Data Breach QuickView

2015 Data Breach Trends

Sponsored by:
Risk Based Security

Issued in January 2016

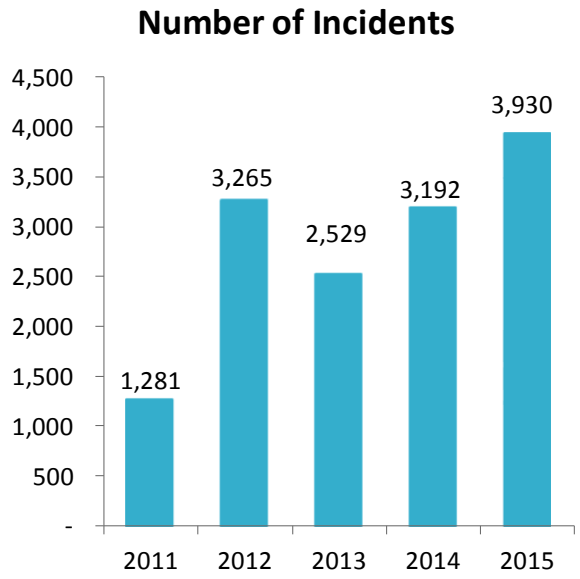
Data Breaches and 2015 …

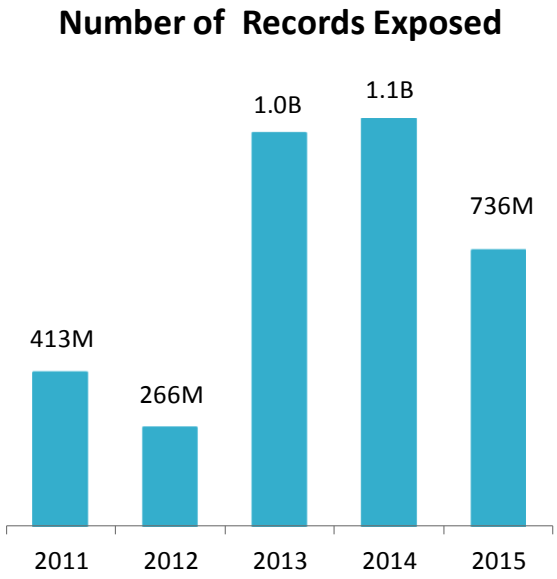
- There were 3930 incidents reported during 2015 exposing 736 million records.
- Four Hacking incidents alone exposed a combined 237.8 million records.
- A single database mis-configuration exposed 191 million records on the Internet.
- The Business sector accounted for 47.2% of reported incidents, followed by Unknown (19.9%), Education (13.9%), Government (12.2%), and Medical (6.8%).
- The Business sector accounted for 51.4% of the number of records exposed, followed by Unknown (34.3%), Government (12.8%) and Medical (1.5%).
- 64.6% of reported incidents were the result of Hacking, which accounted for 58.7% of the exposed records.
- Web accounted for 30.6% of the exposed records, but represented just 2.8% of the reported incidents.
- Breaches involving U.S. entities accounted for 40.5% of the incidents and 64.7% of the exposed records.
- 55.4% of the incidents exposed between one and 1000 records.
- 288 incidents involved Third Parties
- Forty-six incidents in 2015 exposed more than one million records.
- Three of 2015 incidents have secured a place on the Top 20 All Time Breach List.
- The number of reported incidents tracked by Risk Based Security has exceeded 18,900 exposing over 4.6 billion records.

