Data Breach QuickView

Data Breach Trends during the First Nine Months of 2014

Sponsored by:
Risk Based Security

Issued in October 2014

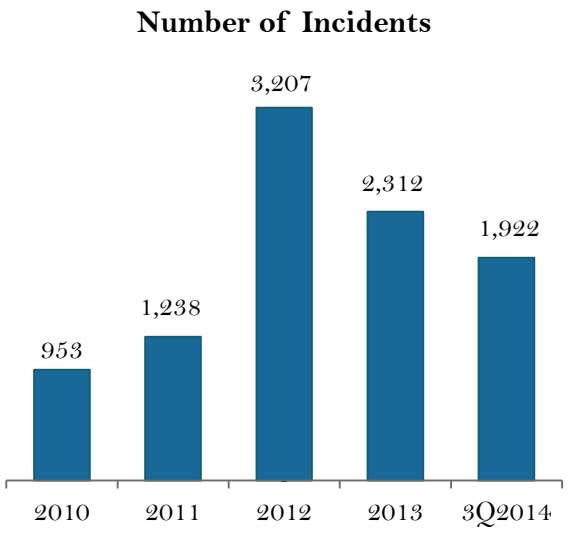
At the ¾ Pole …

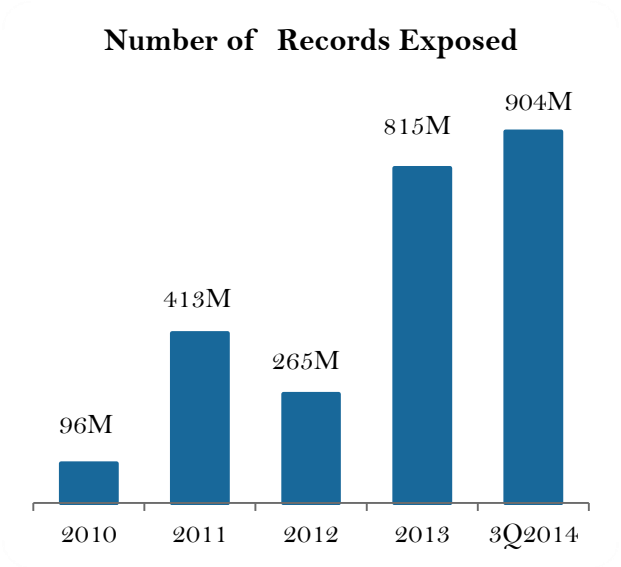
- There were 1922 incidents reported during the first nine months of 2014 exposing 904 million records.
- Three Hacking incidents alone exposed a combined 538 million records.
- A single act of Fraud exposed 104 million records.
- The Business sector accounted for 54.9% of reported incidents, followed by Government (15.2%), Unknown (12.3%), Medical (8.9%), and Education (8.7%).
- The Business sector accounted for 51.9% of the number of records exposed, followed by Unknown (27.4%), and Government (27.4%).
- 74.3% of reported incidents were the result of Hacking, which accounted for 84.8% of the exposed records.
- Fraud accounted for 11.5% of the exposed records, but represented just 2.9% of the reported incidents.
- Breaches involving U.S. entities accounted for 41.1% of the incidents and 48.9% of the exposed records.
- 60.2% of the incidents exposed between one and 1000 records.
- Twenty incidents have exposed one million or more records.
- Four of 2014 incidents have secured a place on the Top 10 All Time Breach List.
- The number of reported incidents tracked by Risk Based Security has exceeded 13,300 exposing over 3.3 billion records.

