Data Breach QuickView

An Executive's Guide to Data Breach Trends in 2012

Sponsored by:

Risk Based Security

Open Security Foundation

February 2013

Executive Summary

As we had predicted throughout the year, 2012 broke the previous record in terms of number of reported data loss incidents. With 2,644 incidents recorded through mid-January 2013, 2012 more than doubled the previous highest year on record (2011). On a positive note, however, although the number of reported incidents increased, the number of records exposed decreased. Over 267 million records were exposed in the 2,644 incidents, significantly less than the 412 million records exposed in 2011.

More than half of the records exposed in 2012 incidents were from a single incident in which employees of Dun & Bradstreet's marketing unit, Shanghai Roadway[1] D&B Marketing Services Co., Ltd., stole and sold 150 million customer records. The incident, categorized as *Malicious-Insider Fraud*, resulted in the closure of the business unit, fines for Dun & Bradstreet, and fines and jail time for four employees. The impact of the breach on D&B's operations in China remains to be seen.

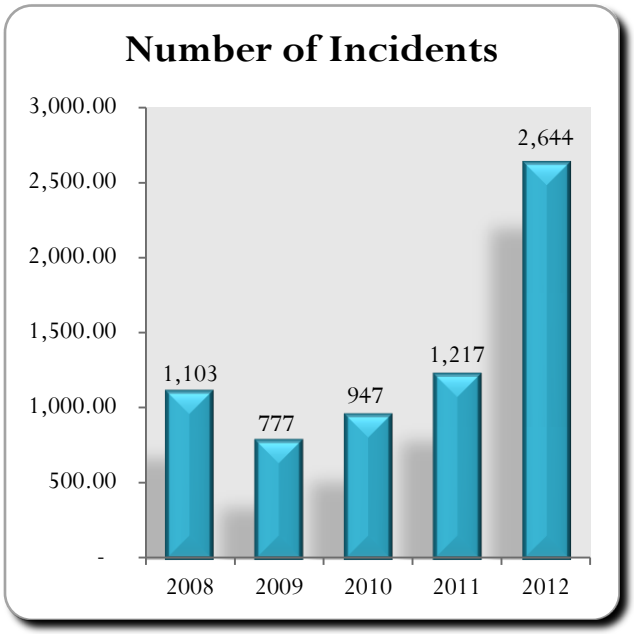
The goal of this report is to provide an executive level summary of the key findings from RBS' analysis of 2012's data breach incidents. Contact Risk Based Security for the complete analysis of the 2012 data breaches, available in March 2013.

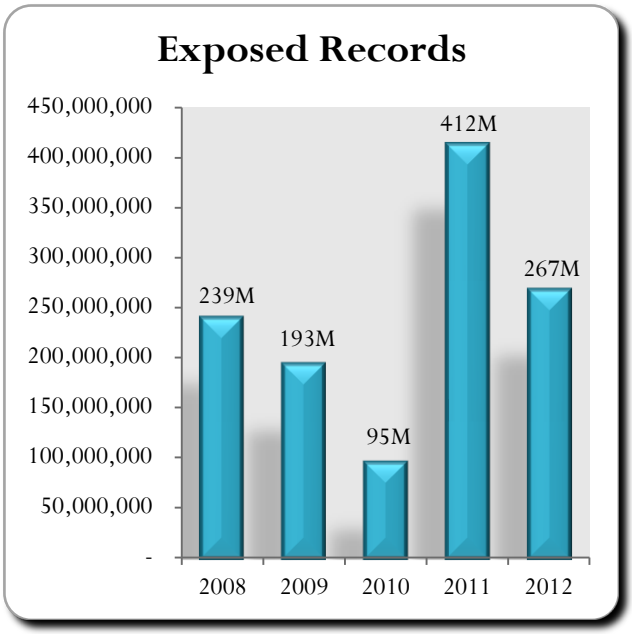
[1] Free registration/login required to DataLossDB.org to access referenced incidents.