RiskBased SECURITY

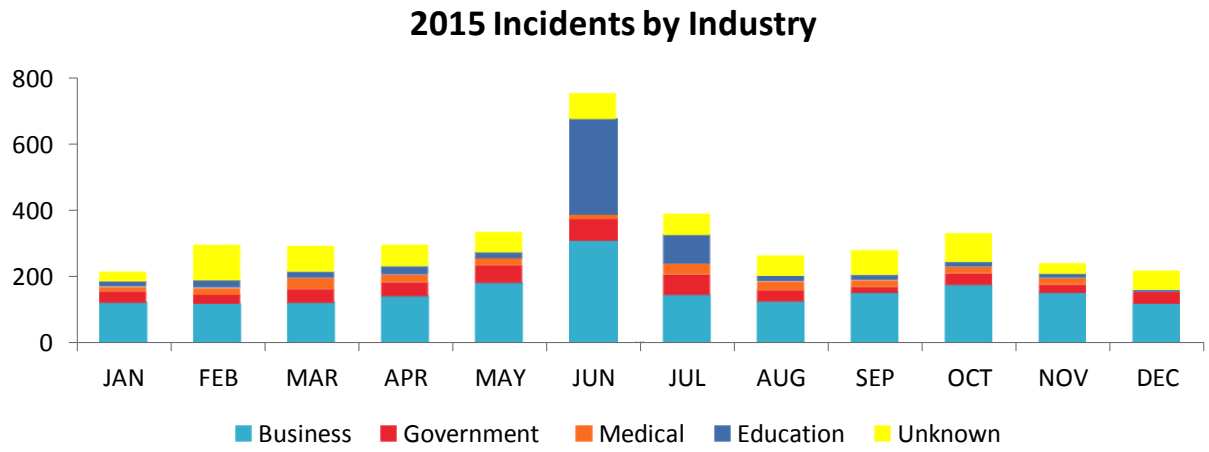
Not Just Security, the Right Security.

