Data Breach QuickView

Mid-Year 2015 Data Breach Trends

Sponsored by:
Risk Based Security

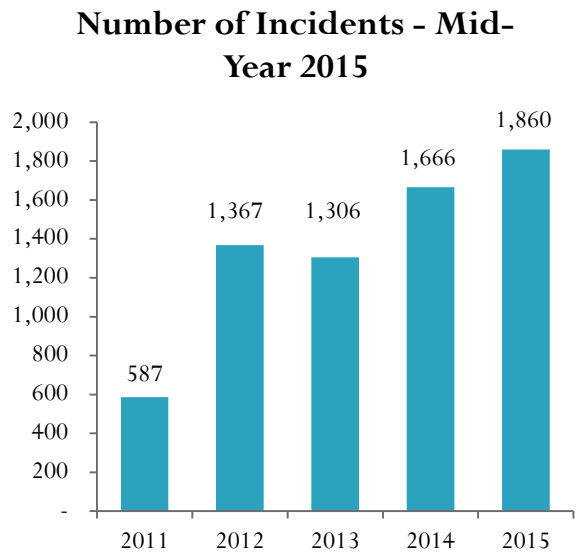
Data Breaches - the first six months …

- There were 1860 incidents reported during the first six months of 2015 exposing 228 million records.
- Five Hacking incidents alone exposed a combined 181.3 million records.
- A single act of Hacking exposed 78.8 million records.
- The Business sector accounted for 43.6% of reported incidents, followed by Unknown (19.2%), Education (19.1%), Government (12.3%), and Medical (5.8%).
- The Business sector accounted for 59.4% of the records exposed, followed by Government (34.1%), and Unknown (5.5%).
- 78.4% of reported incidents were the result of Hacking, which accounted for 95.3% of the exposed records.
- Phishing accounted for seventeen incidents and the exposure of 1.4 million records.
- Breaches involving U.S. entities accounted for 37.6% of the incidents and 55.3 of the exposed records.
- 40.4% of the incidents exposed between one and 100 records.
- Seventeen (17) incidents exposed one million or more records.
- The Anthem Insurance breach of 78.8 million records rests at #15 all time.
- The number of reported incidents tracked by Risk Based Security has exceeded 16,700 exposing nearly 3.9 billion records.