RiskBased SECURITY

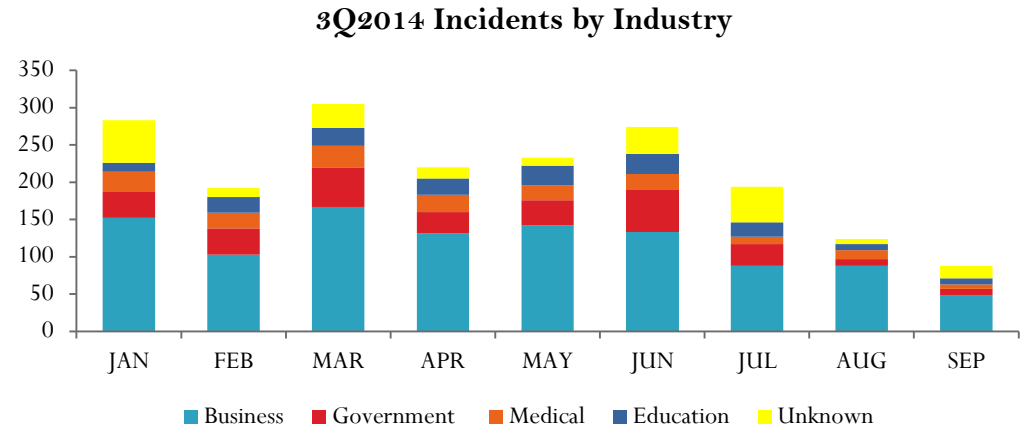
Not Just Security, the Right Security.