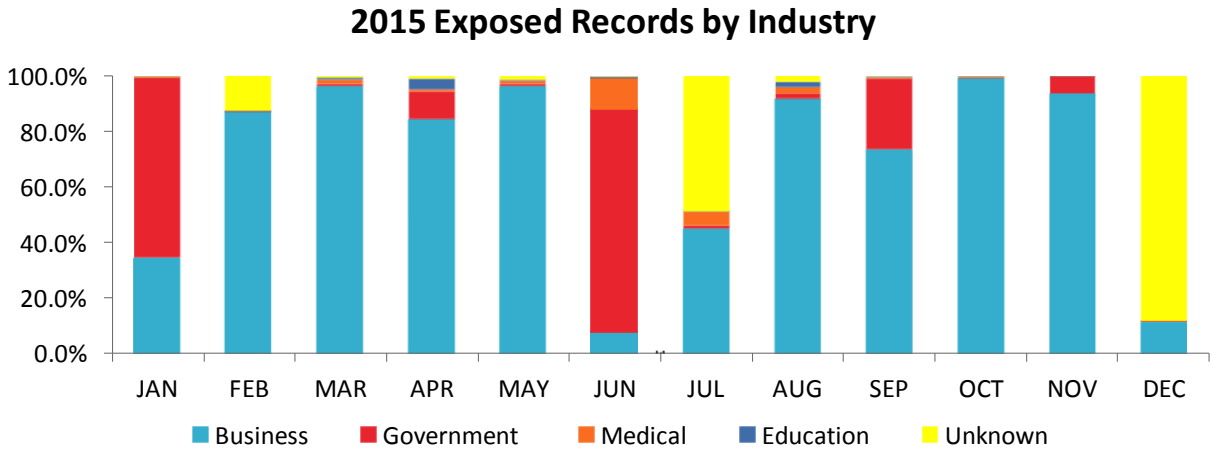
2015 Compared to the Past Four Years





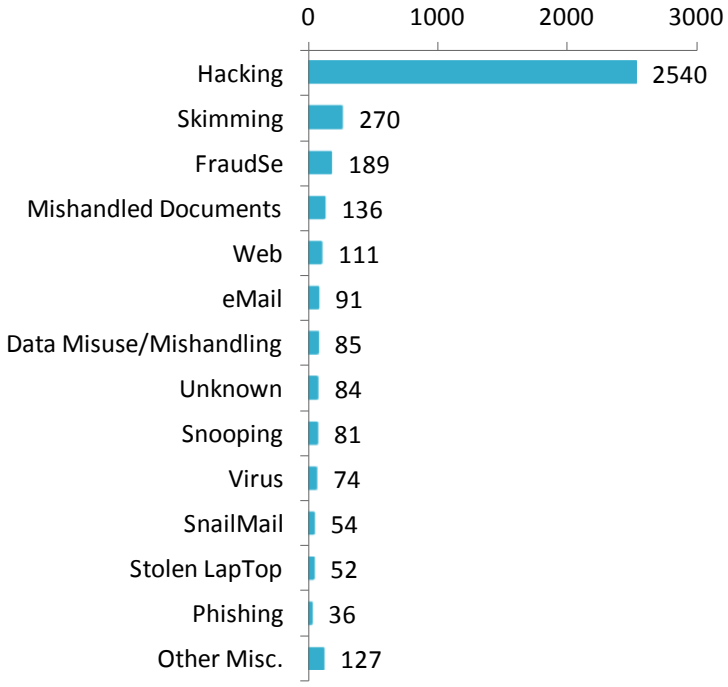
2015 by Industry by Month





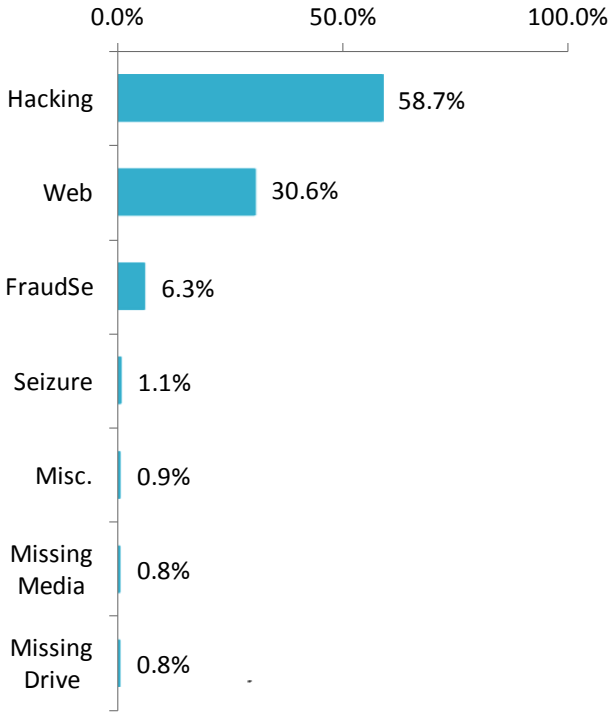
2015 Analysis by Breach Type

2015 Incidents by Breach Type



A number of "New" breach types emerged in 2015 and will be incorporated into the 2016 reporting.

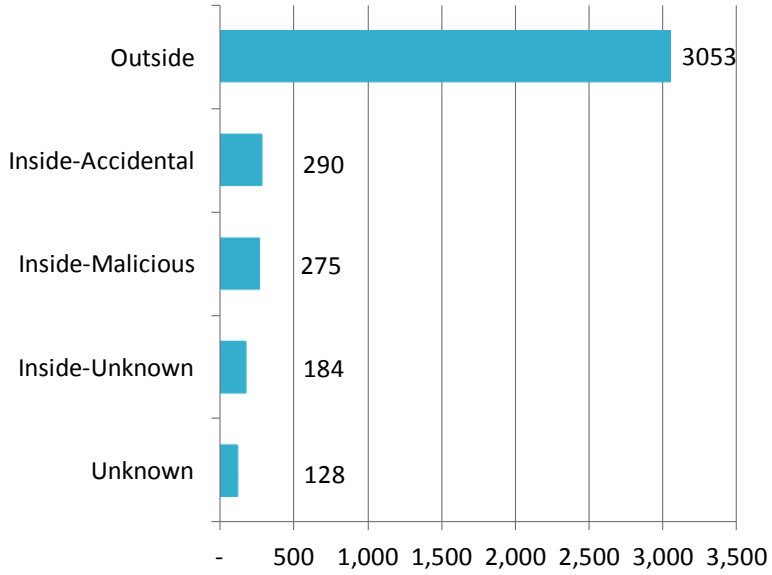
Records Exposed by Breach Type



Hacking and Web resulted in 89.3% of all exposed records.

2015 Analysis by Threat Vector

2015 Incidents by Threat Vector



77.7% of incidents involved outside the organization activity.

2015 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	375,768,013
Inside-Accidental	236,404,844
Inside-Malicious	73,814,654
Inside-Unknown	49,431,541
Unknown	769,798
Total	**736,188,850**

51.0% of the total exposed records are the result of Outside activity.

