Data Breach QuickView

2014 Data Breach Trends

Sponsored by:
Risk Based Security

Issued in February 2015

Data Breaches and 2014 …

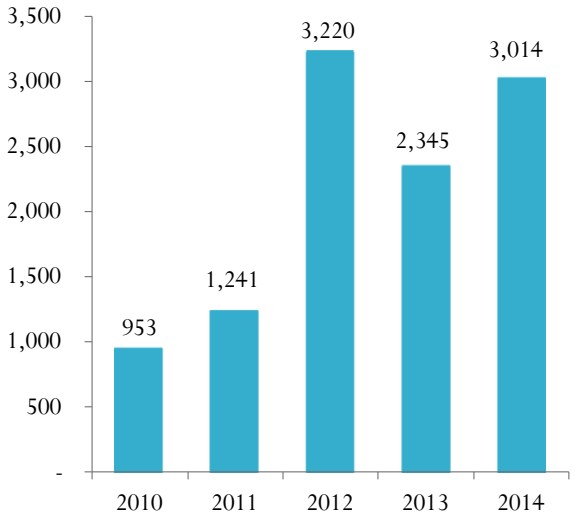
- There were 3,014 incidents reported during 2014 exposing 1.1 billion records.
- Four Hacking incidents alone exposed a combined 647 million records.
- A single act of Fraud exposed 104 million records.
- The Business sector accounted for 52.9% of reported incidents, followed by Government (15.5%), Unknown (13.2%), Medical (9.6%), and Education (8.8%).
- The Business sector accounted for 55.1% of the number of records exposed, followed by Unknown (25.9%), and Government (17.9%).
- 67.7% of reported incidents were the result of Hacking, which accounted for 83.3% of the exposed records.
- Fraud accounted for 14.3% of the exposed records, but represented just 4.3% of the reported incidents.
- Breaches involving U.S. entities accounted for 44.5% of the incidents and 47.9% of the exposed records.
- 35.8% of the incidents exposed between one and 100 records.
- Thirty-one incidents in 2014 exposed more than one million records.
- Five 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 14,400 exposing over 3.6 billion records.

RiskBased SECURITY

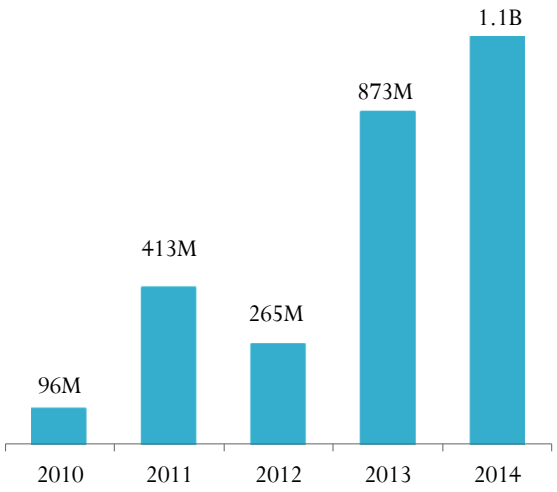
Not Just Security, the Right Security.

