study whitepaper, go to http://www.3MPrivacyFilters.com/whitepapers. The following key findings and implications outline some of the highlights from the whitepaper.

Key Study Findings:

Employees are exposing regulated customer information, as well as confidential corporate information outside the office. Two-thirds (67%) of working professionals surveyed had worked with some type of sensitive data outside the trusted confines of the office within the past year, including highly sensitive information such as customer credit card numbers (26%), customer social security numbers (24%), patient medical information (15%) and internal corporate financial information (42%).

Convenience is more important than privacy for employees working outside the office. One in four (26%) conference internet kiosk users accessed corporate email on an unprotected network in a high-traffic public area, though many had the opportunity to use a more secure corporate laptop or smart phone. Furthermore, attendees who used the internet kiosks had the choice of using a computer either equipped or not equipped with a privacy filter so neighbors and passersby couldn't see the information they were accessing; the majority (65%) of kiosk users chose one without a privacy filter. These findings illustrate that some employees are careless with corporate data by choosing convenience over security.

Significant gap exists between risk and corporate policy/tools to prevent visual data breaches. There is a basic expectation that companies will keep sensitive information secure at all times. However, 70 percent of working professionals surveyed said their company had no explicit policy on working in public places and 79 percent reported no company policy on the use of privacy filters to prevent visual data breaches.

Protection against visual data breaches last to be addressed by corporations. Data security practices such as VPN access (46%), disk encryption software (38%) two-factor authentication (19%) were all more commonly used to protect against breaches compared to the use of privacy filters (13%).

The threat of a visual data breach is growing. Fifty-five percent of working professionals surveyed worked on their laptop in a high-traffic public area at least 1 hour per week. IT analyst firm IDC estimates that more than 72 percent of the US workforce has some level of mobility3, and by 2013 this number will increase to more than 75 percent. Many of these workers will access corporate email/data in public areas through laptops and smart phones, putting that data at risk for exposure. According to a recent survey, more than 60 percent of US households now have at least one camera phone4. This means that most users have the ability to capture images, including screens shots, further increasing the risk of visual data breaches.

Opportunity to increase productivity when privacy-concerned employees work outside the office with stronger privacy protection measures in place. Fifty-seven percent of working professionals surveyed said they have stopped working on their laptops because of privacy concerns in a public place and 70 percent said they would be more productive in public places if they thought no one else could see their screen. This concept that security-conscious employees would be more productive working outside the office when using privacy-enhancing tools such as privacy filters was further indicated through observation during the experiment.

About 3M

A recognized leader in research and development, 3M produces thousands of innovative products for dozens of diverse markets. 3M's core strength is applying its more than 40 distinct technology platforms – often in combination – to a wide array of customer needs. With $23 billion in sales, 3M employs 75,000 people worldwide and has operations in more than 65 countries. For more information, visit www.3m.com or follow @3MNews on Twitter.

3M is a trademark of 3M Company © 3M 2010

1 Luth Research conducted the survey of 800 working professionals who were employed either part-time or full-time at the time of the survey and used a computer for at least a portion of the day from August 30 to September 13, 2010. The margin of error is +/- 3.5 percentage points.

2 Conference included 1,000 attendees who worked in the IT departments (directors, managers, programmers, support, etc.) in a wide range of industries (e.g. finance, healthcare, retail, etc.).

3 IDC Worldwide Mobile Worker Population 2009–2013 Forecast, http://www.idc.com/getdoc.jsp?containerId=221309

4 PMA Marketing Research, http://pmanewsline.com/2010/03/15/pma-data-watch-camera-phone-penetration-continues-to-rise/

Hunter Public RelationsTrisha Seminara, 212-679-6600, ext. 212tseminara@hunterpr.comor3MKatherine Hagmeier, 651-575-4368

---

https://news.3m.com/2010-12-06-New-Study-Identifies-Snooping-as-Growing-Threat-for-Corporate-Data-Breaches