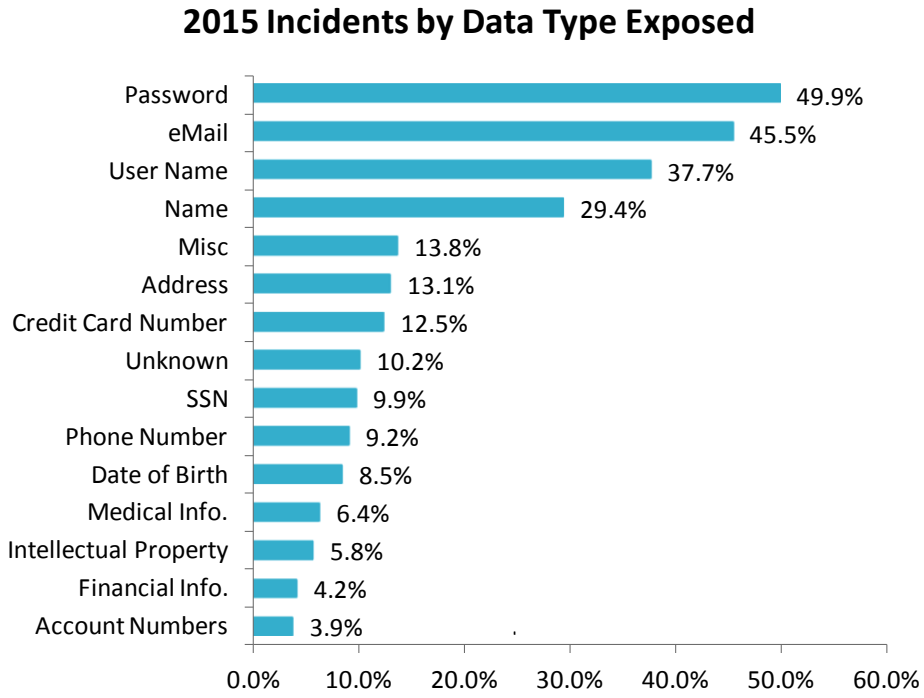
Six incidents, (four Hacks, one Insider Fraud and one Web), accounted for 473.1 million exposed records, (64.3%).

2015 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**	**2015**	**2015**
Electronic	89.7%	99.9%	89.9%	99.7%
Physical	7.7%	<0.1%	7.0%	<0.15%
Unknown	2.6%	< 0.1%	3.1%	< 0.15%

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.

2015 Analysis by Data Type – Percentage of Incidents



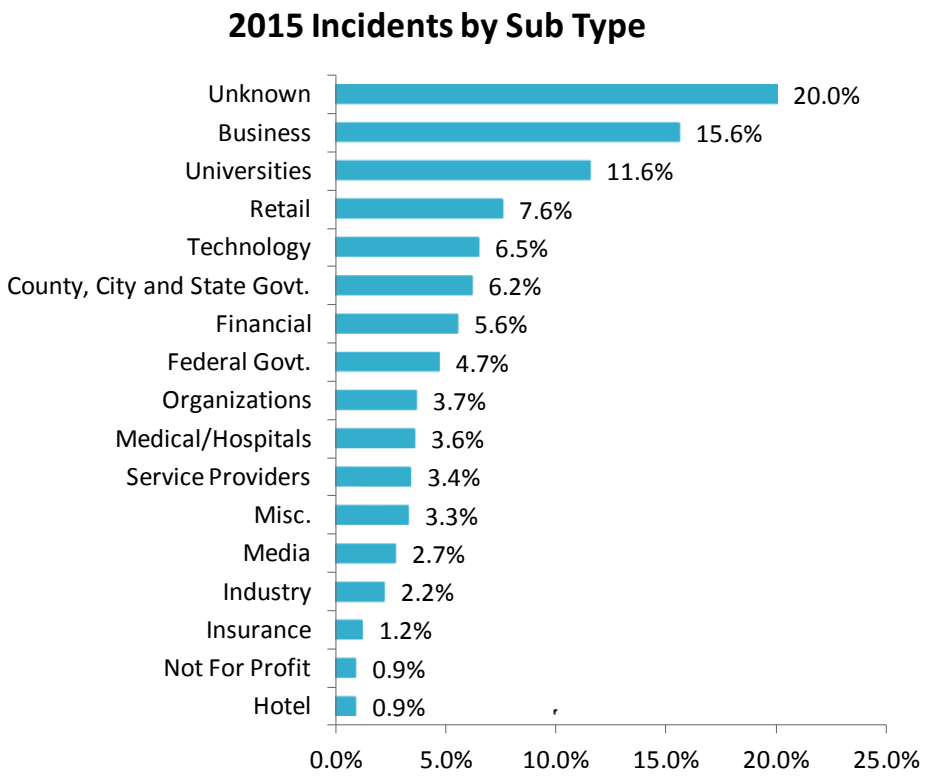
Passwords and eMail Addresses remain a prize target.

2015 Percentage of Incidents Exposing Data Types vs. 2014

Data Type	2014	2015
Password	62.6%	49.9%
eMail	49.2%	45.5%
User Name	50.5%	37.7%
Name	31.9%	29.4%

Close to 50% of all incidents expose Passwords and eMail Addresses.

