Data Breach QuickView

First Nine Months of 2016 Data Breach Trends

Sponsored by:
Risk Based Security

Issued in October 2016

2016 after the first three quarters …

- There were 2,991 breaches reported during the first nine months of 2016 exposing over 2.2 billion records.
- Top 10 breaches (8 Hacks[1] and 2 Web) exposed a combined 1.6 billion records.
- Top 10 Severity scores averaged 9.87 out of 10.0.
- The Business sector accounted for 49.26% of reported breaches, followed by Unknown (24.1%), Government (12.2%), Medical (9.8%), and Education (4.7%).
- The Business sector accounted for 75.9% of the number of records exposed, followed by Unknown (15.1%), Government (8.3%), Medical (.6%), and Education < .1%.
- 52.6% of reported breaches were the result of Hacking, which accounted for 89.2% of the exposed records.
- Web accounted for 7.8% of the exposed records, but represented just 3.4% of the reported breaches.
- Breaches involving U.S. entities accounted for 49.8% of the breaches and 59.4% of the exposed records.
- 39.8% of the breaches exposed at between one and 1000 records.
- 198 breaches involved Third Parties
- Sixty-eight (68) breaches so far in 2016 exposed one million or more records.
- Three 2016 breaches have taken their place on the Top 10 List All Time at Number One, Number Two and Number Six.
- Nine breaches have involved Technology companies exposing more than 802 million records.
- The number of reported breaches tracked by Risk Based Security has exceeded 22,000, exposing over 7.4 billion records.

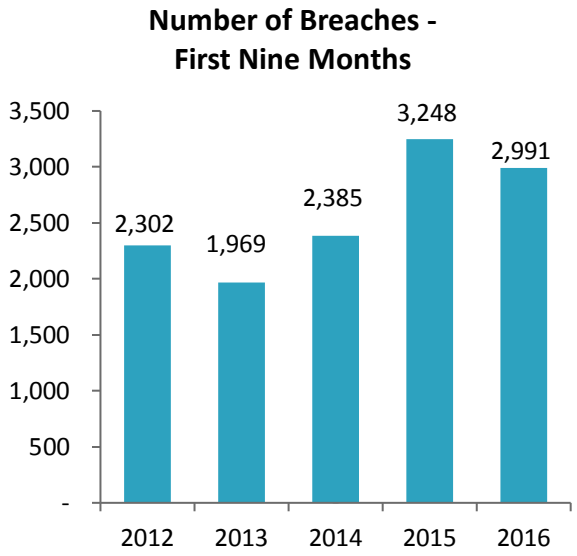
RiskBased SECURITY

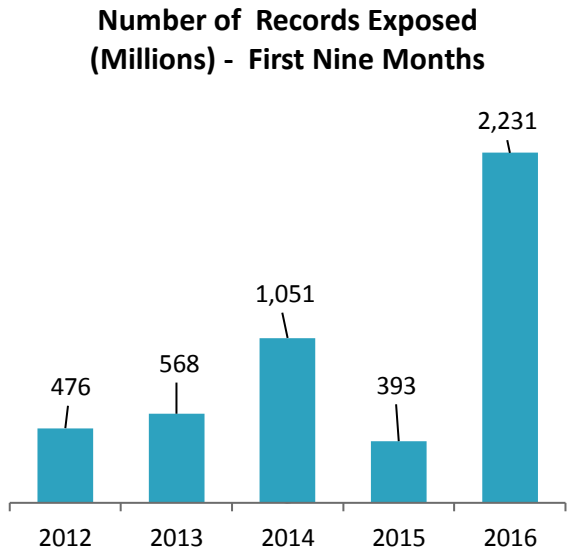
Not Just Security, the Right Security.