2014 Compared to the Past Four Years

Number of Incidents

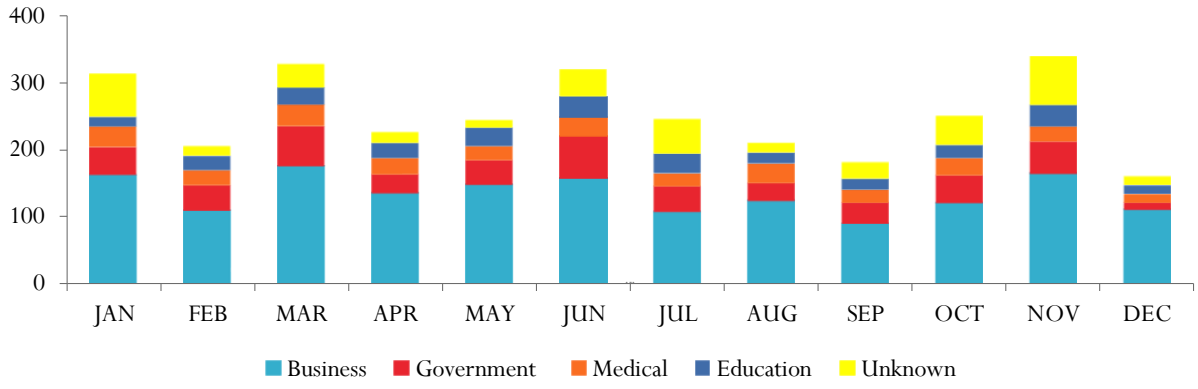


Number of Records Exposed

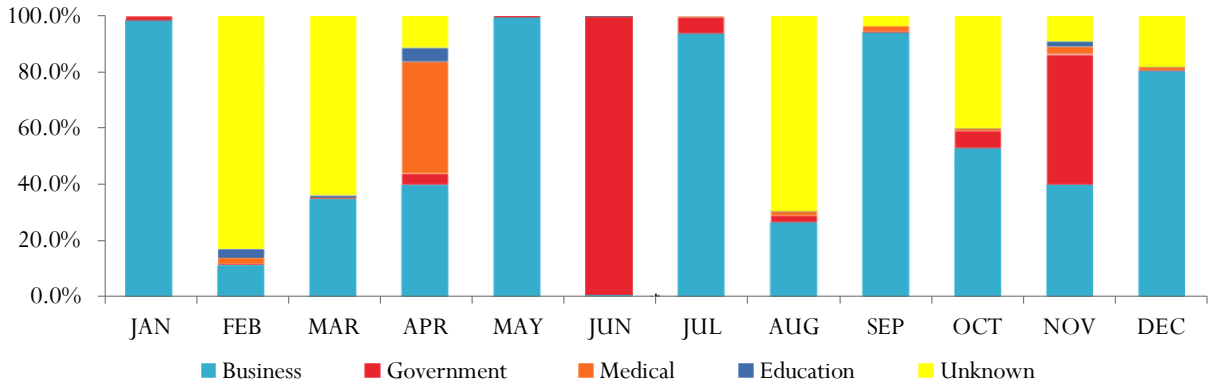


2014 by Industry by Month

2014 Incidents by Industry

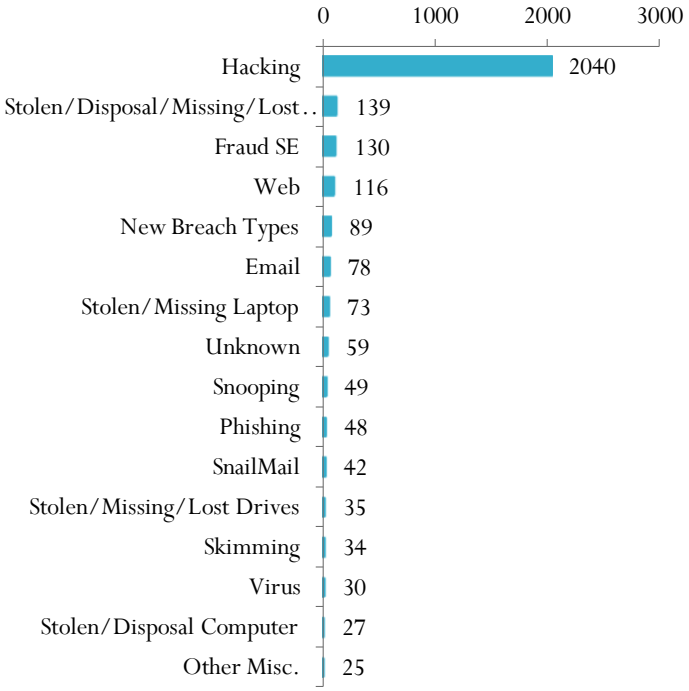


2014 Exposed Records by Industry



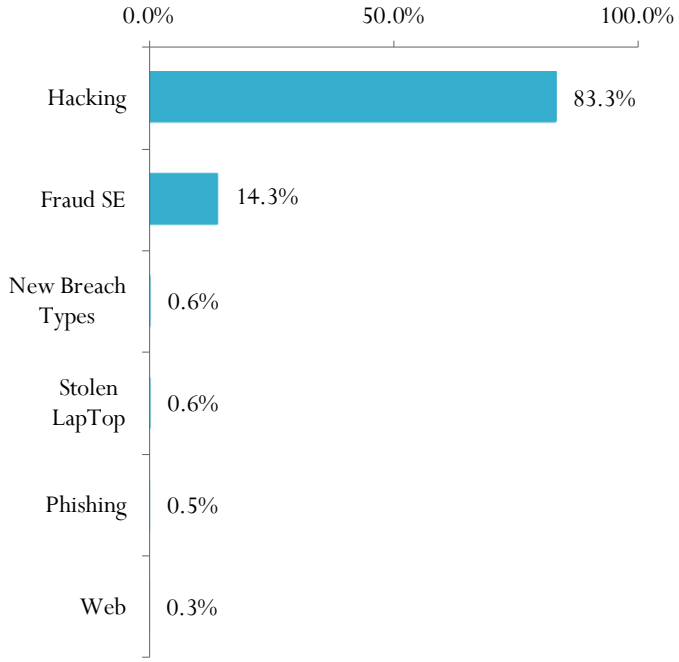
2014 Analysis by Breach Type

2014 Incidents by Breach Type



A number of "New" breach types emerged in 2014, including: "Improper Security Procedure", Unauthorized Publication and Stolen Files.

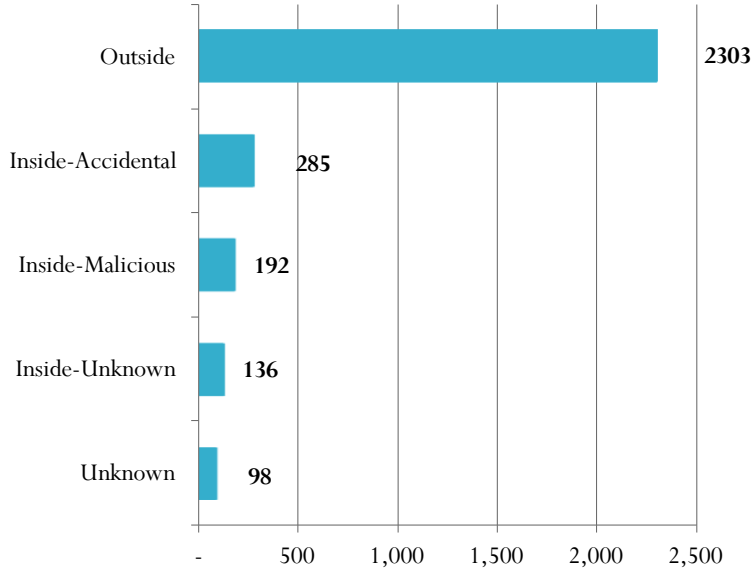
Records Exposed by Breach Type



