


Most Data Breaches Involve Paper

February 4, 2009 7:33AM

 **Keep all sensitive information and files safely locked away. Restrict access to those who need it and closely watch your files. Ensure all company computers have the most up-to-date antivirus, anti-spyware, and firewall software. Also, check to make sure wireless networks are protected with the proper security settings.**

If current headlines are to be believed, data breaches involving electronic devices occur with mind-numbing frequency. Stories about missing laptops and stolen passwords appear daily, yet a recent study debunks the conventional wisdom that the majority of data breaches occur electronically.

"The Security of Paper Documents in the Workplace" study, commissioned by the Alliance for Secure Business Information (ASBI), reveals that most breaches involve paper. In fact, 49 percent of respondents whose companies have been affected by a data breach said that one or more of the breaches involved the loss or theft of paper, not electronic, documents. Even more surprising, 80 percent of respondents polled indicated their company had experienced one or more data breaches in the past 12 months alone.

Data breaches, whether via paper or electronic means, affect businesses of all sizes. Of survey respondents who represent larger companies, 46 percent estimate the annual financial impact of data breaches within their organization to be between \$10 million to \$30 million.

The survey reveals that all companies need to more tightly control their paper trails through stronger enforcement of security policies. For example:

* According to 56 percent of respondents, more than half of their organizations' sensitive or confidential information is contained within paper documents.

* 61 percent of those surveyed said there are not enough resources and controls available to secure paper documents.

* 57 percent of respondents reported that it is more difficult to control access to paper documents than it is to control access to electronic documents.


* Nearly half (41 percent) of respondents are uncertain whether their organization has a strict policy in place for securing paper documents.

The ASBI, a group formed to address these issues and the need for awareness and education for businesses and employees about how to protect confidential information in the workplace, suggests the following actions to protect your company and yourself from a data breach:

* Shred all proprietary information with a crosscut shredder. Desk-side shredders are ideal for business professionals who regularly handle sensitive information including legal, accounting, human resource, or finance departments.

* Develop office guidelines for all employees that outline the proper procedures for protecting sensitive information.

* Keep all sensitive information and files locked away. Restrict access to those who need it and closely watch your files.

* Ensure all company computers have the most up-to-date antivirus, anti-spyware, and firewall software. Also, check to make sure [wireless](#)  networks are protected with the proper security settings.

* Limit the use of Social Security numbers (SSNs) in the workplace. Don't use SSNs on items such as employee identification badges, time cards, or paychecks.

* Avoid leaving documents in communal copiers, shared printing spaces, conference rooms, or other open areas for extended periods of time.

* Memorize passwords instead of writing them down. In addition, do not use your date of birth for your passwords, and change them frequently.

* At the end of each work day, all employees should log off their computers and lock their workstations or office doors. All confidential documents should be filed away rather than left on desks.

Respondents said they consider certain departments within an organization to be more at risk due to their inability to secure paper documents, including: human resources (45 percent), finance and accounting (40 percent), and information technology (38 percent).

© 2009 Information Management Journal. All rights reserved.

© 2009 Sci-Tech Today. All rights reserved.