Data Breach QuickView

Data Breach Trends in the First Quarter of 2014

Sponsored by:
Risk Based Security
Open Security Foundation

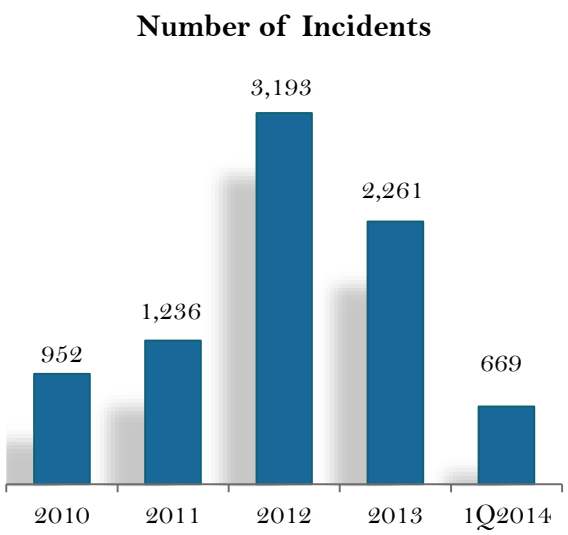
April 2014

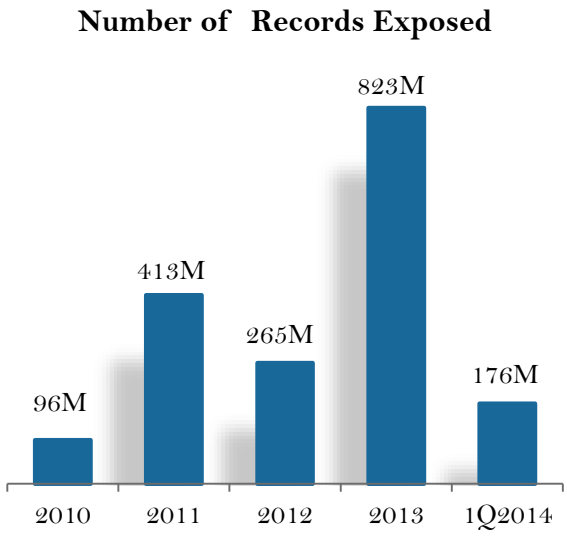
1Q2014 at a Glance …

- There were 669 incidents reported during the first three months of 2014 exposing 176 million records.
- A single incident of insider Fraud involving Korea Credit Bureau exposed 104 million credit cards with expiration dates, 20 million names, social security numbers and phone numbers.
- The Business sector accounted for 57.5% of reported incidents, followed by Government (15.7%), Unknown (13.0%), Education (7.3%), and Medical (6.4%).
- The Business sector accounted for 98.3% of the number of records exposed.
- 79.4% of reported incidents were the result of Hacking, but only accounted for 14.4% of the exposed records.
- Fraud accounted for 59.1% of the exposed records, but represented just 1.9% of the reported incidents.
- Breaches involving U.S. entities accounted for 37.1% of the incidents and 29.3% of the exposed records.
- 62.9% of the incidents exposed between one and 1000 records.
- Six incidents exposed more than one million records.
- One 1Q2014 incident has secured a place on the Top 10 All Time Breach List, (Korea Credit Bureau).