2012 at a Glance …

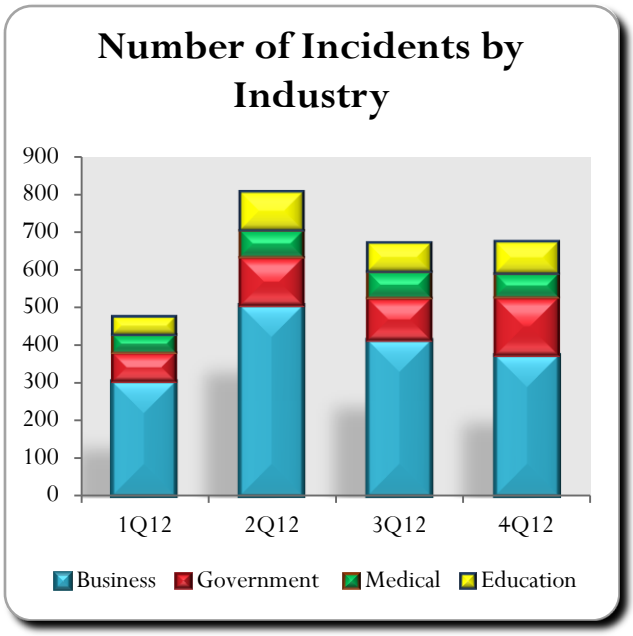
- The 2,644 incidents represent a 117.3% increase over the previous high mark recorded in 2011.
- Over 267 million records were exposed. Over 150 million records were exposed in a single incident (Shanghai Roadway), setting a new record for number of records exposed in a breach or data loss incident.
- The *Business* sector accounted for 60.6% of reported incidents, followed by *Government* (17.9%), *Education* (12.0%), and *Medical* (9.5%).
- The *Business* sector accounted for 84.7% of the number of records exposed, followed by *Government* (12.6%), *Education* (1.6%), and *Medical* (1.1%).
- The *Data Services* industry accounted for just 0.3% of incidents, but 56.2% of exposed records.
- 76.8% of reported incidents were the result of external agents or activity outside the organization:
  - *Hacking* accounted for 68.2% of incidents and remained the #1 breach type for the second consecutive year. *Hacking* accounted for 22.8% of exposed records in 2012.
  - 7.3% of reported incidents involved a third party. These incidents accounted for 6.2% of the exposed records.
- Insiders accounted for 19.5% of incidents and 66.7% of exposed records:
  - Insider wrong-doing accounted for 7.1% of reported incidents and 56.8% of exposed records.
  - Insider errors accounted for 8.9% of incidents and 5.1% of exposed records.
- Breaches involving U.S. entities accounted for 40.7% of the incidents reported and 25.0% of the records exposed.
- Individuals' names, passwords, email addresses, and other miscellaneous data were exposed in nearly 45% of reported incidents. In combination, this data is more than enough information to commit identity fraud on a large scale.
- 14.4% of breaches included a Social Security Number or Non-US Equivalent.
- After removing the single incident of 150 million and any incidents for which we do not have the number of records exposed, on average, 55,863 records were exposed per incident in 2012.