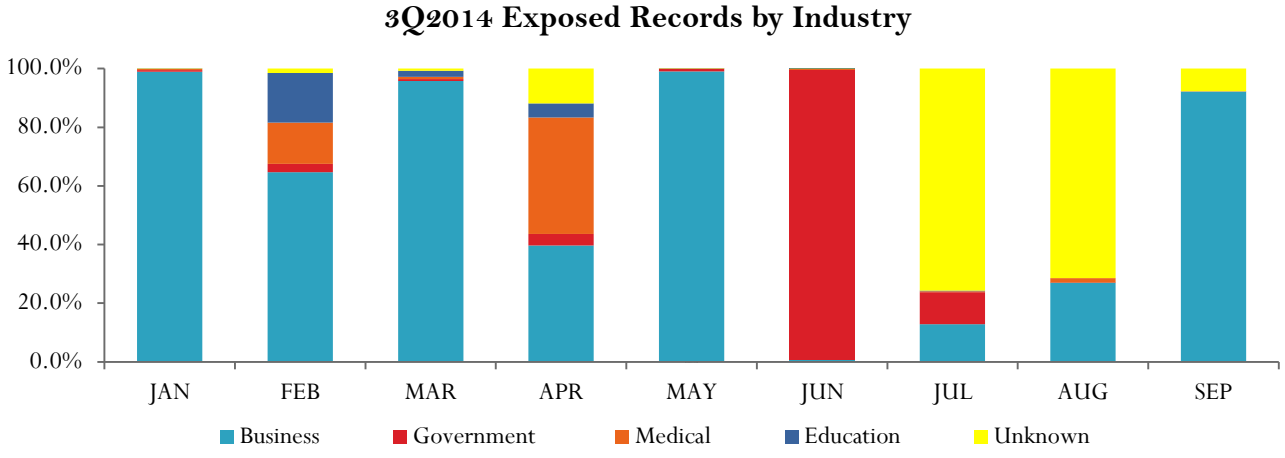
Looking Back at the Last Five Years





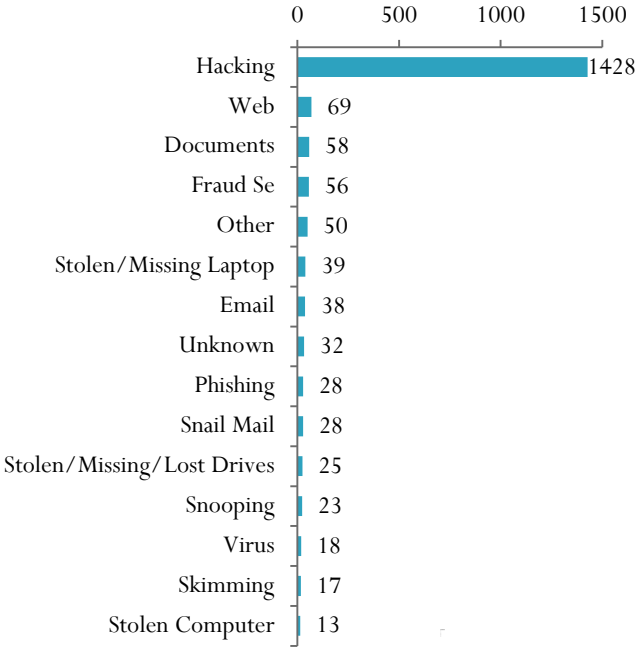
3Q2014 by Industry by Month



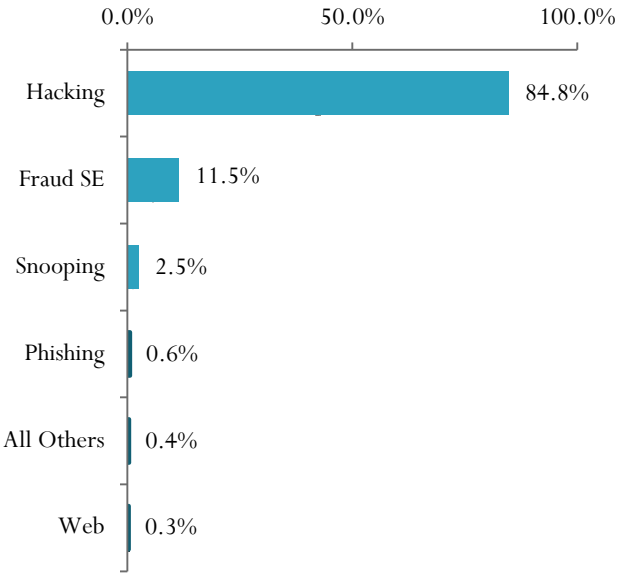


3Q2014 Analysis by Breach Type

3Q2014 Incidents by Breach Type

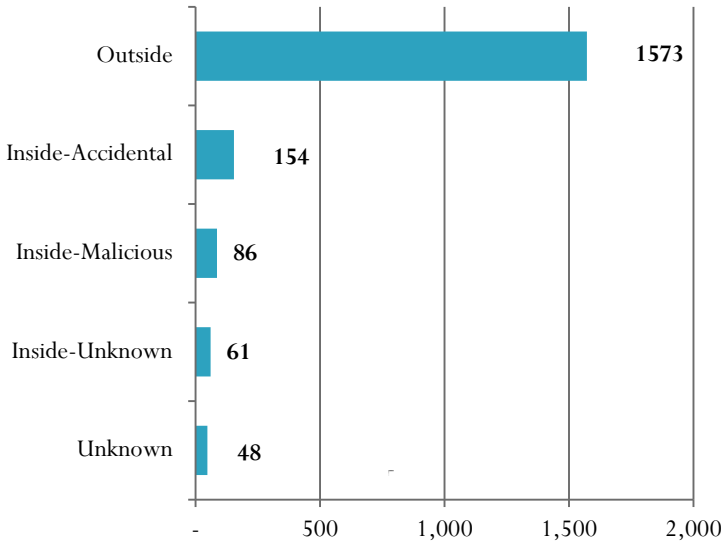


3Q2014 Records Exposed by Breach Type



3Q2014 Analysis by Threat Vector

3Q2014 Incidents by Threat Vector



81.8% of incidents involved outside the organization activity.

3Q2014 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	772,761,099
Inside-Malicious	126,984,593
Inside-Accidental	2,743,931
Inside-Unknown	1,647,903
Unknown	347,259
Total	**904,484,785**

85.4% of the total exposed records are the result of Outside activity.