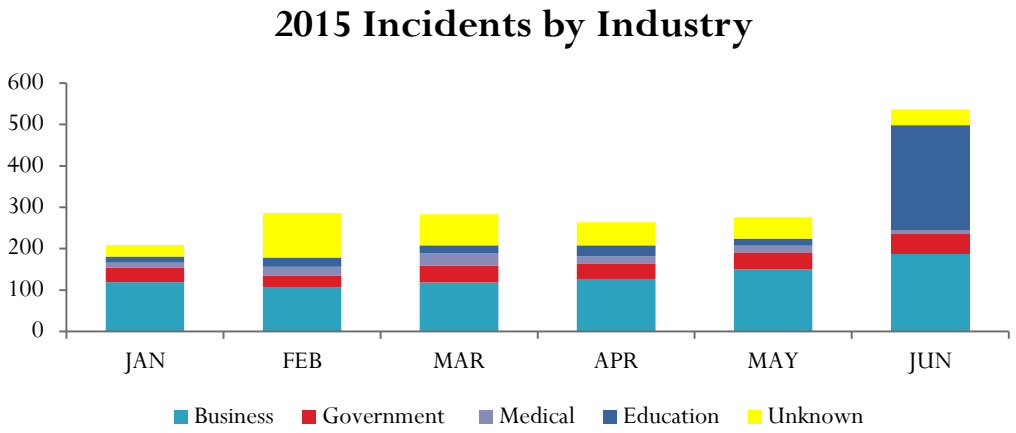
RiskBased SECURITY

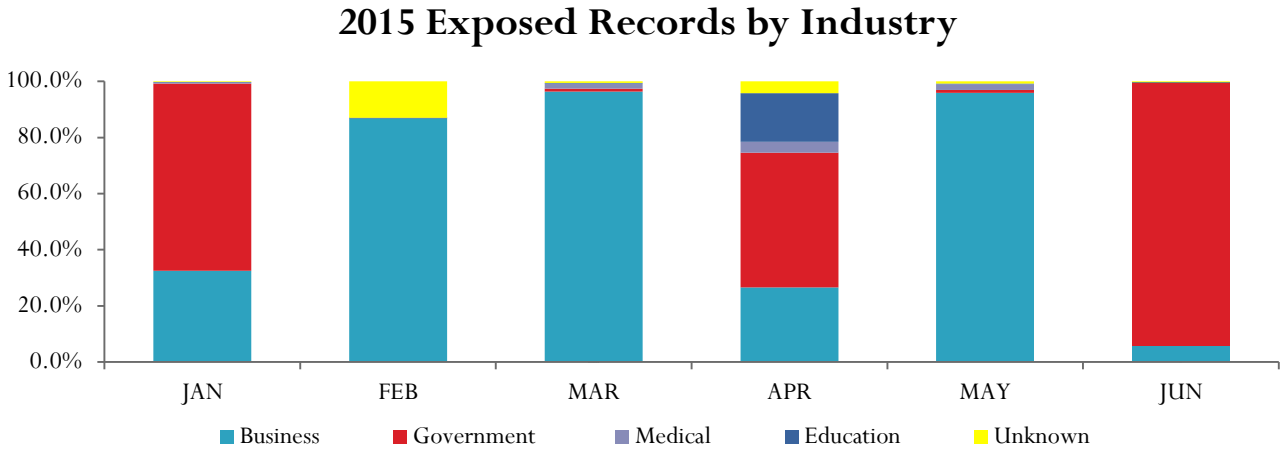
Not Just Security, the Right Security.

