

Security Breaches Continue To Reach Record Highs

Security and data breaches were up a staggering 50% in 2008 over the previous year, affecting 35.7 million people. Breaches attributed to data theft by employees more than doubled, and breaches of both digital and paper confidential records are expected to grow in 2009. Are your clients prepared?

Top 10 Security Breaches of 2008

- 1. TJX Companies** (parent of retailer TJ Maxx). With 11 hackers accused of stealing more than 40 million credit and debit cards, the TJX case proved that information breaches can cost a company over \$500 million dollars in overall expenses.
- 2. Bank of New York Mellon.** A missing backup tape containing social security numbers and bank information of 4.5 million customers points to risks once data leaves an institution.
- 3. Hannaford** (Supermarket). Despite the company being compliant with PCI credit processing regulations, it suffered a breach of 4.2 million credit cards.
- 4. Countrywide Financial.** One rogue employee stole the information of over 2 million loan applicants, illustrating the risk of disgruntled employees having access to confidential records.
- 5. GE Money.** When Iron Mountain couldn't locate a backup tape belonging to GE Money, serious questions arose regarding the security of offsite storage services. GE Money had credit monitoring costs for 650,000 clients.
- 6. RSA.** After three years and 500,000 records stolen, this security vendor uncovered a single Trojan computer virus employed by a hacking gang.
- 7. Compass Bank.** One million records were stolen in an insider heist involving a staff computer programmer. This individual is now serving a jail sentence.
- 8. Okemo Ski Resort.** Hackers installed malicious code to intercept credit card transactions.
- 9. Montgomery Ward.** After this retailer's website was breached, the company learned the importance of alerting its customers in a timely fashion.
- 10. Citibank.** After \$750,000 of funds was illegally withdrawn from ATMs, the bank was required to notify its customers of the breach. The bank claims the breach occurred at a 3rd party vendor's site; however, the bank was still responsible for the information.

No matter how comprehensive an organization's information security practices are, the organization is vulnerable to a breach of confidential information.

Do your clients know their exposures? Have they implemented privacy and security controls? Any client that collects confidential information needs privacy coverage.



S.H. Smith & Company, a nationally recognized expert with regard to the placement of Cyber, Security & Privacy policies, is taking a leadership position in recognizing the importance of educating its customers on the Cyber, Security & Privacy issues which are confronting organizations of all sizes. For more information and materials to share with your clients including how to better protect against cyber, security & privacy risks, contact:

David Perkins
Massachusetts Office
781.247.6223
800.735.1023
David_Perkins@shsmith.com

Jeanine Loomis
Minnesota Office
651.414.3863
877.279.8500
Jeanine_Loomis@shsmith.com

Ed McGuire
Massachusetts Office
781.247.6225
800.735.1023
Ed_McGuire@shsmith.com

 **S.H. Smith & Company, Inc.**

OFFICES IN: Connecticut, Florida, Massachusetts, Maryland, Minnesota, New York, Ohio and Rhode Island

www.shsmith.com