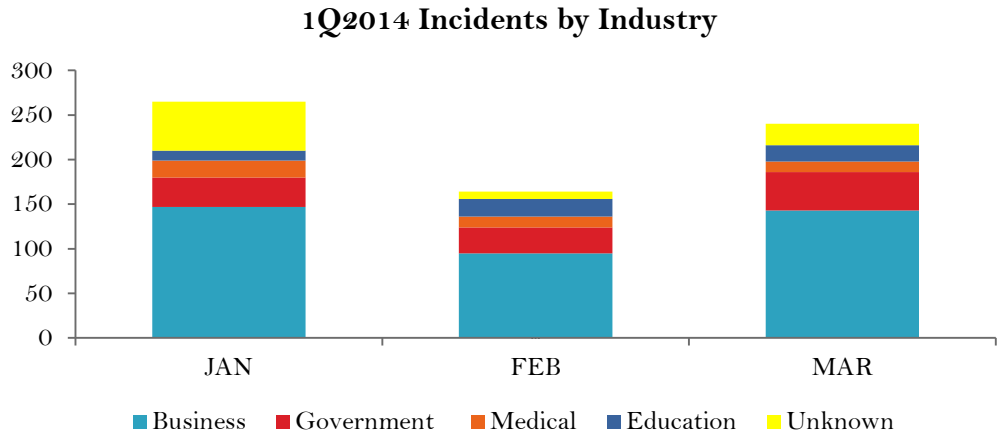
The number of reported incidents tracked by Risk Based Security exceeded 12,100 exposing over 2.6 billion records.