Mid-Year 2015 Compared to Mid-Year of the Past Four Years



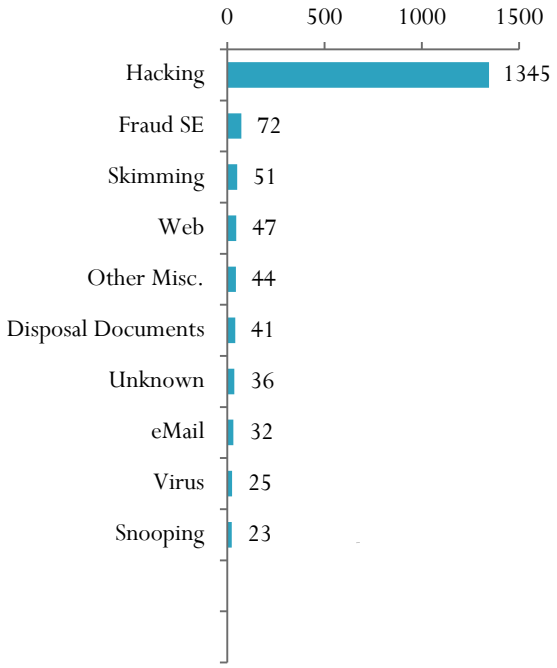
Mid-Year 2015 by Industry by Month





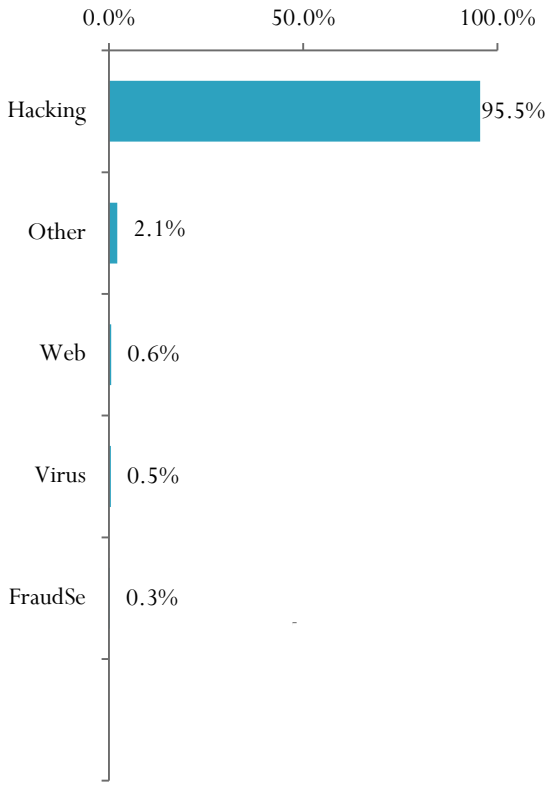
Mid-Year 2015 Analysis by Breach Type

Top 10 Mid-Year 2015 Incidents by Breach Type



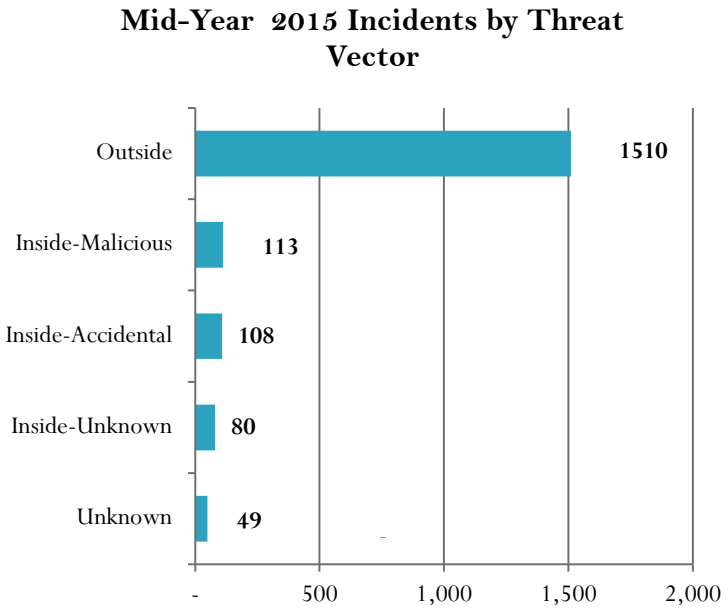
The number of breaches caused by Hacking, (78.4%), dwarfs all other breach types reported.

Mid-Year 2015 Records Exposed by Breach Type



Hacking alone resulted in 95.5% of all exposed records.

Mid-Year 2015 Analysis by Threat Vector



81.2% of incidents involved outside the organization activity.

Mid-Year 2015 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	220,463,149
Inside-Malicious	2,661,499
Inside-Accidental	3,733,436
Inside-Unknown	1,307,568
Unknown	125,668
Total	**228,291,320**

96.6% of the total exposed records are the result of Outside activity.