[1] See page 16 for definitions

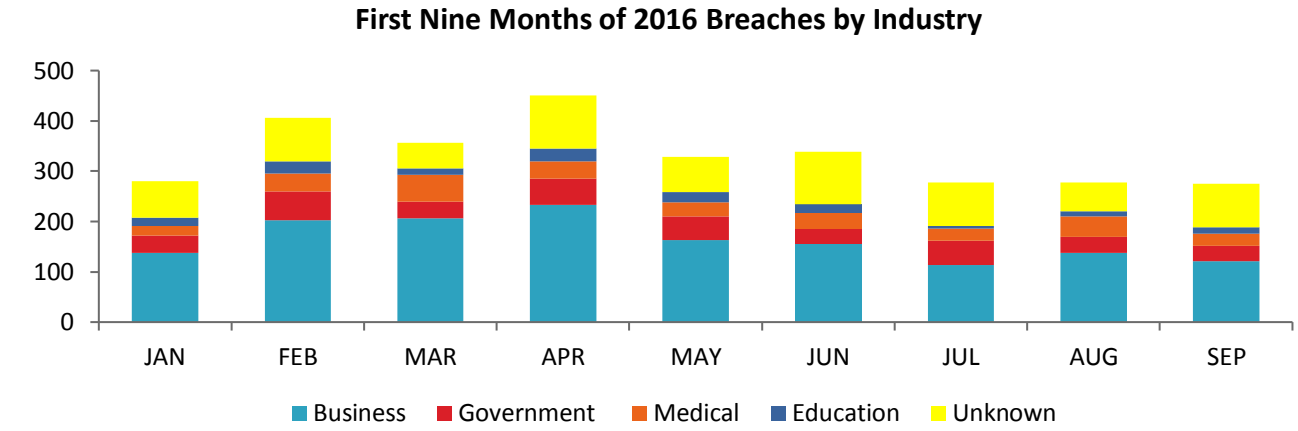
Table of Contents

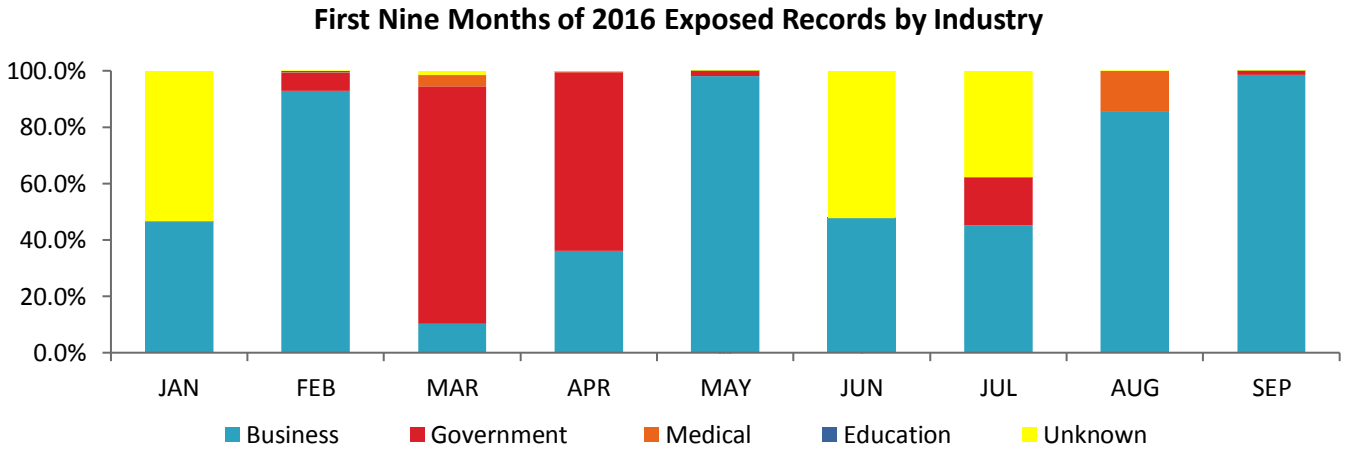
First Nine Months of 2016 Compared to the Past Four Years





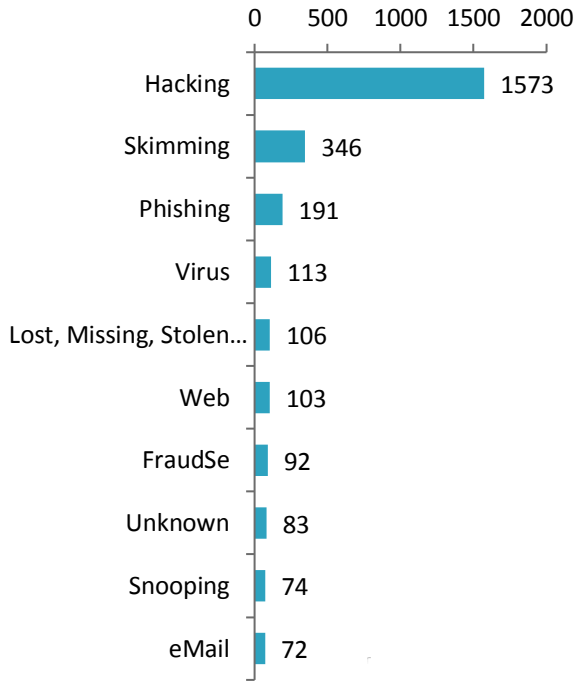
First Nine Months of 2016 by Industry by Month