Hacking and Fraud SE resulted in 95.2% of all exposed records.

2014 Analysis by Threat Vector

2014 Incidents by Threat Vector



76.4% of incidents involved outside the organization activity.

2014 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	896,785,851
Inside-Malicious	160,825,714
Inside-Accidental	3,530,756
Inside-Unknown	6,262,577
Unknown	786,447
Total	**1,068,191,345**

83.9% of the total exposed records are the result of Outside activity.

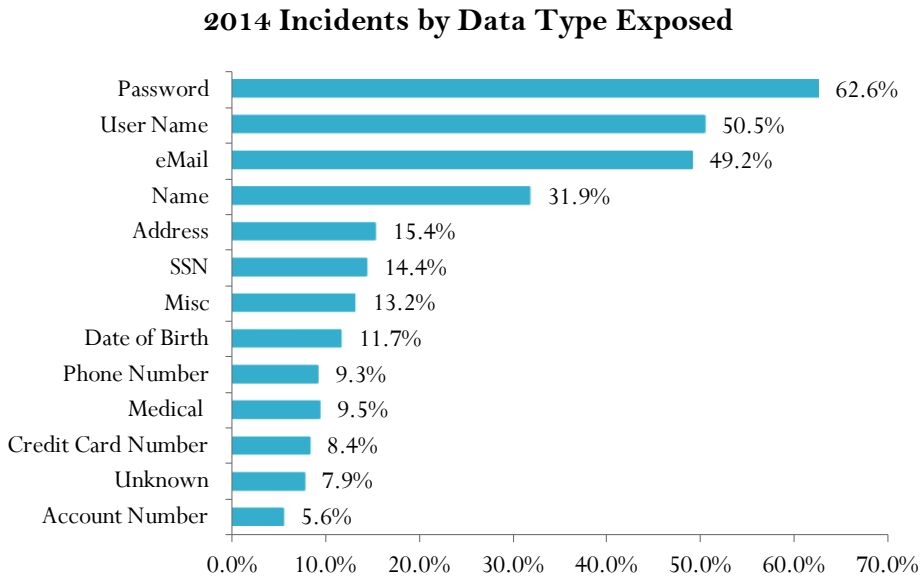
Five incidents, (four Hacks and one Insider Fraud) accounted for 751 million exposed records, (70.3%).