2015 Analysis by Industry Sub Business Type



- Business and Unknown sub types remain in the top two spots with Universities coming in at number three in number of incidents.
- Unknown sub-sector accounted for 34.3% of the exposed records followed by Technology at 24.1%, Insurance at 13.7% and the Government sub-sector at 12.7%. All other sub-sectors accounted for the remaining exposed records.

2015 Analysis of Records per Incident

Exposed Records	Number of Incidents	Percent of Total
Unknown	1132	28.8%
1 to 100	1469	37.4%
101 to 1,000	708	18.0%
1,001 to 10,000	415	10.6%
10,001 to 100,000	109	2.8%
100,001 to 500,000	37	.9%
500,001 to 999,999	14	0.4%
1 M to 10 M	32	0.8%
> 10 M	16	0.4%

The number of incidents with exposed records reported as "Unknown" is 28.8% for 2015 – up from 2014's 19.2%.

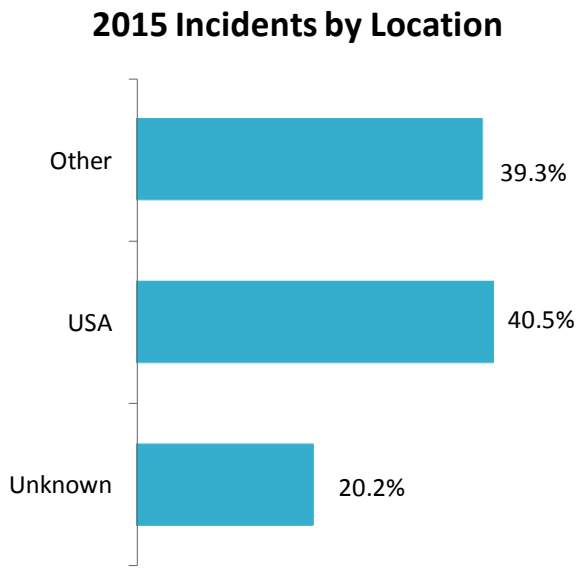
- 55.4% of incidents exposed between 1 and 1000 records, level from 2014.

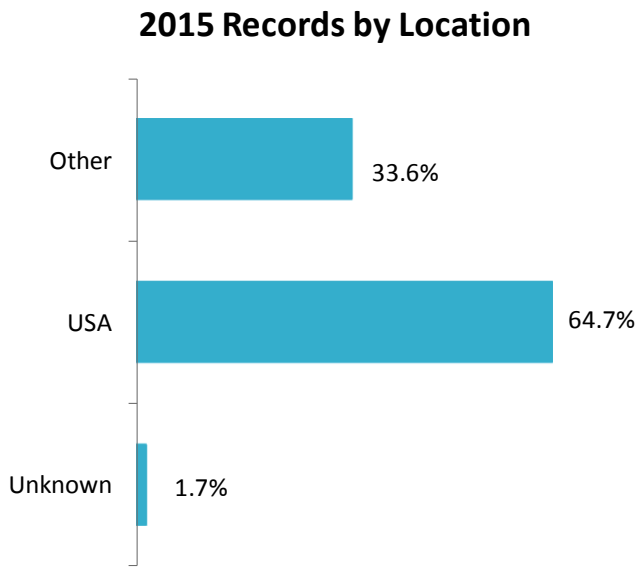
2015 Analysis of Breach Types/Records Exposed – Top 10

Breach Category	Number of Incidents	Number of Records Exposed	Average Records per Incident	Percent of Total Records Exposed
Hacking	2540	432,546,155	170,294	58.75%
Web	111	225,390,562	2,030,546	30.62%
Fraud/Social Engineering	189	46,237,521	244,643	6.28%
Seizure	2	7,850,000	3,925,000	1.07%
Misc.	117	6,809,243	58,199	0.92%
Missing Media	3	6,246,954	2,082,318	0.85%
Missing Drive	15	6,076,849	405,123	0.83%
Phishing	36	1,516,965	42,138	0.21%
Virus	73	1,473,666	20,187	0.20%
Unknown	84	1,031,467	12,279	0.14%

- Seizure is #1 in records per incident.
- Missing Media accounted for the 2nd highest records per incident.
- Web was #3 in records per incident.