First Nine Months of 2016 Analysis by Breach Type

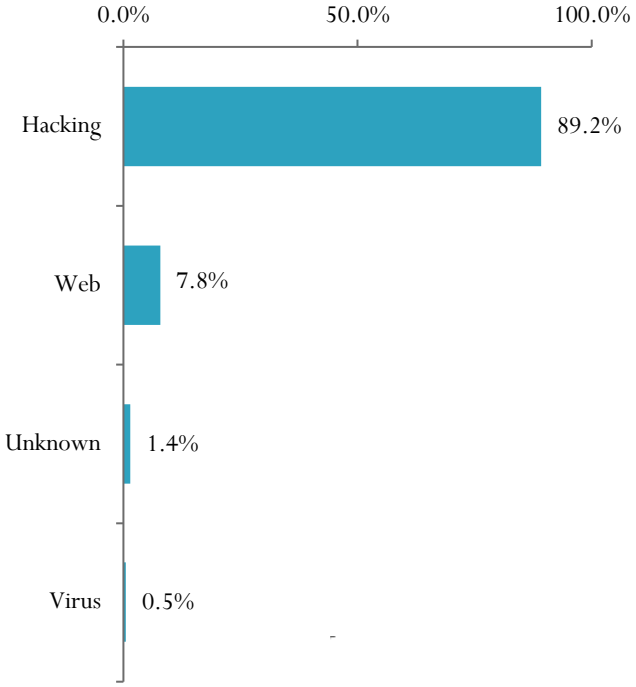
First Nine Months of 2016 Breach Types - Top 10 Breach Types



Hacking continues to dominate as the leading breach type.

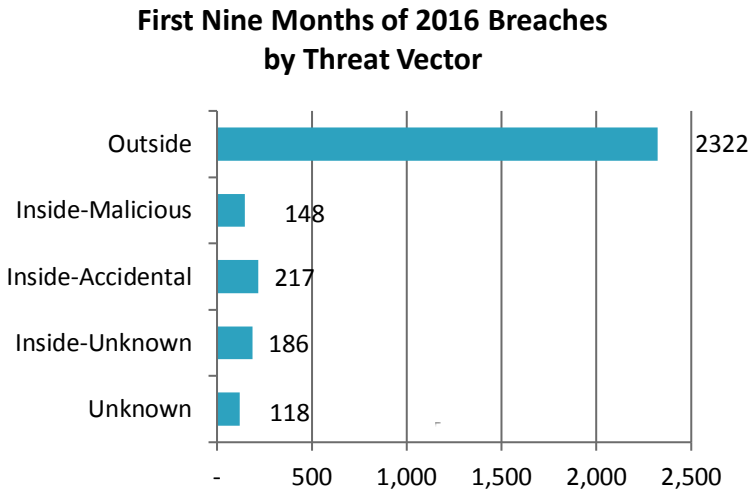
Skimming & Phishing take spots #2 and #3.

First Nine Months of 2016 Records Exposed by Breach Type



Hacking and Web resulted in 97.0% of all exposed records.

First Nine Months of 2016 Data Breach Analysis by Threat Vector



77.6% of breaches involved activity from Outside the organization

First Nine Months of 2016 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	1,889,300,033
Inside-Accidental	76,694,876
Inside-Malicious	2,077,750
Inside-Unknown	31,697,874
Unknown	231,852,291
Total	**2,231,622,824**

84.6% of the total exposed records are the result of Outside activity.

Top 10 Breaches – Data Types and Severity Scores

Breach Type	Records Exposed	Percentage of Total Exposed	Data Types[2]	Severity Score
Hack	500,000,000	22.41%	DOB/EMA/MISC/NAA/NUM/PWD	10.0
Hack	360,213,024	16.14%	EMA/PWD/USR	10.0
Hack	154,000,000	6.9%	ADD/EMA/MISC/NAA/NUM	10.0
Hack	127,343,437	5.71%	DOB/EMA/NAA/PWD/USR	9.7
Hack	98,167,935	4.4%	EMA/MISC/PWD/USR	9.6
Web	93,424,710	4.19%	ADD/DOB/MISC/NAA	9.8
Hack	93,338,602	4.18%	EMA/NAA/NUM/PW	10.0
Hack	70,000,000	3.14%	DOB/EMA/MISC/USR	9.7
Hack	65,469,298	2.93%	EMA/PWD	9.4
Web	56,000,000	2.51%	ADD/MISC/NAA/NUM	8.5
		72.5%		