2014 Analysis by Data Family

	Percentage of Total Incidents	Percentage of Total Exposed Records	Percentage of Total Incidents	Percentage of Total Exposed Records
Data Family	2014	2014	2013	2013
Electronic	89.71%	99.90%	87.20%	99.90%
Physical	7.7%	<0.1%	9.30%	<0.1%
Unknown	2.59%	< 0.1%	3.5%	< 0.1%

Nearly 90% of all incidents involved electronic data and nearly 100% of the exposed records were in electronic form. This is a constant theme year over year.

2014 Analysis by Data Type – Percentage of Incidents



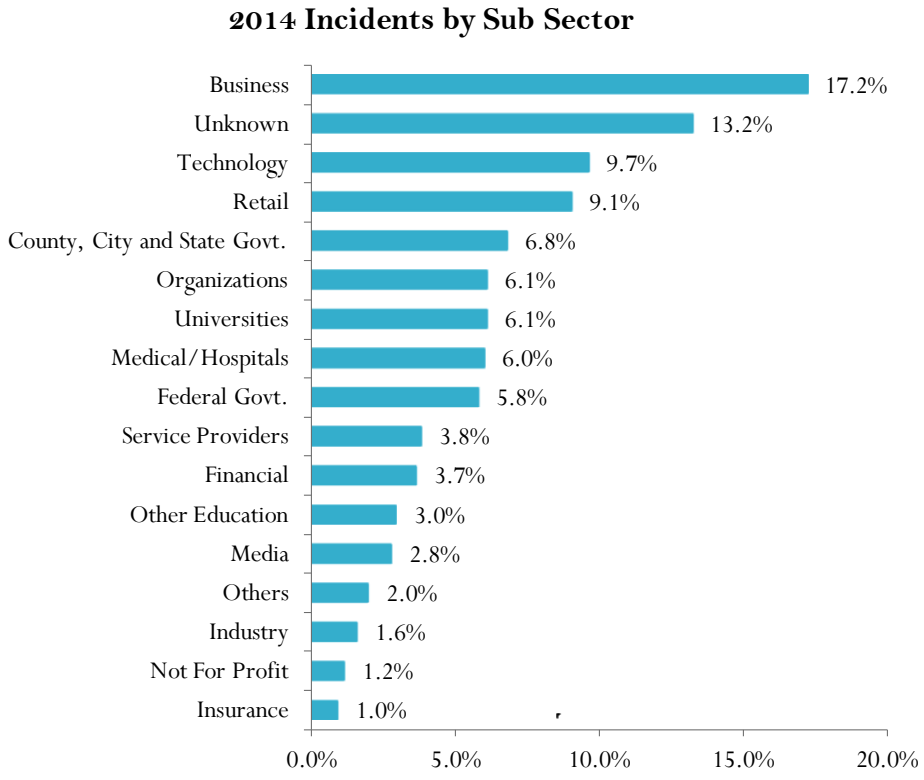
2014 Percentage of Incidents Exposing Data Types vs. 2013

Data Type	2014	2013
Password	62.6%	47.8%
User Name	50.5%	37.4%
eMail	49.2%	39.0%
Name	31.9%	41.4%

User names and passwords remain a prize target.

- 30.9% increase in incidents exposing Passwords over 2013
- 35.0% increase in incidents exposing User Names over 2013

2014 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 25.9% of the exposed records followed by Financial at 17.9%, City Governments at 16.2%, and the Business sub-sector at 14.2%. All other sub-sectors accounted for the remaining exposed records.

2014 Analysis of Records per Incident

Exposed Records	Number of Incidents	Percent of Total
Unknown	578	19.2%
1 to 100	1078	35.8%
101 to 1,000	589	19.5%
1,001 to 10,000	518	17.2%
10,001 to 100,000	175	5.8%
100,001 to 500,000	31	1.0%
500,001 to 1 Million	14	0.5%
1 M to 10 M	20	0.7%
> 10 M	11	0.4%

The number of incidents with exposed records reported as "Unknown" is 19.2% for 2014 - down from 2013's 26.4%.