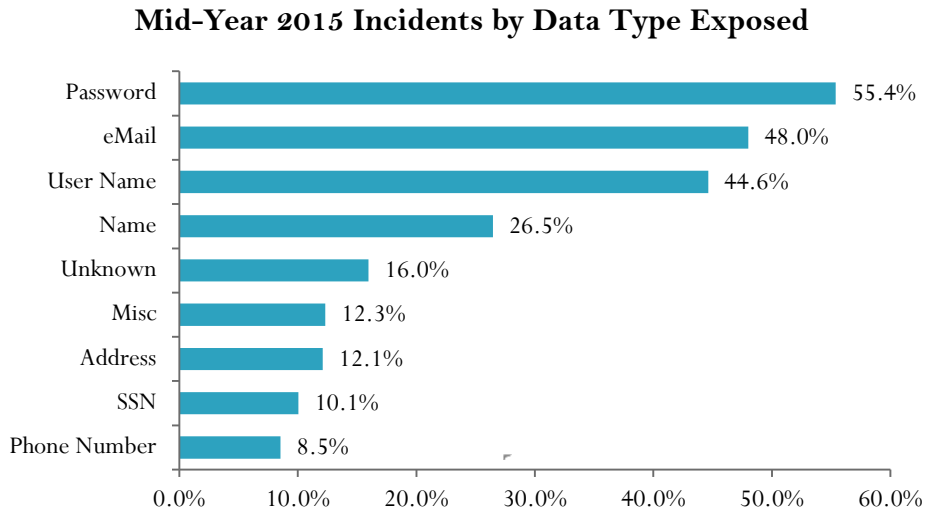
Five incidents, all Hacks, Anthem (78.8 million), Republic of Turkey (50.0 million), U.S. Office of PM, (21.5 million), Topface, (20.0 million), and Premera Blue Cross Blue Shield, (11 million) accounted for 181.3 million exposed records, (82.2%).

Mid-Year 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	**Mid-Year 2015**	**Mid-Year 2015**	**2014**	**2014**
Electronic	91.3%	99.99%	89.71%	99.90%
Physical	6.6%	<0.1%	7.7%	<0.1%
Unknown	2.1%	< 0.1%	2.59%	< 0.1%

Over 91% 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.

Mid-Year 2015 Analysis by Data Type – Percentage of Incidents



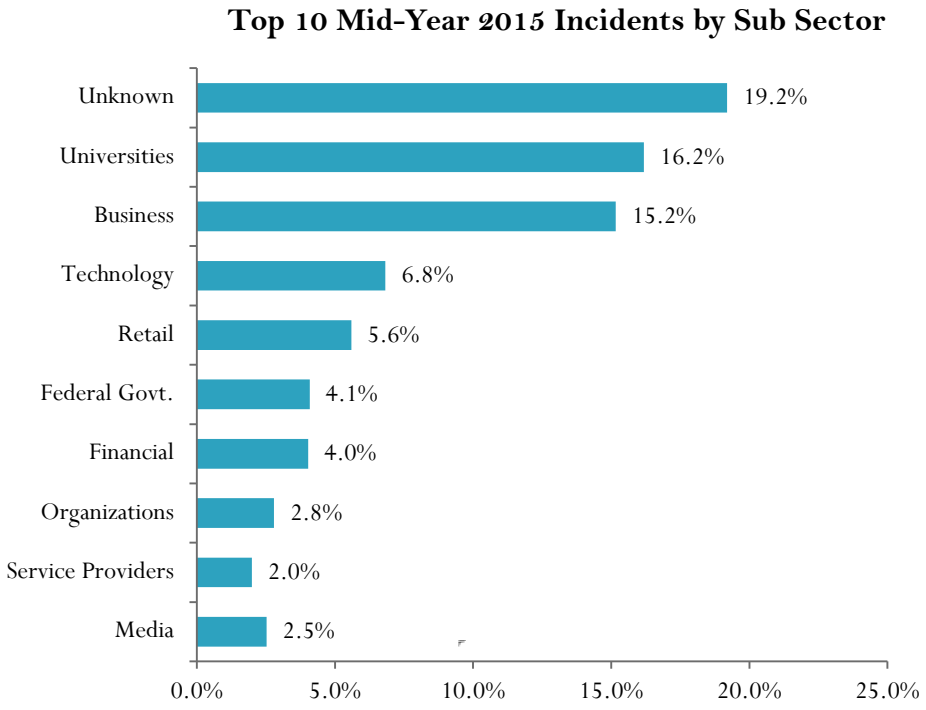
Mid-Year 2015 Percentage of Incidents Exposing Data Types vs. 2014

Data Type	Mid-Year 2015	2014
Password	55.4%	62.6%
User Name	44.6%	50.5%
eMail	48.0%	49.2%
Name	26.5%	31.9%

User names, email addresses and passwords remain a prize target.