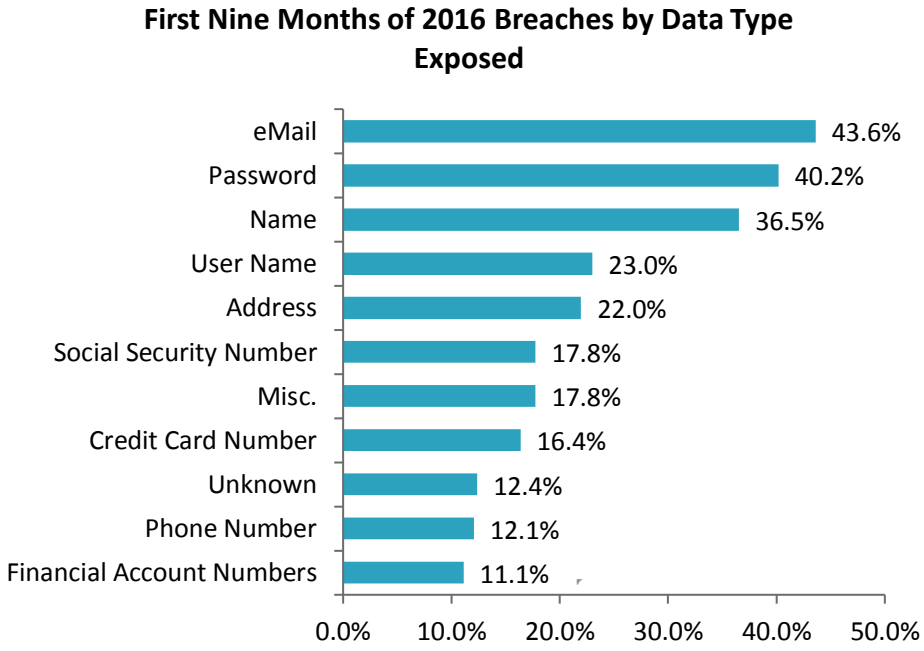
[2] See page 17 for definition

First Nine Months of 2016 Analysis by Data Family

Data Family	Percentage of Total Breaches 2015	Percentage of Total Exposed Records 2015	Percentage of Total Breaches First Nine Months of 2016	Percentage of Total Exposed Records First Nine Months of 2016
Electronic	89.9%	99.7%	90.5%	99.9%
Physical	7.0%	<0.15%	6.5%	<0.1%
Unknown	3.1%	< 0.15%	3.0%	< 0.1%

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

First Nine Months of 2016 Analysis by Data Type – Percentage of Breaches



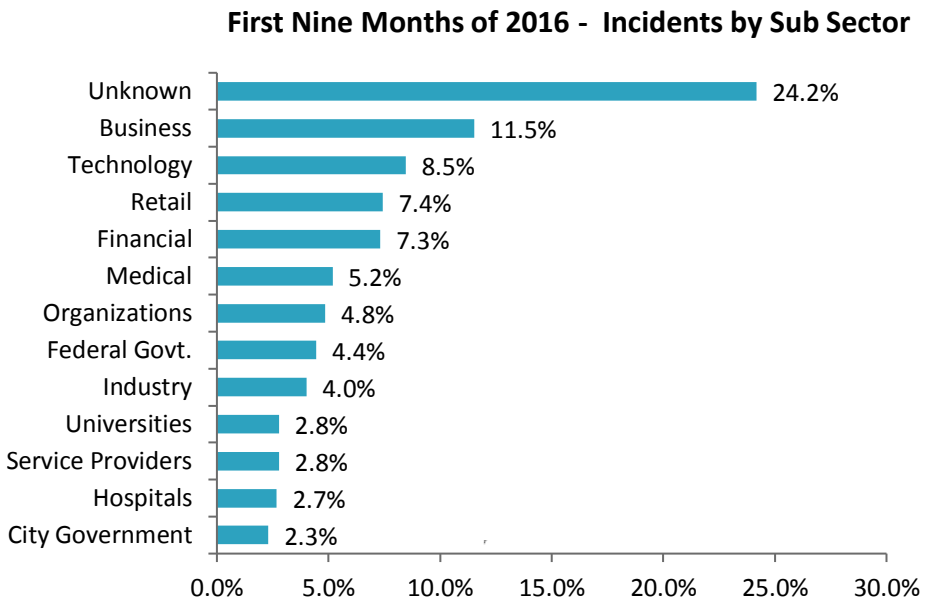
43.6% of data breaches exposed eMail Addresses. Passwords and eMail Addresses remain a prize target.

2016 Percentage of Breaches Exposing Data Types vs. 2015

Data Type	2015	First Nine Months of 2016
Password	49.9%	40.2%
eMail	45.5%	43.6%
User Name	37.7%	23.0%
Name	29.4%	36.5%

Over 40% of all breaches expose Passwords and eMail Addresses.