- 55.3% of incidents exposed between 1 and 1000 records

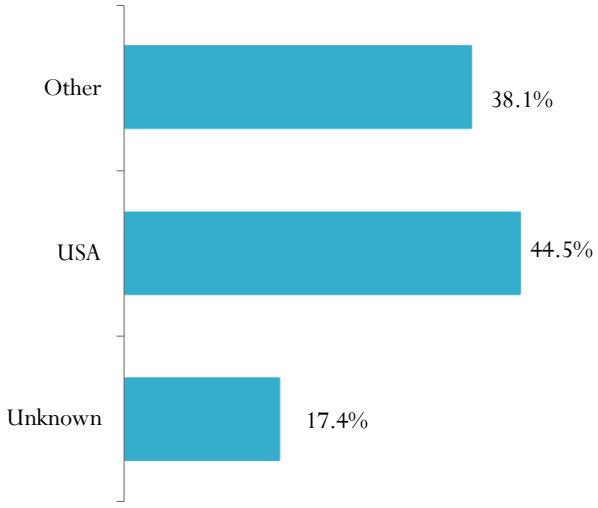
2014 Analysis of Breach Types/Records Exposed – Top 11

Breach Category	Number of Incidents	Number of Records Exposed	Average Records per Incident	Percent of Total Records Exposed
Hacking	2040	889,833,759	436,193	83.30%
Lost/Stolen/Missing Documents	141	249,008	1,766	0.02%
Fraud/Social Engineering	130	152,787,190	1,175,286	14.30%
Web	116	3,317,593	28,600	0.31%
New Breach Types	89	6,243,309	70,150	0.58%
Email	78	351,709	4,509	0.03%
Stolen/Missing Laptop	73	6,044,790	82,805	0.57%
Unknown	59	232,010	3,932	0.02%
Snooping	49	188,060	3,838	0.02%
Phishing	48	5,036,467	104,926	0.47%
Seizure	2	2,097,000	1,048,500	0.20%

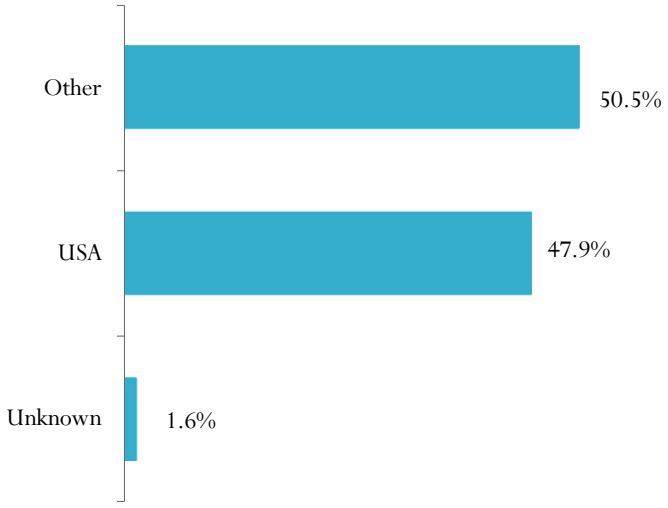
- Insider Fraud is #1 in records per incident.
- Seizure accounted for the 2nd highest records per incident.
- Hacking was #3 in records per incident.