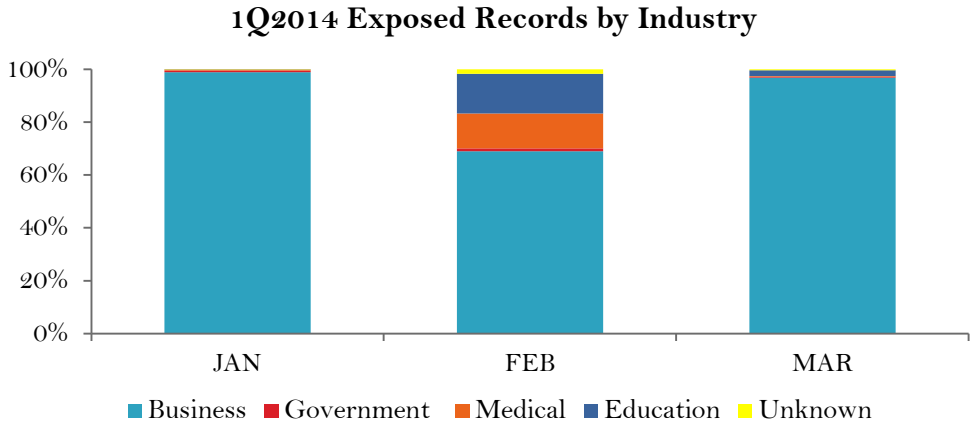
Looking Back at the Last Five Years



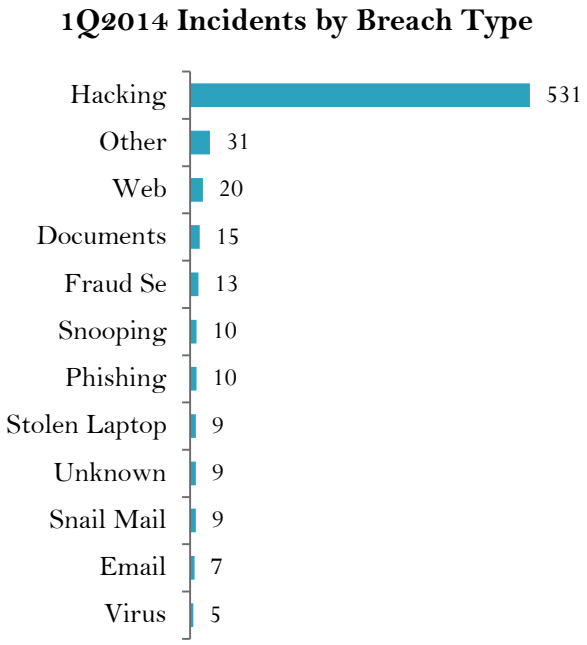


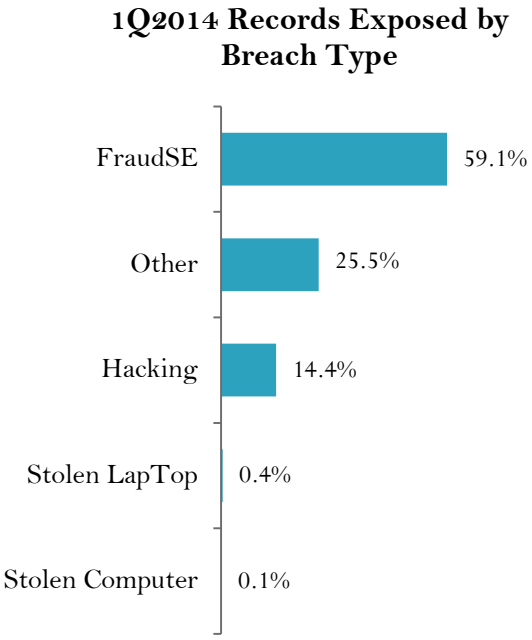
1Q2014 by Industry by Month



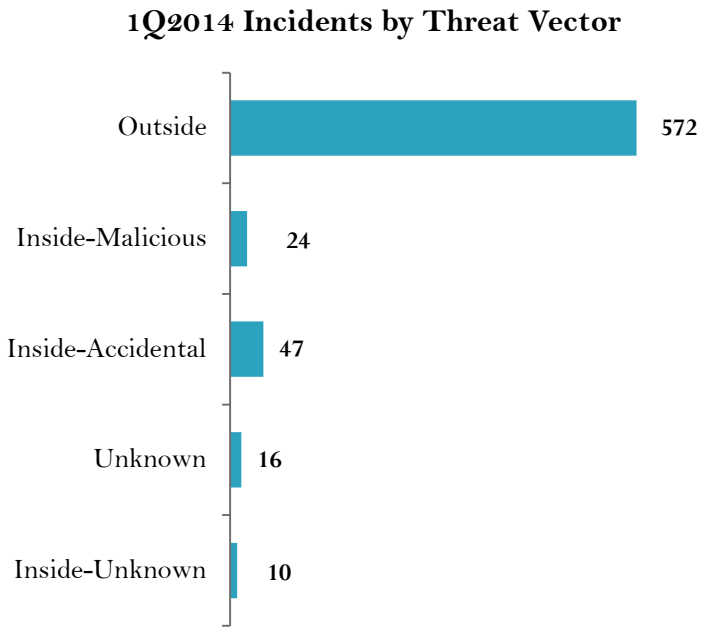


1Q2014 Analysis by Breach Type





1Q2014 Analysis by Threat Vector



85.5% of incidents involved outside the organization activity.

1Q2014 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	71,485,795
Inside-Malicious	104,198,237
Inside-Accidental	292,414
Unknown	108,416
Inside-Unknown	76,850
Total	**176,161,712**

59.4% of the total exposed records are the result of Insider activity.