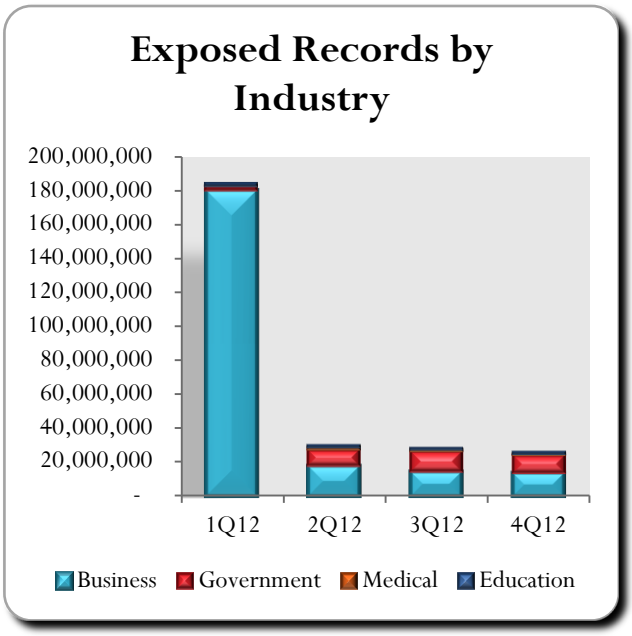
Looking Back at the Last Five Years



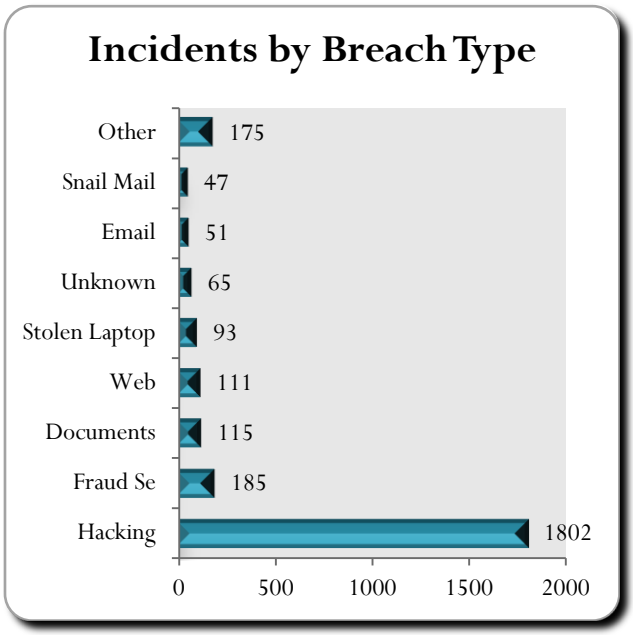


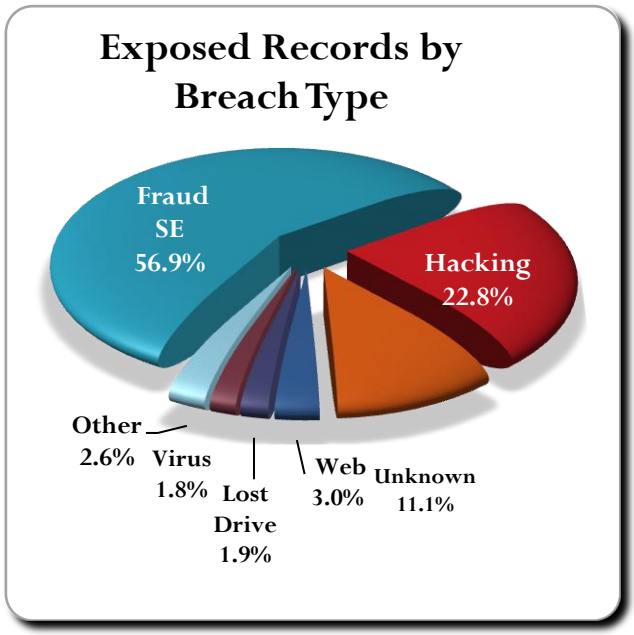
2012 Quarterly Statistics





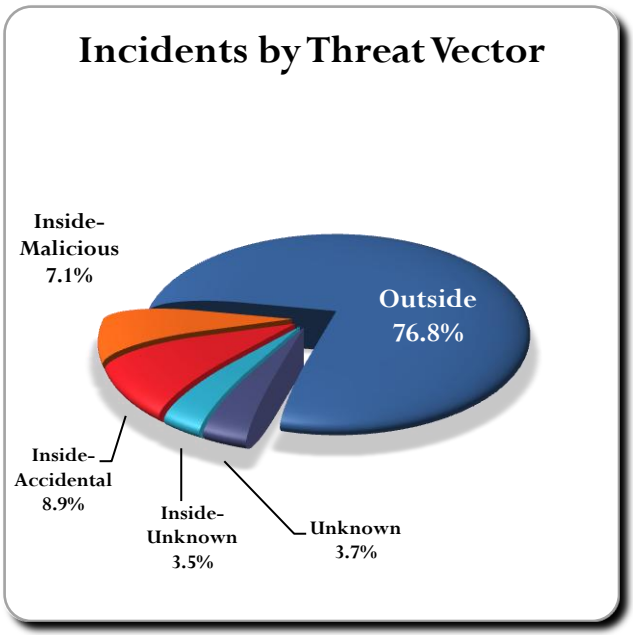
2012 Analysis by Breach Type

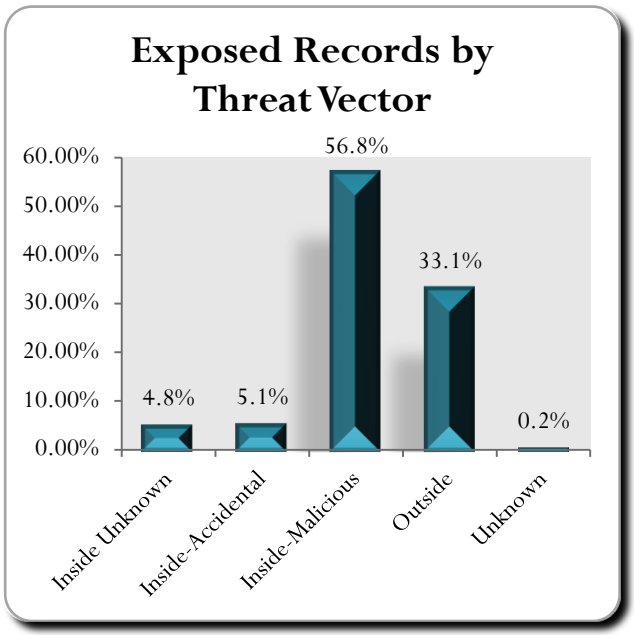




76.8% of incidents involved outside the organization activity.