2015 Analysis by Country

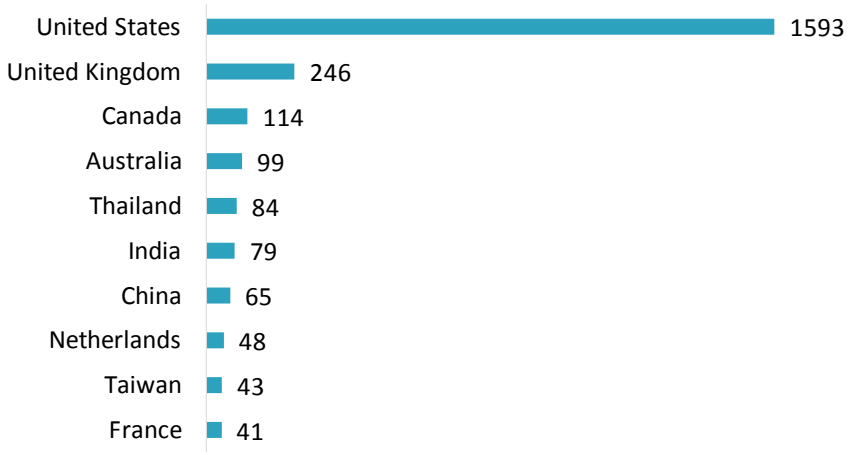




- There were 111 countries reporting at least one data breach in 2015.
- With the Top 10 countries accounting for 61.4% of the incidents.

2014 Analysis by Country – Top 10

2015 Incidents by Country - Top 10

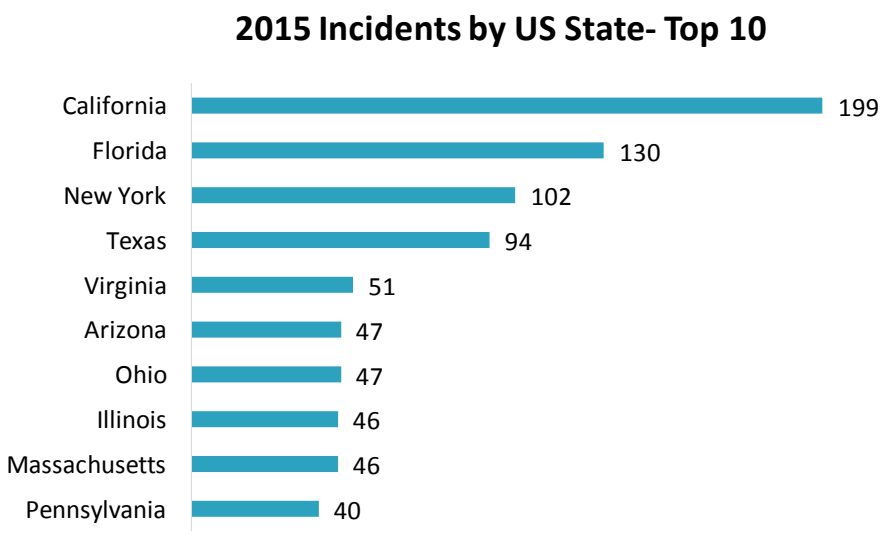


USA and UK account for 46.8% of incidents.

2015 Exposed Records by Country – Top 10

Exposed Records Ranking	Country	Total Exposed Records	Average Records per Incident	Percentage of Exposed Records
1	United States	476,156,734	298,906	64.68%
2	Republic of Turkey	50,000,910	2,941,230	6.79%
3	Republic of Korea	44,168,681	2,324,667	6.00%
4	Canada	45,131,583	395,891	6.13%
5	Russian Federation	26,721,624	2,055,510	3.63%
6	United Kingdom	21,583,574	87,738	2.93%
7	Germany	13,715,607	342,890	1.86%
8	Hong Kong	11,333,302	596,490	1.54%
9	Pakistan	10,057,197	558,733	1.37%
10	Japan	9,907,474	330,249	1.35%

2015 Analysis of US State Rankings



Top 10 represent 50.3% of US incidents.

- California stays at number one with Florida moving into the number two spot.

Exposed Records Ranking	US State	Total Exposed Records	Exposed Records/Incident	Percentage of USA Exposed Records
1	Unknown	225,892,113	1,751,102	47.4%
2	Indiana	83,217,029	2,377,629	17.5%
3	Texas	70,373,482	748,654	14.8%
4	District of Columbia	21,962,859	954,907	4.6%
5	California	19,253,058	96,749	4.0%
6	Washington	11,549,561	398,261	2.4%
7	New York	11,529,576	113,035	2.4%
8	Arkansas	11,001,576	1,833,596	2.3%
9	Georgia	6,362,038	163,129	1.3%
10	Colorado	4,658,426	160,635	1.0%

Top two states represent 64.9% of exposed US records.