2014 Analysis by Country

2014 Incidents by Location



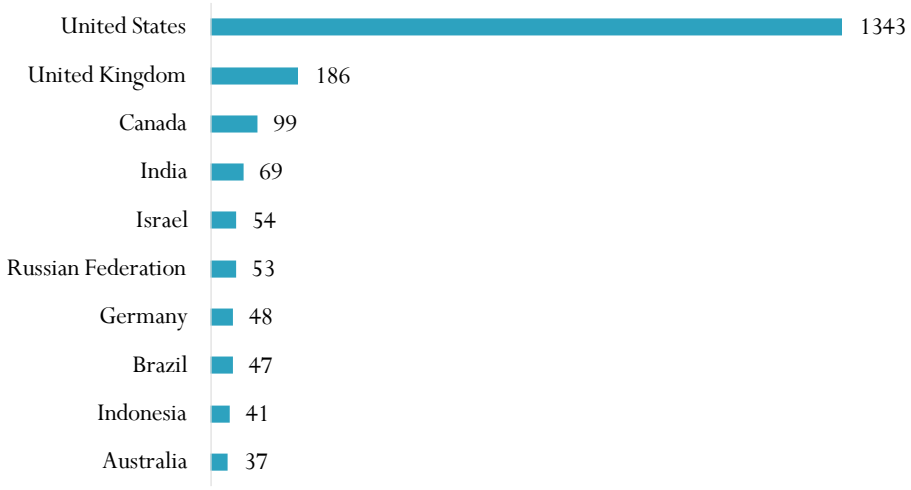
2014 Records by Location



- There were 87 countries reporting at least one data breach in 2014.
- With a median of 5 data breaches and a median of one.

2014 Analysis by Country – Top 10

2014 Incidents by Country - Top 10



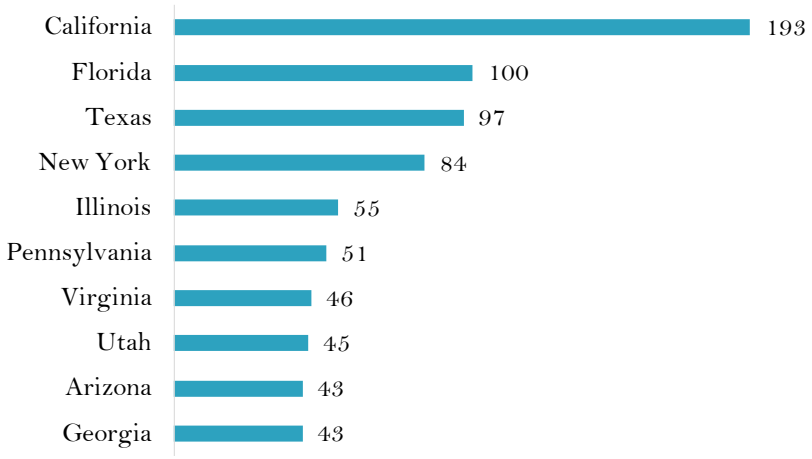
USA and UK account for 50.7% of incidents.

2014 Exposed Records by Country – Top 10

Exposed Records Ranking	Total Exposed Records	Average Records per Incident	Country	Percentage of Exposed Records
1	512,137,986	381,338	United States	46.48%
2	385,746,000	42,861,777	Republic of Korea	39.10%
3	84,221,387	1,589,082	Russian Federation	8.54%
4	23,504,871	2,475,871	Japan	2.38%
5	16,099,087	30,993	Unknown	1.63%
6	4,600,408	2,300,204	Panama	0.47%
7	2,707,287	246,117	Turkey	0.27%
8	3,503,581	18,836	United Kingdom	0.25%
9	2,116,719	78,397	France	0.21%
10	1,811,307	86,252	Denmark	0.18%

2014 Analysis of US State Rankings

2014 Incidents by US State- Top 10



Top 10 represent 25.1% of US incidents.

- Virginia and Georgia replace Ohio and Michigan in Top 10.

Exposed Records Ranking	US State	Total Exposed Records	Exposed Records/Incident	Percentage of USA Exposed Records
1	NY	219,604,392	2,614,338	42.9%
2	CA	147,562,327	764,572	28.8%
3	GA	109,130,008	2,537,907	21.3%
4	TX	6,777,520	69,871	1.3%
5	AZ	5,260,134	122,329	1.0%
6	TN	4,710,801	196,283	0.9%
7	WI	2,457,811	204,818	0.5%
8	PA	1,531,527	30,030	0.3%
9	DC	1,411,882	78,438	0.3%
10	MT	1,301,900	325,475	0.3%

Top two states represent 71.7% of exposed US records.

- District of Columbia, Florida, Tennessee, and Georgia replace "Unknown", North Dakota, Illinois, and Idaho in Top 10 from 3Q2014.

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 exposed customer names, IDs, encrypted passwords and debit/ credit card numbers with expiration dates, source code and other customer order information.	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.	110 Million	Target Brands, Inc.	Business - Retail	United States
Number 9 9/2/2014	Hack exposed the details from 56 million payment cards and an additional 53 million customer email addresses.	109 Million	Home Depot	Business - Retail	United States
Number 10 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

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

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