2012 Analysis by Threat Vector





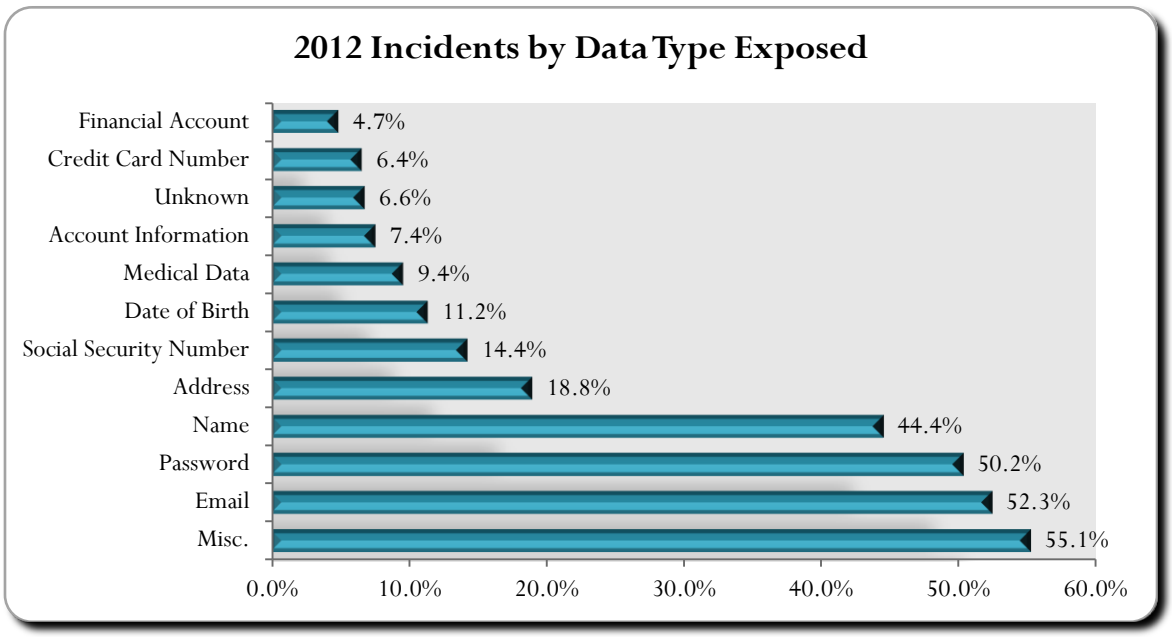
Analysis by Data Family

	Percentage of Total Incidents	Percentage of Total Lost Records
Data Family	2012	2012
Electronic	89.6%	99.6%
Physical	8.1%	0.4%
Other	0.1%	< 0.0%
Unknown	2.2%	< 0.1%

Nearly 90% of all incidents involved electronic data and nearly 100% of exposed records were in electronic form.