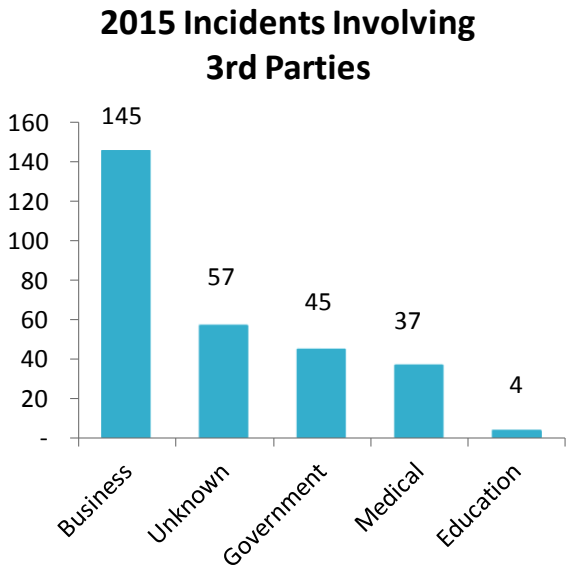
- Indiana's 35 incidents top records per incident calculation.

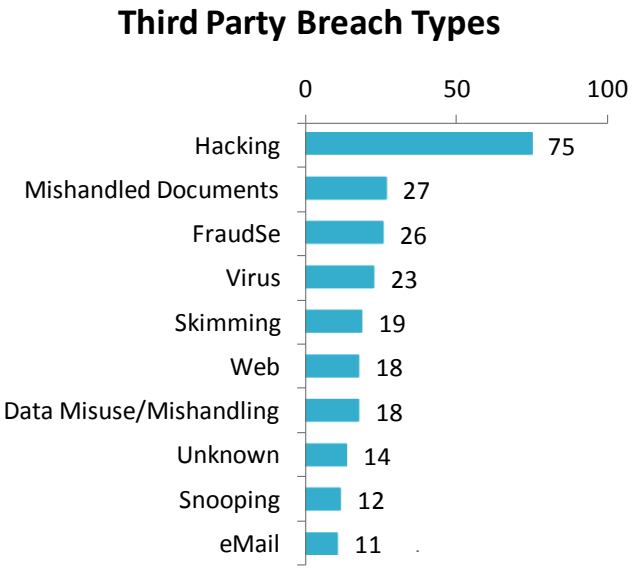
2015 Analysis of Business Types

Business Type	Incidents	Exposed Records	Average Records per Breach	#1 Breach Type (Incidents)	#2 Breach Type (Incidents)
Business	1851	376,581,685	203,448	Hack (68.2%)	Skimming (12.8%)
Education	546	789,995	1,447	Hack (86.2%)	eMail (3.0%)
Medical	265	9,794,920	36,962	Hack (16.3%)	Snooping (15.8%)
Government	477	93,438,021	195,887	Hack (49.0%)	Misc. (9.1%)
Unknown	780	251,382,027	322,285	Hack (82.2%)	Skimming (5.6%)

Business Type	#1 Sector (Incidents)	#2 Sector (Incidents)	#1 Exposed Data Type	#2 Exposed Data Type	#1 Sector (Records)	#2 Sector (Records)
Business	Retail (16.6%)	Technology (13.8%)	Passwords (52.4%)	User Names (42.5%)	Technology (48.0%)	Insurance (27.9%)
Education	University (83.0%)	High School (5.9%)	Passwords (57.3%)	User Names (52.4%)	University (91.4%)	High School (1.0%)
Medical	Provider (51.1%)	Hospital (26.7%)	Name (63.8%)	Medical Info. (56.2%)	Provider (52.6%)	Technology (39.9%)
Government	Federal (38.9%)	City (19.9 %)	Name (38.2%)	Password (31.4%)	Federal (85.0%)	State (13.3%)
Unknown	N/A	N/A	eMail (75.0%)	Password (64.1%)	N/A	N/A