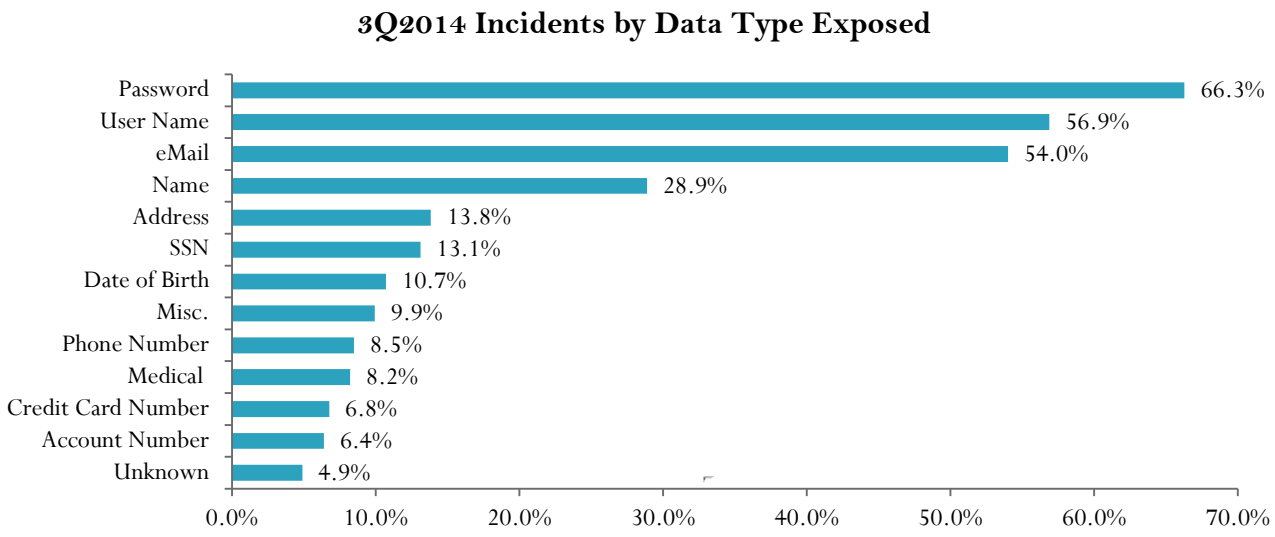
Four incidents, (three Hacks and one Insider Fraud) accounted for 642 million exposed records, (70.9%).

3Q2014 Analysis by Data Family

	Percentage of Total Incidents	Percentage of Total Exposed Records	Percentage of Total Incidents	Percentage of Total Exposed Records
Data Family	**3Q2014**	**3Q2014**	**2013**	**2013**
Electronic	92.3%	99.90%	87.20%	99.90%
Physical	5.5%	<0.1%	9.30%	<0.1%
Other	2.1%	<0.1%	3.20%	<0.1%
Unknown	< 0.1%	< 0.1%	0.03%	< 0.1%

Nearly 93% of all incidents involved electronic data and nearly 100% of the exposed records were in electronic form. A constant theme year over year.

3Q2014 Analysis by Data Type – Percentage of Incidents



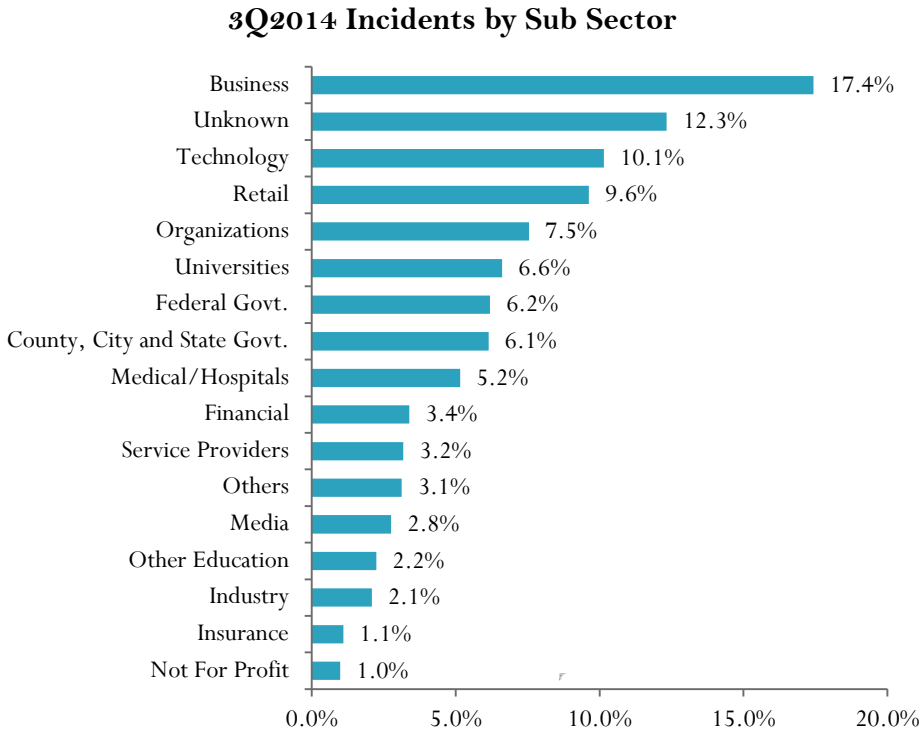
3Q2014 Percentage of Incidents Exposing Data Types vs. 2013