A single Inside-Malicious incident exposing 150 million records dominates the 2012 statistics.

2012 Analysis by Data Type



In 2012, we saw a shift in the prevalence of data types being exposed by incidents. In past years, the individual's name was the single most common data type involved in incidents. In 2012, however, name was replaced at the top spot by *Miscellaneous*, a category that, until recently, included usernames as well as other types of personal information not covered by specific data types previously tracked. Email address and password ranked second and third respectively in 2012 data types compromised, with individual names coming in fourth. The fact that an increasing number of websites now use a user's email address as a UserID may account for the significant increase in this type of exposure, but given that many users re-use their usernames, email addresses, and passwords across sites or accounts, the acquisition of such information by hackers may give them access to users' email account or financial accounts.

Comments

The global economy remained weak in 2012, and not surprisingly, criminal efforts to compromise and monetize personal information appeared to be gaining strength. Although many of the hacks resulting in data dumps were performed to embarrass the entities affected, we also saw resurgence in the use of ransom-ware and extortion demands as criminals sought a quick way to make money. The 267 million records exposed in 2012, although less than 2011's 412 million, should be interpreted as a significant underestimate of records exposed because 20.6% of incidents did not report the number of records involved.

One of 2012's incidents, Shanghai Roadway, has taken the top spot on the Top 10 list all-time with the exposure of 150 million records as the result of insider wrong-doing. This single incident supports the longstanding notion that is perpetuated by historical CSI / FBI computer crime surveys as well as surveys of the computer industry that insiders are more dangerous than outsiders. Combined with four 2011 incidents including Sony Corporation (77 million records), Tianya (40 million), SK Communication (35 million) and Steam / Valve Inc. (35 million), five incidents in the past 12 months now occupy spots on the top 10 all-time list.

Many incidents, however, involve both insiders and outsiders in large-scale conspiracies to acquire personal information to use for tax refund fraud, Medicare/Medicaid fraud, or other illicit purposes. As a single example, in one incident (Florida Hospital), one employee improperly accessed 763,000 patients' records and then sold information on 12,000 patients to an outsider who solicited the patients for lawyers and chiropractors.

As breach incidents continued at an unprecedented pace, governments increasingly imposed enforcement actions and monetary penalties on entities that did not adequately secure personally identifiable information. As examples, in 2012, the Federal Trade Commission:

- settled charges with PLS Financial and Payday Loan Store over improper dumping of customer data;
- sued Wyndham Hotel & Resorts over hacked customer credit card information;
- settled charges with EPN, Inc., and Georgia auto dealer Franklin Budget Car Sales, Inc. over P2P software on their system that exposed customer data; and
- settled charges with Compete, Inc. over failure to adhere to their stated data security policy and for transmitting customer financial data in clear text.

The U.S. Department of Health & Human Services also imposed fines in the healthcare sector, including:

- fining Hospice of North Idaho $50,000 after a laptop with unencrypted patient information was stolen from an employee's car; and
- fining Massachusetts Eye & Ear $1.5 million after a laptop with unencrypted patient information was stolen from a physician while traveling.

Similarly, in the United Kingdom, the Information Commissioner's Office issued a number of monetary fines to councils and police departments in 2012 following data protection breaches. A fine of £150,000 was also imposed on Welcome Financial Services Limited over the loss of two backup tapes containing 510,000 customers' names, addresses, telephone numbers, and loan account information.

Summary

If the reported incidents in 2012 tell us anything, it is that data breach reporting and disclosures of data compromises are on the rise and that every organization that creates, receives, stores, or transmits data can fall victim to a breach with extremely detrimental consequences - even when the data may not seem particularly sensitive. There appears to be no let-up in sight and every organization needs to understand what critical information assets they have and what specific preventive security controls are in place to protect them.

Organizations in all industries and of all sizes need to prepare for the very real threat from security breaches. Whether it is the constantly increasing security threats, ever-evolving IT technologies, or limited security resources, data breaches and the costs related to response and mitigation continue to escalate. Organizations need timely and accurate analytics in order to better prioritize security spending based on their unique risks.