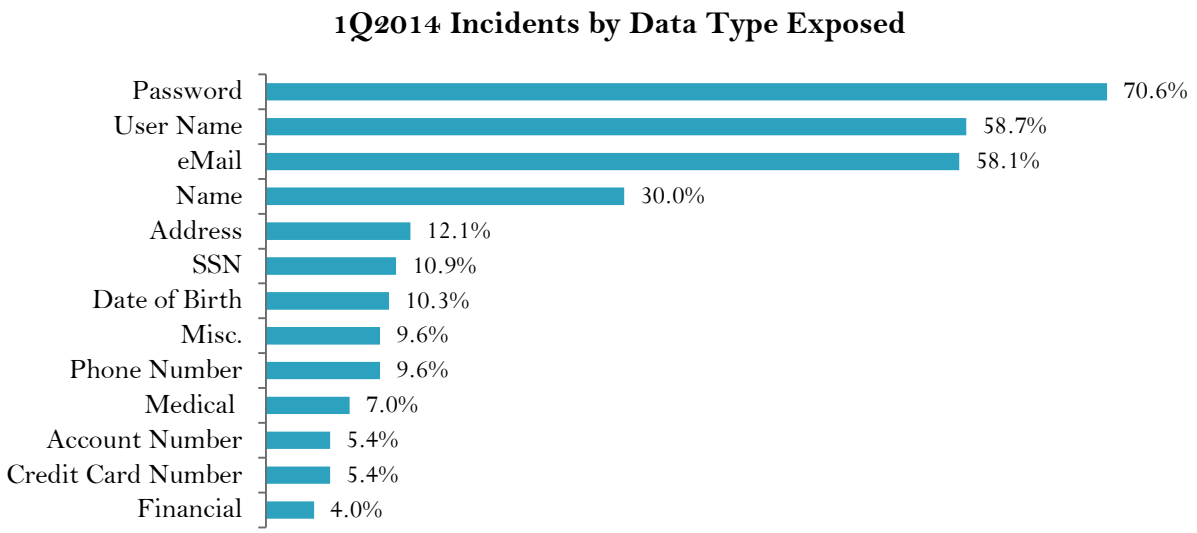
A single incident exposed credit card information of 104 million customers through Insider Fraud.

1Q2014 Analysis by Data Family

	Percentage of Total Incidents	Percentage of Total Exposed Records	Percentage of Total Incidents	Percentage of Total Exposed Records
Data Family	**1Q2014**	**1Q2014**	**2013**	**2013**
Electronic	92.80%	99.90%	87.20%	99.90%
Physical	4.60%	<0.1%	9.30%	<0.1%
Other	2.50%	<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.

1Q2014 Analysis by Data Type – Percentage of Incidents



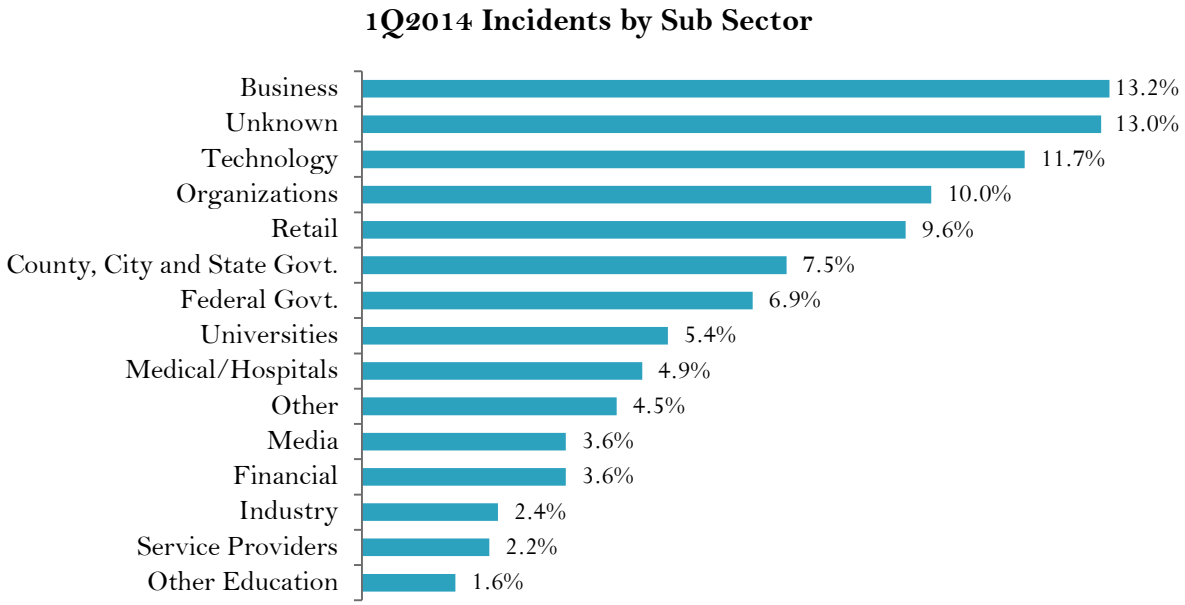
1Q2014 Percentage of Incidents Exposing Data Types vs. 2013

Data Type	1Q2014	2013
Password	70.6%	47.8%
User Name	58.7%	37.4%
eMail	58.1%	39.0%
Name	30.0%	41.4%

User names and passwords offer greater pay-off?