First Nine Months of 2016 Analysis by Industry Sub Business Type



- Unknown[3] and Business sub types remain in the top two spots with Technology coming in at number three in number of breaches.
- Unknown sub-sector accounted for 24.2% of the exposed records followed by Business at 11.5%, Technology at 8.5%, Retail at 7.4% and Financials at 7.3%.

2016 Analysis of Records per Breach

Exposed Records	Number of Breaches	Percent of Total
Unknown	1088	36.4%
1 to 100	599	20.0%
101 to 1,000	590	19.7%
1,001 to 10,000	423	14.1%
10,001 to 100,000	146	4.9%
100,001 to 500,000	57	1.9%
500,001 to 999,999	20	0.7%
1 M to 10 M	44	1.5%
> 10 M	24	0.8%

The number of breaches with exposed records reported as "Unknown" is 36.4% for the first nine months of 2016 – up from 2015's 27.6%.

- 39.7% of breaches exposed at least 1 and not more than 1,000 records.

[3] In certain situations, the party responsible for the breach cannot be identified with certainty. When this happens, the marker "Unknown Organization" is used and the associated business type and sub-type are also "Unknown".

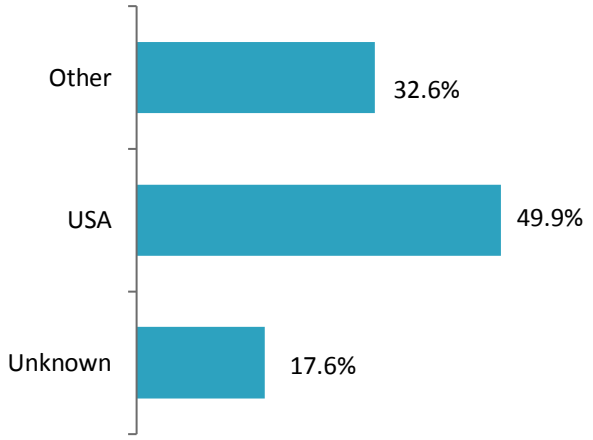
First Nine Months of 2016 - Breach Types/Records Exposed – Top 5

Breach Category	Number of Breaches	Number of Records Exposed	Average Records per Breach	Percent of Total Records Exposed
Hacking	1573	1,989,692,299	1,264,905	89.16%
Web	103	175,045,445	1,699,470	7.84%
Unknown	83	32,212,693	388,105	1.44%
Virus	113	12,124,798	107,299	.54%
All Other Types	1119	22,547,589	38,101	1.01%

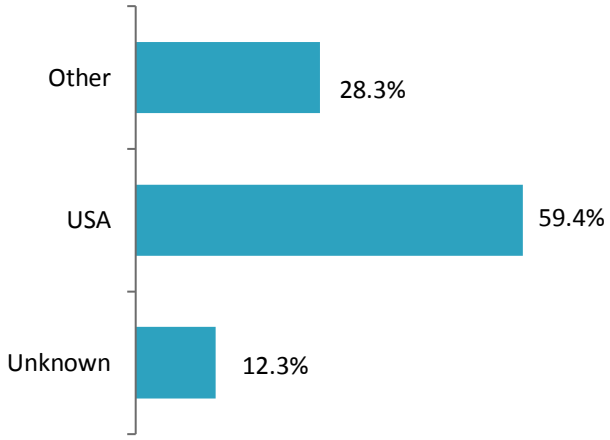
- Web is #1 in records per breach.
- Hacking accounted for the 2nd highest records per breach.
- Unknown breach type was #3 in records per breach.