2015 Incidents Involving Third Parties



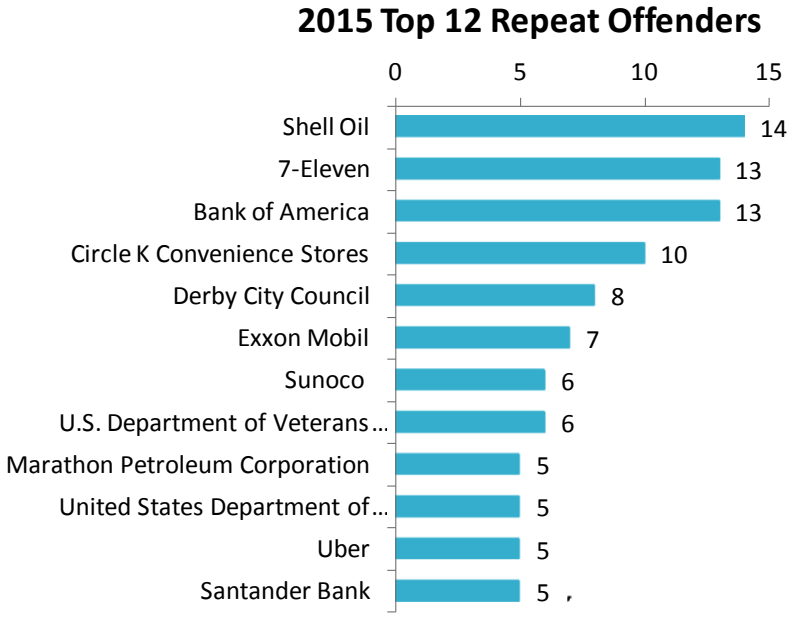


2015 Repeat Offenders

One Hundred Forty-two (142) organizations have multiple reported data breaches in 2015.

2015 saw 142 organizations reporting multiple incidents, with four organizations reporting in the double digits. It remains hard to tell the root cause in each case with the available information, but something seems to be very wrong at a number of organizations that appear not to be learning from their mistakes.

Government agencies top the 2015 list with 37 multiple incident organizations. The retail sector comes in second with 32 multiple incident organizations and Education, primarily universities, comes in third with 27 multiple incident organizations.



Four energy companies in the Top 12 multiple incident organizations.

- Skimming at Gas pumps on the rise impacting Energy sector.
- Hacking continues to stand out as the leading breach type in multiple incident organizations.

Top 20 Incidents All Time (Exposed Records Count)

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 12/28/2015	Mis-configured database exposes voter names, dates of birth, addresses, phone numbers, political party affiliations, genders, and other assorted personal details	191 Million	Organization's Name has not been reported	Unknown	United States
Number 3 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 4 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 5 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 6 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 7 6/8/2013	North Korean Hackers expose email addresses and identification numbers	140 Million	Unknown Organizations	Unknown	South Korea
Number 8 1/20/2009	Hack/Malicious Software exposes credit cards at processor	130 Million	Heartland Payment Systems	Business - Finance	United States
Number 9 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 10 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

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Number 11 1/17/2007	Hack exposes credit card numbers and transaction details	94 Million	TJX Companies Inc.	Retail	United States
Number 12 6/1/1984	Hackers access credit-reporting database	90 Million	TRW	Data	United States
Number 13 8/27/2014	Hackers gained access to names, addresses, phone numbers, email addresses, and other information belonging households and small businesses	83 Million	JPMorgan Chase	Financial	United States
Number 14 7/16/2008	Glitch during testing new design exposed users' birth dates publicly	80 Million	Facebook Inc.	Technology	United States
Number 15 2/4/2015	Hackers gained access to names, addresses, dates of birth, SSNs, medical ID numbers, email addresses and employment details of current and former customers and employees	78.8 Million	Anthem Insurance Companies	Insurance	United States
Number 16 4/26/2011	Hackers gained access to names, addresses, email addresses, birthdates, passwords and logins, profile data, purchase history and possibly credit cards	77 Million	Sony Corporation	Retail	United States
Number 17 8/26/2013	Flaw in API exposed users' email addresses	70 Million	Pinterest	Technology	United States
Number 18 11/11/2015	Hackers gained access to private phone logs between prisoners, callers and attorneys.	70 Million	Securus Technologies, Inc.	Technology	United States
Number 19 3/13/2013	IRS agents allegedly seized records during raid of covered entity	60 Million	Organization's Name has not been reported	Unknown	United States
Number 20 7/2/2013	Unauthorized access to a website database exposed user names, email addresses and encrypted passwords	58 Million	Ubisoft	Technology	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)

Name	Description
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

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