- 47.7% increase in incidents exposing Passwords over 2013
- 56.9% increase in incidents exposing User Names over 2013

1Q2014 Analysis by Industry Sub Type



- The Business and Technology sectors remain in the top two spots in number of incidents.
- Although the percentage of incidents classified as Unknown sector nearly doubled during 1Q2014 over 2013, the number of exposed records remained very low.
- The Financial sector accounted for 59.1% of the exposed records followed by Technology at 35.8% and Retail at 2.3%. All others accounted for less than 1.0%.

1Q2014 Analysis of Records per Incident

Exposed Records	Number of Incidents	Percent of Total
Unknown	75	11.2%
< 1,001	499	74.6%
< 10,0001	616	92.1%
< 100,0001	651	97.3%
< 500,0001	660	98.7%
< 1,000,0001	663	99.1%
< 10,000,0001	666	99.6%
> 10,000,000	3	0.4%

The number of incidents with exposed records reported as "Unknown" is 11.2% for 1Q2014 - down from 2013's 26.4%.

- 63.4% of incidents exposed between 1 and 1000 records

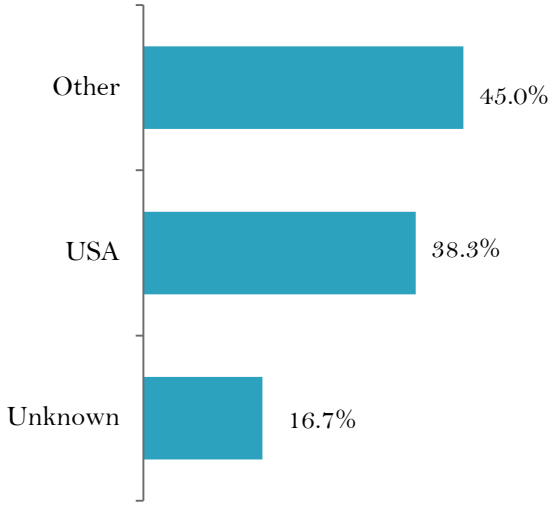
1Q2014 Analysis of Breach Types/Records

Breach Category	Number of Incidents	Number of Records Exposed	Average Records per Incident	Percent of Total Records Exposed
Hacking	530	70,421,697	132,871	39.98%
Web	21	252,871	12,041	0.14%
Lost/Stolen/Missing	16	8,518	532	0.00%
Fraud/Social Engineering	14	104,020,681	7,430,049	59.05%
Snooping	11	154,600	14,055	0.09%
Phishing	10	14,094	1,409	0.01%
Missing/Lost/Stolen Drive	10	70,787	7,079	0.04%
Unknown	9	74,018	8,224	0.04%
Stolen Laptop	9	701,753	77,973	0.40%
Snail Mail	9	111,282	12,365	0.06%
eMail	7	7,686	1,098	0.00%
Virus	6	54,700	9,117	0.03%
Improper Disposal	6	29,877	4,980	0.02%
Other	4	4,696	1,174	0.00%
Skimming	4	55	14	0.00%
Stolen Computer	3	234,397	78,132	0.13%