First Nine Months of 2016 Analysis by Country

First Nine Months of 2016 Breaches by Location

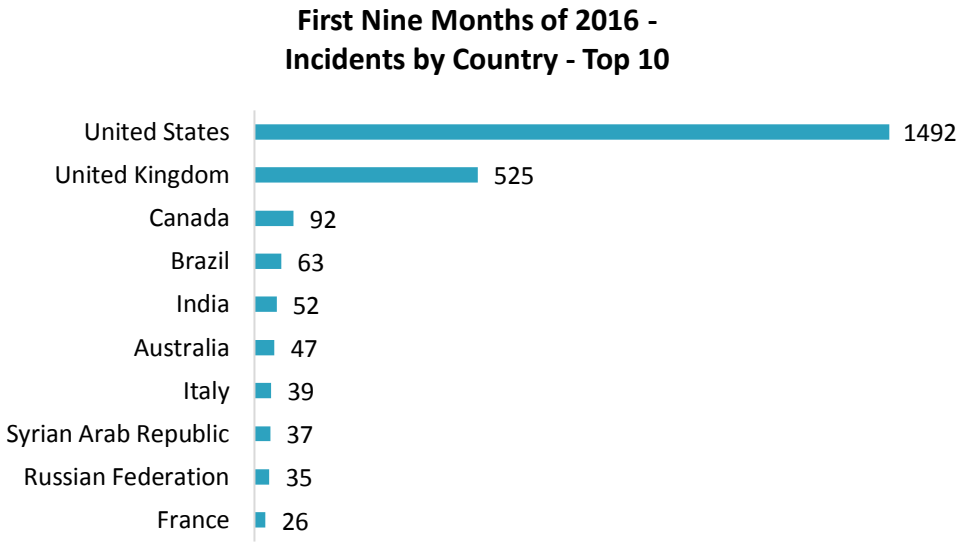


First Nine Months of 2016 Exposed Records by Location



- There were 90 countries reporting at least one data breach in the first nine months of 2016.
- The Top 10 countries accounted for 68.2% of the breaches.
- There were 65 countries with multiple data breaches in 2016.

First Nine Months of 2016 Analysis by Country – Top 10



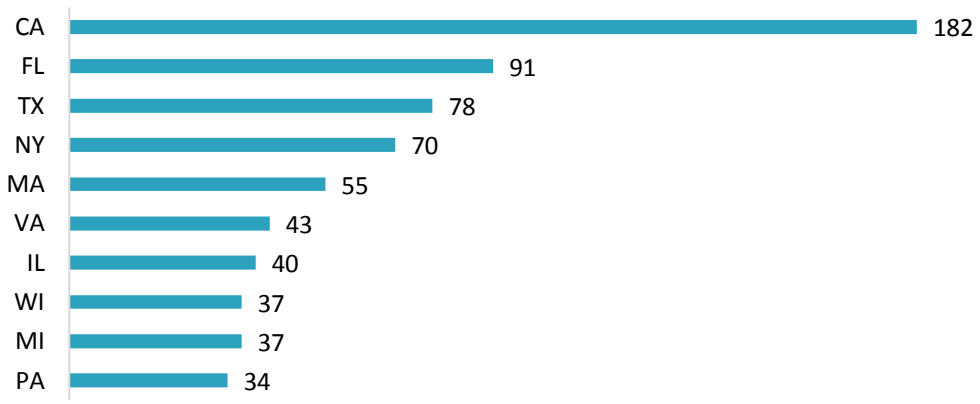
USA and UK account for 67.4% of breaches.

First Nine Months of 2016 Exposed Records by Country – Top 10

Exposed Records Ranking	Number of Breaches	Country	Total Exposed Records	Average Records per Breach	Percentage of Exposed Records
1	1492	United States	1,326,121,611	888,821	59.42%
2	35	Russian Federation	259,452,232	7,412,921	11.63%
3	7	Mexico	93,427,454	13,346,779	4.19%
4	92	Canada	73,071,047	794,251	3.27%
5	8	Philippines	55,003,294	6,875,412	2.46%
6	9	Iran	35,333,154	3,925,906	1.58%
7	3	Taiwan	30,000,051	10,000,017	1.34%
8	11	China	22,603,609	2,054,874	1.01%
9	5	South Korea	10,347,071	2,069,414	0.46%
10	52	India	10,031,275	192,909	0.45%

First Quarter 2016 Analysis of US State Rankings

First Nine Months of 2016 Breaches by US State - Top 10



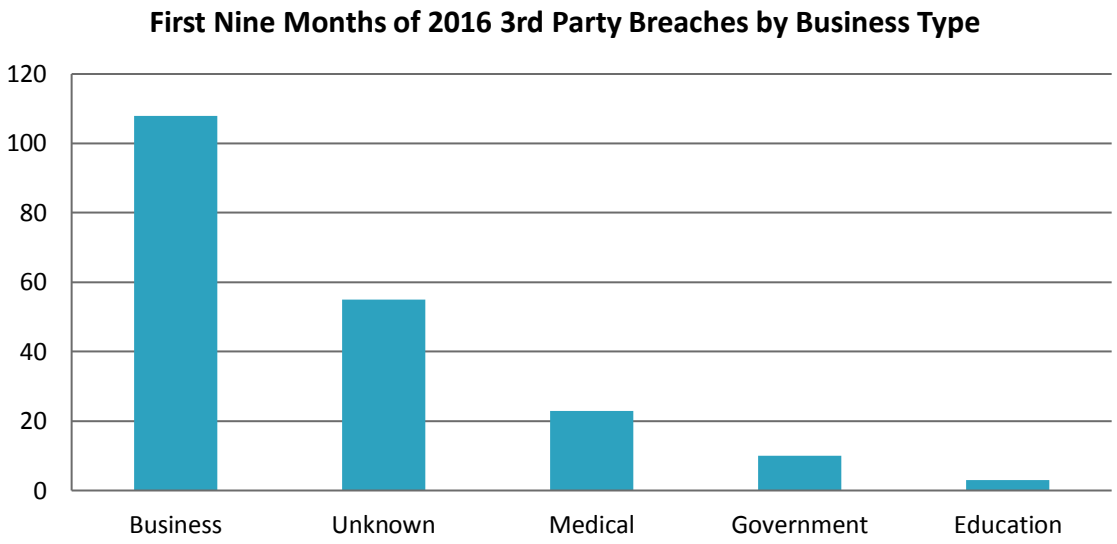
Top 10 represent 52.2% of US breaches with known State.