- Percentage of incidents exposing Passwords remains relatively level
- Percentage of incidents exposing eMail addresses remains level.

Mid-Year 2015 Analysis by Industry Sub Type



- The Insurance sector accounted for 39.4% of the exposed records followed by the Federal Governments at a close 34.7%.
- Universities move into the #2 spot in number of incidents accounting for 17.0%.

Of the 301 incidents occuring at colleges and universitiies during the first six months of 2015, 112 impacted campuses located in the USA. The Average number of records exposed equaled 3,075, with a high of 364,012, reported by Auburn University as the result of inadvertently allowing access to a file on the Internet. In eighty of the 301 incidents the university was unable to determine or unwilling to share how many records were actually exposed during the breach. Of the incidents including the number of exposed records, the median number of exposed records equaled sixteen, (16). The most frequent data types exposed in university breaches were Passwords (62.5%), User Names (57.1%), and eMail Addresses (45.8%). With research revealing that any where from 30% to as high as 50% of users reuse their passwords from site to site and even for their business accounts, it's obvious why attacked see user names and passwords as prize targets.

Mid-Year 2015 Analysis of Records per Incident

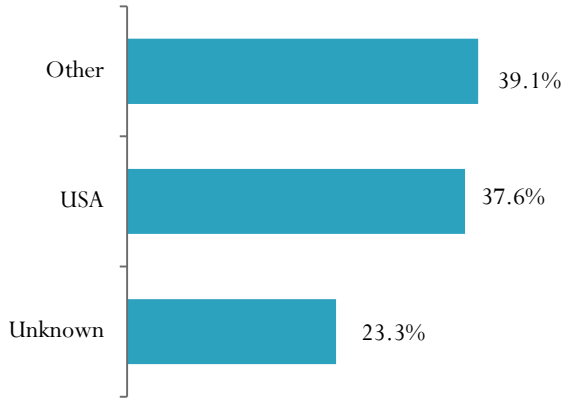
Exposed Records	Number of Incidents	Percent of Total
Unknown	476	25.6%
1 to 100	752	40.4%
101 to 1,000	347	18.7%
1,001 to 10,000	196	10.5%
10,001 to 100,000	49	2.6%
100,001 to 500,000	18	1.0%
500,001 to 1 Million	5	0.3%
1 M to 10 M	12	0.6%
> 10 M	5	0.3%

The number of incidents with exposed records reported as "Unknown" is 25.5% for Mid-Year 2015 – an increase over 2014's 19.2%.

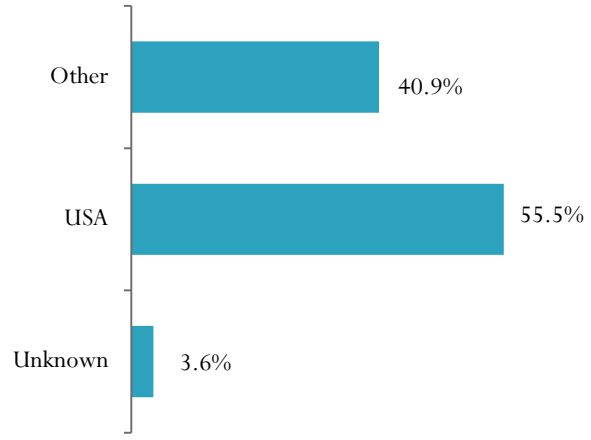
- 59.1% of incidents exposed between 1 and 1000 records

Mid-Year 2015 Analysis by Country (78 countries reporting at least one breach)