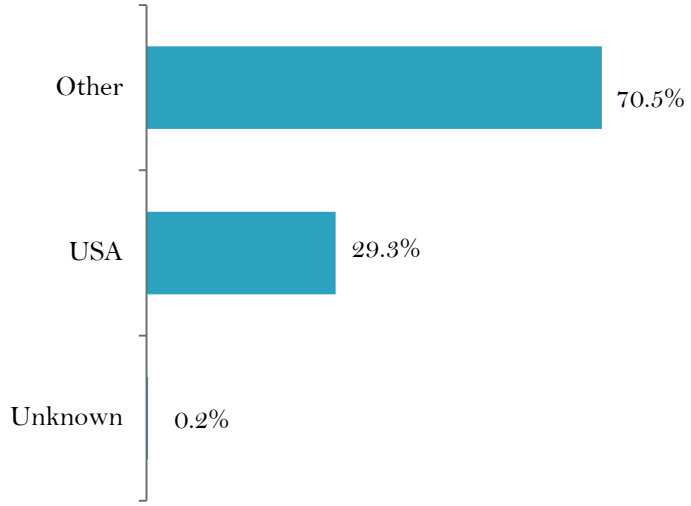
- A single Insider Fraud accounted for 104 million records
- Hacking accounted for the 2nd highest records per incident average
- Stolen Laptop was #3 in records per incident and #3 in percentage of records exposed

1Q2014 Analysis by Country

1Q2014 Incidents by Location

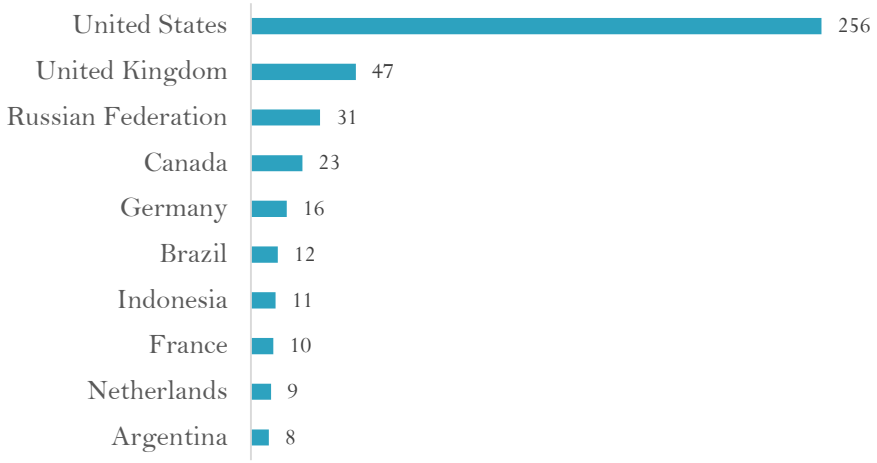


1Q2014 Incidents by Location



1Q2014 Analysis by Country – Top 10

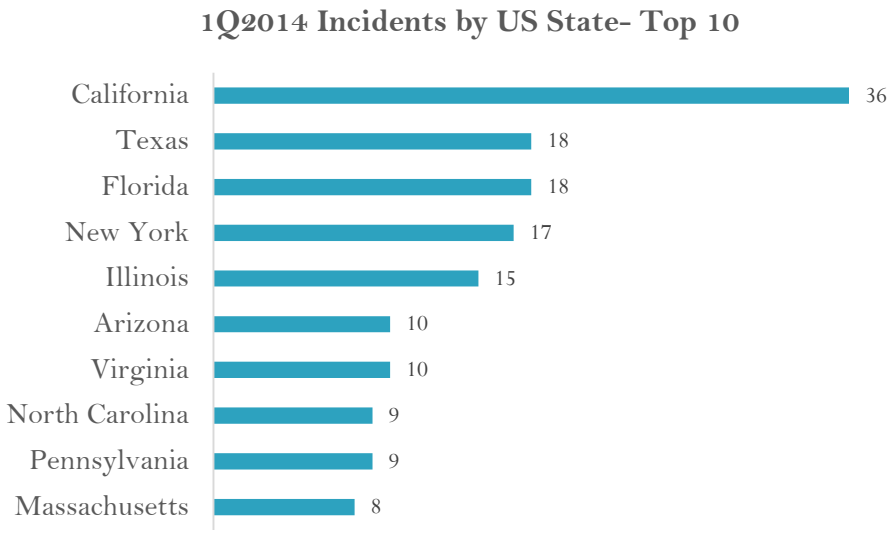
1Q2014 Incidents by Country - Top 10



USA and UK account for 45.3% of incidents.