Data Type	3Q2014	2013
Password	66.3%	47.8%
User Name	56.9%	37.4%
eMail	54.0%	39.0%
Name	28.9%	41.4%

User names and passwords remain a prize target.

- 38.7% increase in incidents exposing Passwords over 2013
- 52.1% increase in incidents exposing User Names over 2013

3Q2014 Analysis by Industry Sub Type



- The Business, Unknown and Technology sectors remain in the top three spots in number of incidents.
- Unknown sub-sector accounted for 27.4% of the exposed records followed by Financial at 20.8%, City Government 19.1% and the Business sub-sector at 16.6%. All other sub-sectors accounted for the remaining 16.1%.

3Q2014 Analysis of Records per Incident

Exposed Records	Number of Incidents	Percent of Total
Unknown	294	15.3%
< 1,001	1451	75.5%
< 10,0001	1769	92.0%
< 100,0001	1872	97.4%
< 500,0001	1892	98.4%
< 1,000,0001	1903	99.0%
< 10,000,0001	1913	99.5%
> 10,000,000	9	.5%

The number of incidents with exposed records reported as "Unknown" is 15.3% for the first nine months in 2014 - down from 2013's 26.4%.

- 60.2% of incidents exposed between 1 and 1000 records

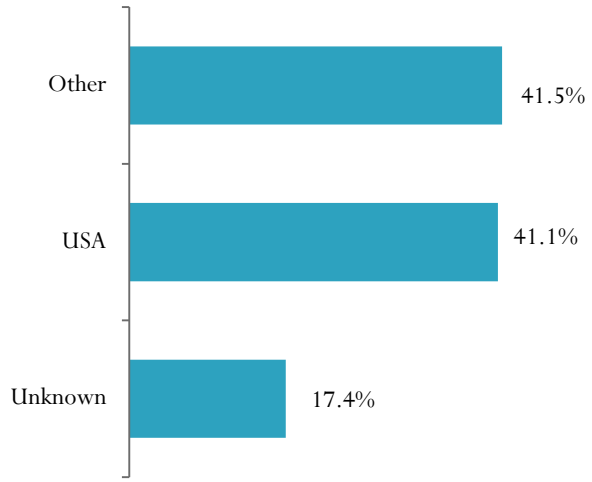
3Q2014 Analysis of Breach Types/Records

Breach Category	Number of Incidents	Number of Records Exposed	Average Records per Incident	Percent of Total Records Exposed
Hacking	1427	766,236,063	536,956	84.8%
Web	69	2,483,104	35,987	.27%
Lost/Stolen/Missing Documents	37	25,356	685	.003%
Fraud/Social Engineering	56	104,148,681	1,859,798	11.51%
Snooping	23	22,781,411	990,496	2.52%
Phishing	28	4,957,128	177,040	.55%
Missing/Lost/Stolen Drive	21	259,538	12,359	.03%
Unknown	32	129,803	4,056	.01%
Stolen/Missing Laptop	35	876,769	25,051	.1%
Snail Mail	28	257,635	9,201	.03%
eMail	38	235,099	6,187	.03%
Virus	18	78,420	4,357	.01%
Improper Disposal	59	37,219	1,283	.004%
Other	51	1,578,195	30,945	.17%
Skimming	17	22,238	1,308	.002%
Stolen Computer	13	378,126	29,087	.04%