Methodology & Terms

Risk Based Security's proprietary application crawls the Internet 24x7 to capture and aggregate data breach incidents for our researchers to analyze. In addition, our researchers, in partnership with the Open Security Foundation, manually scour news feeds, blogs, and other websites looking for new data breaches as well as past breaches that requiring updating. The database also includes information obtained through Freedom of Information Act (FOIA) requests to obtain breach notification documents as a result of state notification legislation.

Definitions: Primary Industry types/sectors are reported as Business, Educational, Government, and Medical.

Each primary industry/sector is further defined by one of the following subtypes: Retail, Financial, Technology, Medical (Non-Hospital and non Medical Provider), Federal Government, Data Services/Brokerage, Media, University, Industry, State Government, Not-For-Profit, County Government, Organization, Hospital, High School, Insurance, City Government, Hotel, Legal, Elementary School, Educational, Business, Government, Service Provider, and Agriculture.

Data Types: Name, Address, Date of Birth, Email, User Name, Password, Social Security Number, Credit Card or Debit Card Number, Medical Information, Financial Information, Account Information, Phone Numbers, Intellectual Property, and Unknown.

Breach Types are defined as follows:

Name	Description
Disposal Computer	Discovery of computers not disposed of properly
Disposal Document	Discovery of documents not disposed of properly
Disposal Tape	Discovery of backup tapes not disposed of properly
Disposal Drive	Discovery of disk drives not disposed of properly
Email	Email communication exposed to unintended third party
Fax	Fax communication exposed to unintended third party
Fraud SE	Fraud or scam (usually insider-related), social engineering
Hack	Computer-based intrusion, data not generally publically exposed
Lost Computer	Lost computer (unspecified type in media reports)
Lost Document	Discovery of documents not disposed of properly, not stolen
Lost Drive	Lost data drive, unspecified if IDE, SCSI, thumb drive, etc)
Lost Laptop	Lost laptop (generally specified as a laptop in media reports)
Lost Media	Media (e.g. disks) reported to have been lost by a third party
Lost Mobile	Lost mobile phone or device such as tablets, etc
Lost Tape	Lost backup tapes
Missing Document	Missing document, unknown or disputed whether lost or stolen
Missing Drive	Missing drive, unknown or disputed whether lost or stolen
Missing Laptop	Missing laptop, unknown or disputed whether lost or stolen
Missing Media	Missing media, unknown or disputed whether lost or stolen
Skimming	Using electronic device (skimmer) to swipe victims' credit/debit card numbers
Snail Mail	Personal information in "snail mail" exposed to unintended third party
Snooping	Exceeding intended privileges and accessing data not authorized to view
Stolen Computer	Stolen desktop (or unspecified computer type in media reports)
Stolen Document	Documents either reported or known to have been stolen by a third party
Stolen Drive	Stolen data drive, unspecified if IDE, SCSI, thumb drive, etc
Stolen Laptop	Stolen Laptop (generally specified as a laptop in media reports)
Stolen Media	Media generally reported or known to have been stolen by a third party
Stolen Mobile	Stolen mobile phone or device such as tablets, etc
Stolen Tape	Stolen backup tapes
Unknown	Unknown or unreported breach type
Virus	Exposure to personal information via virus or Trojan (possibly classified as hack)
Web	Web-based intrusion, data exposed to the public via search engines, public pages

Open Security Foundation

Open Security Foundation is a 501(c)(3) non-profit public organization founded and operated by information security enthusiasts. We exist to empower all types of organizations by providing knowledge and resources so that they may properly detect, protect, and mitigate information security risks. http://www.opensecurityfoundation.org

Risk Based Security, Inc.

Risk Based Security, Inc. was established to support organizations with the technology to turn security data into a competitive advantage. Using interactive dashboards and search analytics, RBS offers a first of its kind risk identification and security management tool. RBS further complements the data analytics and vulnerability intelligence with risk-focused consulting services, to address industry specific information security and compliance challenges including ISO/IEC 27001:22005 consulting. http://www.riskbasedsecurity.com