Exposed Records Ranking	Total Exposed Records	Country	Percentage of Exposed Records
1	126,000,000	South Korea	71.53%
2	51,552,255	United States	29.26%
3	4,600,000	Panama	2.61%
4	1,057,016	Syria	0.60%
5	800,670	France	0.45%
6	676,422	Canada	0.38%
7	610,208	Australia	0.35%
8	300,285	United Kingdom	0.17%
9	42,799	Japan	0.02%
10	17,426	Russian Federation	0.01%

1Q2014 Analysis of US State Rankings



Top 10 represents 58.5% of US incidents.

- North Carolina and Virginia replace Maryland and Georgia in Top 10

Exposed Records Ranking	US State	Total Exposed Records	Percentage of Exposed Records
1	New York	45,021,766	87.33%
2	Texas	4,424,650	8.58%
3	California	366,728	0.71%
4	Maryland	300,263	0.58%
5	North Dakota	290,780	0.56%
6	Unknown	253,479	0.49%
7	Illinois	231,592	0.45%
8	Washington	106,757	0.21%
9	Georgia	100,777	0.20%
10	Massachusetts	77,957	0.15%

Top two states represent 95.9% of exposed US records.

- Four states, California, Illinois, New York and Texas remain in Top 10 from 2013

Repeat Offenders

1Q2014 Review: 97 Organizations were repeat offenders in 1Q2014

Is it the lure of the data that keeps some organizations in the crosshairs? Or is it their lack of security processes that make them easy targets and hard to pass-up? It's hard to tell with the available information but something seems to be very wrong at a number of organizations that appear on the "Repeat Offender" list year after year.

Just in the first quarter of 2014, 97 organizations were breached for the second, third, fourth and in one case the 52nd time over the last eight years. Nearly 15%, of the breaches disclosed in 1Q2014 represented a subsequent incident for the impacted organization. Three organizations reported multiple incidents during the first quarter of 2014.

Businesses, primarily financial institutions and data brokers, topped the list with 44 multiple incident organizations. The education sector, primarily universities, comes in second with 26 incidents followed by government (18) and medical (9).

Hacking continues to stand out as the leading breach type in multiple incident organizations representing 55.7% of all incidents in 1Q2014.

Top 10 Incidents All Time

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Highest All Time 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 2 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 3 6/8/2013	North Korean Hackers expose email addresses and identification numbers	140 Million	Unknown Organizations	Unknown	South Korea
Number 4 1/20/2009	Hack/Malicious Software exposes credit cards at processor	130 Million	Heartland Payment Systems	Business - Finance	United States
Number 5 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 6 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 7 1/17/2007	Hack exposes credit cards and transaction details	94 Million	TJX Companies Inc.	Business - Retail	United States
Number 8 6/1/1984	Hack exposes credit-reporting database	90 Million	TRW	Business - Data	United States
Number 9 7/16/2008	Glitch during testing new design exposed users' birth dates	80 Million	Facebook, Inc.	Business-Technology	United States
Number 10 4/26/2011	Hack exposes names, addresses, email addresses, birthdates, PlayStation Network/ Qriocity passwords and logins, PSN online ID, profile data, purchase history and possibly credit card numbers	77 Million	Sony Corporation	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

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

The Open Security Foundation runs the DataLossDB research project aimed at documenting known and reported data breach incidents world-wide as well as OSVDB project that provides accurate, detailed, current, and unbiased technical information on security vulnerabilities.

http://datalossdb.org/

http://osvdb.org/

http://www.opensecurityfoundation.org