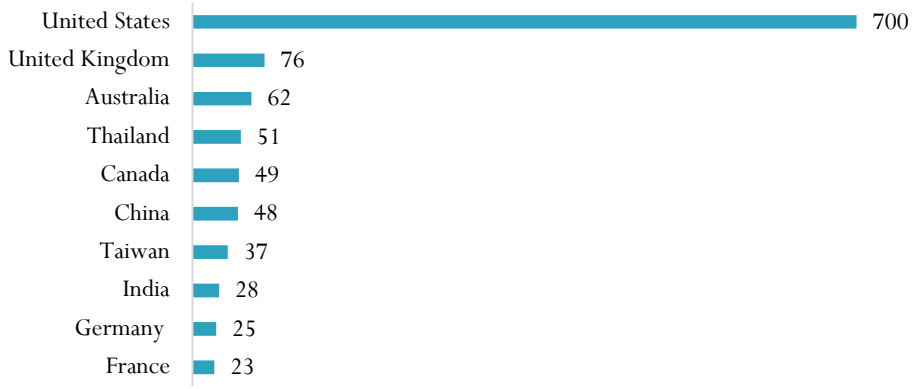
Mid-Year 2015 Incidents by Location



Mid-Year 2015 Records by Location



Mid-Year 2015 Incidents by Country - Top 10

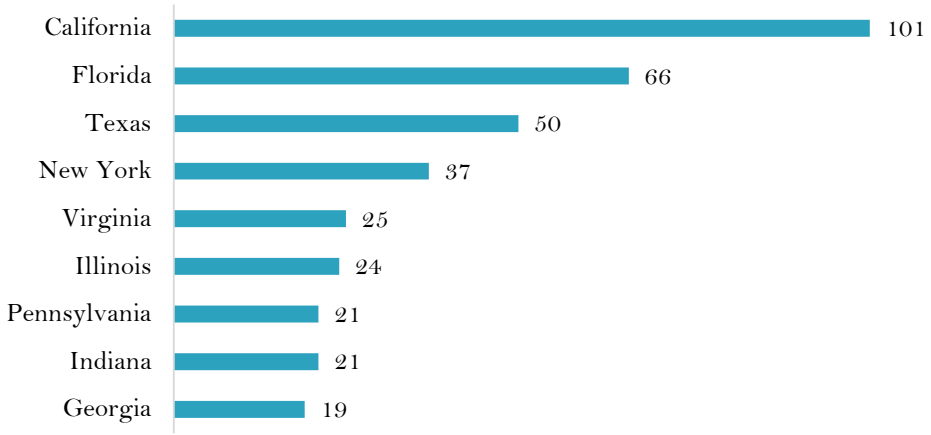


Mid-Year 2015 Exposed Records by Country – Top 10

Exposed Records Ranking	Country	Total Exposed Records	Average Records per Breach	Percentage of Exposed Records
1	United States	126,613,673	180,876	55.46%
2	Republic of Turkey	50,000,000	50,000,000	20.66%
3	Russian Federation	20,000,689	3,333,448	8.26%
4	Pakistan	10,050,223	358,937	4.15%
5	United Kingdom	7,224,633	656,785	2.99%
6	China	2,013,064	26,488	0.83%
7	Japan	1,273,661	19,335	0.53%
8	India	1,001,476	100,148	0.41%
9	Australia	928,075	3,163	0.38%
10	France	196,083	55,377	0.08%

Mid-Year 2015 Analysis of US State Rankings

Mid-Year 2015 Incidents by US State- Top 10



Top 10 represent 52.0% of US incidents.

Exposed Records Ranking	US State	Total Exposed Records	Percentage of USA Exposed Records
1	IN	79,285,819	62.6%
2	DC	21,703,713	17.1%
3	AK	11,000,015	8.7%
4	CA	5,189,624	4.1%
5	WA	1,502,249	1.2%
6	MD	1,127,578	0.9%
7	NY	473,328	0.4%
8	CO	392,127	0.3%
9	AL	364,025	0.3%
10	MN	263,040	0.2%

Top three states represent 88.4% of exposed US records.

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