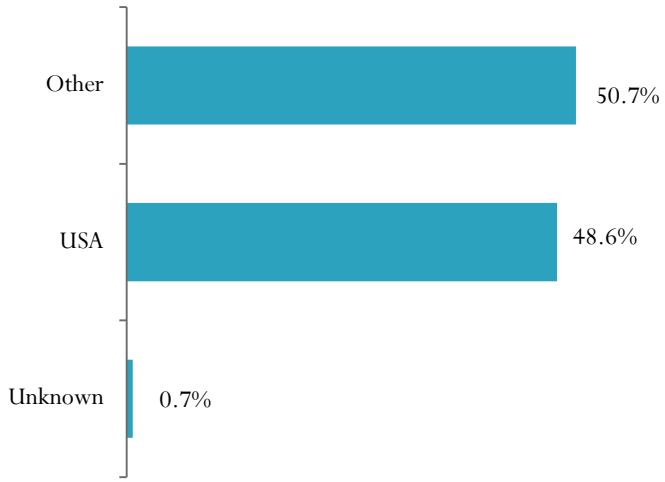
- Insider Fraud is #1 in records per incident.
- Snooping accounted for the 2nd highest records per incident.
- Hacking was #3 in records per incident.

3Q2014 Analysis by Country

3Q2014 Incidents by Location

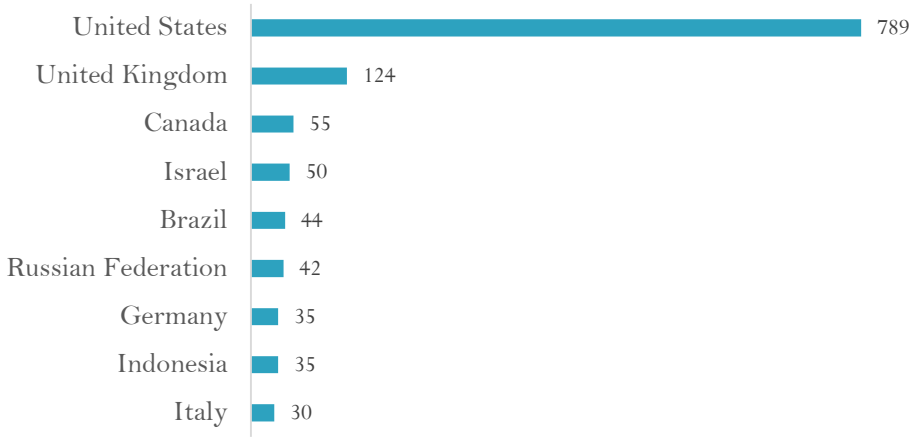


3Q2014 Records by Location



3Q2014 Analysis by Country – Top 10

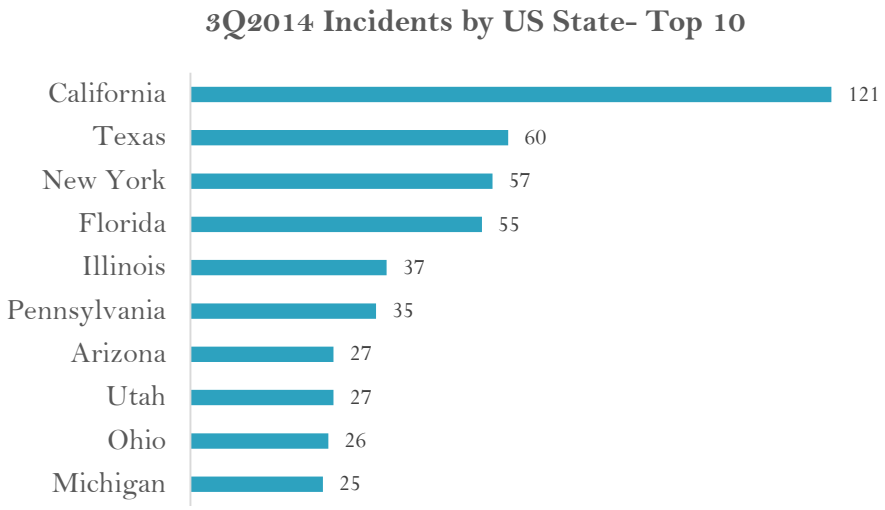
3Q2014 Incidents by Country - Top 10



USA and UK account for 47.5% of incidents.