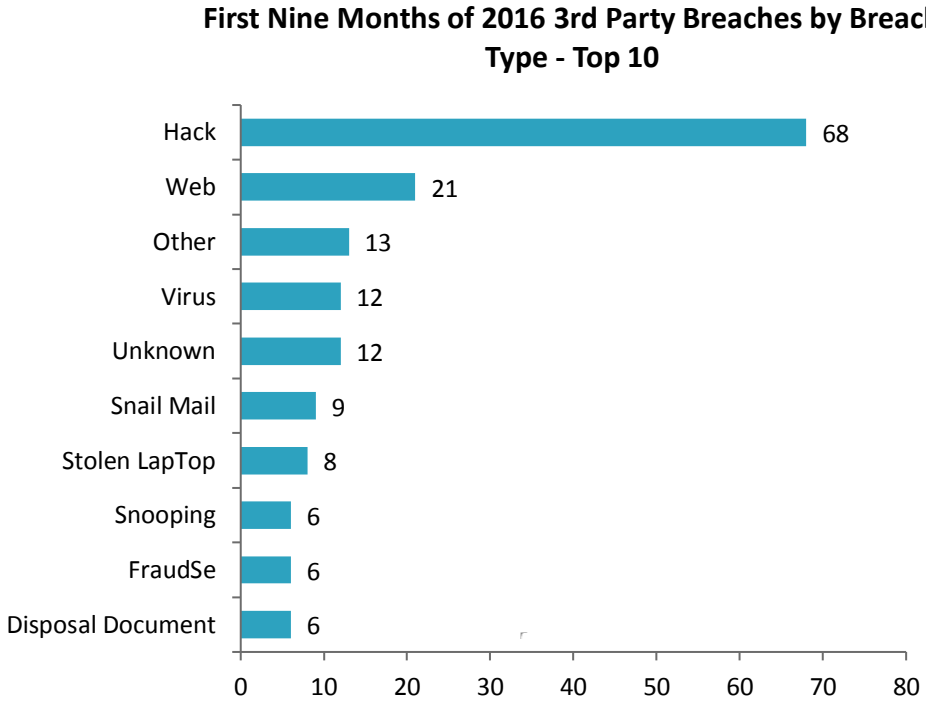
- California stays at number one with Florida taking over the number two spot.

Exposed Records Ranking	US State	Total Exposed Records	Number of Breaches	Exposed Records/Breach	Percentage of USA Exposed Records
1	CA	870,236,860	182	4,781,521	65.62%
2	NY	120,794,837	70	1,725,641	9.11%
3	VA	49,946,515	43	1,161,547	3.77%
4	LA	10,252,379	9	1,139,153	0.77%
5	NC	7,768,927	28	277,462	0.59%
6	WA	6,039,877	30	201,329	0.46%
7	AZ	5,535,534	30	184,518	0.42%
8	OH	4,377,916	34	128,762	0.33%
9	FL	2,633,649	91	28,941	0.20%
10	TX	2,244,367	78	28,774	0.17%

- California's 182 breaches top records per breach calculation.
- Top Ten states represent 81.4% of records exposed in the USA.

First Nine Months of 2016 Breaches Involving Third Parties





First Nine Months of 2016 Repeat Offenders

Eighty-Eight (88) organizations have reported multiple data breaches in the First Nine Months of 2016

The first nine months of 2016 saw 88 organizations reporting multiple breaches. There were 316 breaches in all, with 173 from Skimming, and 52 from Hacking. The Retail sector reported 78 breaches and the Finance sector reported 66 breaches, with 92.4% from Skimming. It remains hard to tell the true impact to organizations or consumers since 224, or 70.5% of the repeat offenders reported 'Unknown' as to the number of records exposed.

