

[Next Blog»](#)

Insurance Leaders: Dream, Learn, Do, & Become

DEVOTED TO THE NUTURING AND DEVELOPMENT OF INSURANCE AND REINSURANCE PROFESSIONALS, AIMING TO OPTIMIZE HAPPINESS, PLEASURE, FULFILLMENT AND PERFORMANCE IN PERSONAL AND CAREER ENDEAVORS.

Subscribe via email

Enter your email address:

Delivered by FeedBurner



Jim Jacobs

Welcome to my Blog

Welcome to my Blog. I hope to engage you curiosity and to share information that for both your professional and personal lives, leads to: success, life satisfaction, flourishing, fulfillment, and genuine happiness. According to leading authorities in psychology, the "good life" is there for our taking if we invest thoughtful work and true effort

Wednesday, January 7, 2009

Data breaches increase 47% in 2008

<http://www.businessinsurance.com/cgi-bin/news.pl?newsId=14931>

BusinessInsurance.com

Data breaches increase 47% in 2008

By Joanne Wojcik Jan. 06, 2009 >

Data breaches in the United States increased dramatically in 2008 with 656 breaches reported, a 47% increase over 446 in 2007, according to the Identity Theft Resource Center. >

While government agencies and the military have significantly reduced the number of data breaches through heightened security measures, the business community's exposure remains high, according to the San Diego-based nonprofit, established to broaden public education and awareness about identity theft.>

Government and the U.S. military reported 110 data breaches in 2008, the same as in 2007. That number represents 16.8% of all data breaches in 2008, down from 24.6% of all data breaches reported in 2007, the center reported. >

Business, by contrast, leads the list of data breaches, reporting 240 in 2008, an 86% increase over the 129 data breaches that were reported in 2007. Business also represented 36.6% of all data breaches that occurred in 2008, up from 28.9% in 2007.>

Other categories with increases in 2008 from 2007 include educational, 131 vs. 111; medical/healthcare, 97 vs. 65; and banking/credit/financial, 78 vs. 31.>

Breaches can occur when laptops are lost or stolen, when backup tapes are lost in transit and when hackers break into systems, along with viruses, internal security failures or employees stealing information or allowing outside access to information. >

invest thoughtful work and true effort to get there.

On an ongoing basis, you'll find information on a variety of subjects leading to the outcomes enumerated above. Beyond individual posts and archives, the left column, provides links to the following topics:





- Insurance/Reinsurance Trends
- Recruiter Tips for Candidates
- Recruiter Tips for Hiring Managers and Companies
- Self Assessment Tools
- Compensation & Employment Agreements
- Corporate Governance
- Innovation
- Leadership
- Relationships
- Positive Psychology & Human Flourishing
- Psychology of Influence
- Behavioral Economics. Finance, and Decision Theory
- The Light Side: Humor
- Useful Websites (One's you've likely missed)

Please send me a note with your suggestions and feedback (contact info below). Happy flourishing. The "good life" is yours for the taking!

Jim In The News

Get Ready for Your Insurance Industry Interview

Subscribe to: <http://>

-  Posts 
-  Comments 

Special Trends & News In Insurance/Reinsurance

- Comprehensive Explanation & Example of Insurance Cycles (Advisen Forecasts End Of Soft Market In Commercial Insurance Premiums

Among the leading causes of data breaches in 2008 were malicious attacks, hacking and insider theft, which collectively accounted for 29.6% of all data breaches that occurred last year, according to the center. The incidence of insider theft represented 15.7% of data breaches last year, more than double that of 2007, while insider theft represented just 6% of all data breaches, according to the center. >


Electronic breaches, which represent 82.3% of all data breaches, continue to outnumber paper breaches, which represent 17.7% of data breaches, the center found.>

To prevent data breaches, the center advises all agencies and companies to take the following risk management steps: >

- Minimize personnel with access to personal identifying information.
- Require that all mobile data storage devices containing identifying information encrypt sensitive data. According to the center, only 2.4% of all breaches had encryption or other strong protection methods in use, and only 8.5% of reported breaches had password protection.
- Limit the number of people who may take information out of the workplace and set into policy safe procedures for storage and transport of data.
- When sending data or back-up records from one location to another, encrypt all data before it leaves the sender and create secure methods for storage of the information, whether electronic or paper.
- Properly destroy all paper documents prior to disposal.
- Verify that servers and personal computers storing sensitive information are secure at all times, updating antivirus, spyware and malware software at least once a week, and allowing software to update itself as necessary in between regular maintenance dates.
- Train employees on safe information handling until it becomes second nature. >

For more information about the center and its data breach reports, visit <http://www.idtheftcenter.org/>.

This posting was made my Jim Jacobs, President & CEO of Jacobs Executive Advisors. Jim also serves as Leader of Jacobs Advisors' Insurance Practice.

Posted by Jim Jacobs at 8:31 AM 

Labels: [insurance industry](#), [Jacobs Advisors](#), [Jacobs Executive Advisors](#), [Jim Jacobs](#), [P and C Trends](#), [property and casualty](#), [reinsurance](#)

Links to this post

[Create a Link](#)
[Newer Post](#)

[Home](#)

[Older Post](#)