Exposed Records Ranking	Total Exposed Records	Country	Percentage of Exposed Records
1	439,472,422	United States	48.59%
2	336,016,000	South Korea	37.15%
3	84,220,229	Russian Federation	9.31%
4	23,471,398	Japan	2.60%
5	4,600,408	Panama	.51%
6	2,212,193	United Kingdom	.24%
7	2,116,048	France	.23%
8	1,808,906	Denmark	.20%
9	1,030,220	Ireland	.11%
10	764,464	Canada	.08%

3Q2014 Analysis of US State Rankings



Top 10 represents 59.6% of US incidents.

- Utah, Ohio, Pennsylvania, Texas and New York replace Georgia, Maryland, Massachusetts, North Carolina and "Unknown" in Top 10.

Exposed Records Ranking	US State	Total Exposed Records	Percentage of USA Exposed Records
1	New York	219,360,910	49.91%
2	California	147,430,168	33.55%
3	Georgia	56,121,793	12.77%
4	Tennessee	4,662,238	1.06%
5	Texas	4,546,231	1.03%
6	District of Columbia	1,409,382	.32%
7	Montana	1,300,000	.3%
8	Florida	1,050,197	.24%
9	Maryland	358,982	.08%
10	Pennsylvania	348,738	.08%

Top two states represent 83.46% of exposed US records.

- District of Columbia, Florida, Tennessee, and Georgia replace "Unknown", North Dakota, Illinois, and Idaho in Top 10 from 1Q2014.

Top 10 Incidents All Time

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Highest All Time 8/22/2014	Hack of websites exposes names, registration numbers, usernames and passwords	220 Million	Organization's Name has not been reported	Unknown	South Korea
Number 2 6/21/2014	Hack exposes trip details of customers after de-anonymizing MD5 hashes	173 Million	NYC Taxi & Limousine Commission	Government - City	United States
Number 3 10/3/2013	Hack of company systems exposed customer names, IDs, encrypted passwords and debit/credit card numbers with expiration dates, source code and other information relating to customer orders	152 Million	Adobe Systems, Inc.	Business - Technology	United States
Number 4 3/17/2012	Firm may have illegally bought and sold customers' information	150 Million	Shanghai Roadway D&B Marketing Services Co. Ltd	Business - Data	China
Number 5 5/21/2014	Hack exposes names, encrypted passwords, email addresses, registered addresses, phone numbers and dates of birth	145 Million	eBay, Inc.	Business - Retail	United States
Number 6 6/8/2013	North Korean Hackers expose email addresses and identification numbers	140 Million	Unknown Organizations	Unknown	South Korea
Number 7 1/20/2009	Hack/Malicious Software exposes credit cards at processor	130 Million	Heartland Payment Systems	Business - Finance	United States
Number 8 12/18/2013	Hack exposed customer names, addresses, phone numbers, email addresses, as well as credit/debit card numbers with expiration dates, PINs and CVV numbers	110 Million	Target Brands, Inc.	Business - Retail	United States
Number 9 1/20/2014	Insider Fraud exposed 104 million credit cards with expiration dates, 20 million names, social security numbers and phone numbers	104 Million	Korea Credit Bureau	Business - Finance	South Korea
Number 10 1/17/2007	Hack exposes credit cards and transaction details	94 Million	TJX Companies Inc.	Business - Retail	United States

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, Medical and Unknown.

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 Drive	Discovery of disk drives not disposed of properly
Disposal Mobile	Discovery of mobile devices not disposed of properly
Disposal Tape	Discovery of backup tapes 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
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
Other	Miscellaneous breach type not yet categorized
Phishing	Masquerading as a trusted entity in an electronic communication to obtain data
Seizure	Forcible taking of property by a government law enforcement official
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

Name	Description
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

NO WARRANTY.

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.

In addition to data breach analytics, RBS maintains a comprehensive vulnerability database, allowing organizations to search the most comprehensive and timely list of software and hardware security vulnerability information.

RBS complements our data breach analytics and vulnerability intelligence with risk-focused consulting services, to address industry specific information security and compliance challenges, including ISO/IEC 27001:2013 consulting.

http://www.riskbasedsecurity.com