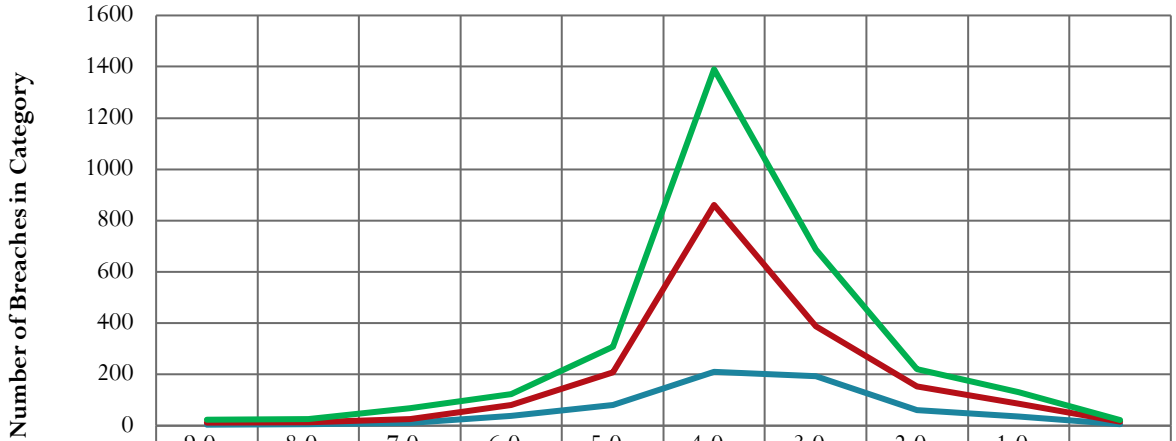
First Nine Months of 2016 – On the Rise

We saw an average of twenty-six (26) Skimming breaches per month in 2015. The first nine months of 2016 reported 346 Skimming breaches (38/month). Financial institutions, gas stations and convenience stores with gas pumps have been the hardest hit.

First Nine Months of 2016 – Breach Severity Scoring

We can all readily agree that all data breaches are not created equal. Where disagreement arises is when we attempt to rate the 'severity' or 'cost' of a breach. At Risk Based Security we have combined our knowledge of the security industry, business experience and our comprehensive data breach information to calculate a Data Breach Severity Score. Taking into account information such as, the total number of records exposed, the type of data exposed, the breached organization's industry, the threat vector responsible for the breach, the type of breach triggering the exposure/lost, the number of third parties associated with the breach, any law suit filings, the type of company (public vs. private) and the intent of the breach agent, (malicious vs. accidental), our Severity Scores range from .1 to 10.0.

First Nine Months of 2016 – Breach Severity Scores



	9.0 - 10.0	8.0 - 8.99	7.0 - 7.99	6.0 - 6.99	5.0 - 5.99	4.0 - 4.99	3.0 - 3.99	2.0 - 2.99	1.0 - 1.99	< 1
1Q2016	4	6	12	39	81	210	192	62	37	5
2Q2016	12	13	25	82	208	861	389	154	86	16
3Q2016	23	25	69	123	309	1390	688	220	131	22

First Nine Months of 2016 – Breach Severity Scores – Top 10

Organization	Top 10 Summary	Score
Yahoo	(Hacking) 500,000,000 user names, email addresses, phone numbers, dates of birth, hashed passwords and some security questions and associated answers compromised.	10
MySpace	(Hacking) 360,213,024 user account records containing SHA1 encrypted passwords, email addresses, 111,341,258 usernames, and 68,493,651 secondary passwords stolen and made available for sale on the Internet	10
Unknown Organization	(Hacking) 154,000,000 names, addresses, phone numbers, political affiliations, income ranges, ethnicities, ages, and voting histories, as well as an unknown number of email addresses, social media profiles, and political poll results of United States voters discovered on an unsecured Google server after being stolen.	10
Unknown Organization	(Hacking) 93,338,602 user accounts with names, email addresses, phone numbers and clear text passwords stolen in 2012 and offered for sale on the Internet	10
VerticalScope Inc.	(Hacking) Nearly 45,000,000 email addresses, usernames, IP addresses, and weakly encrypted passwords for accounts on over 1,100 websites and communities stolen.	9.95
Movimiento Ciudadano	(Web) 93,424,710 voter names, addresses, dates of birth, occupations, and unique voting credential codes discovered on an unsecured Amazon cloud server	9.83
Mail.RU Group	(Hacking) Over 25,000,000 email addresses, dates of birth, usernames, and weakly hashed passwords, as well as an undisclosed number of IP addresses and phone numbers, stolen from three separate Mail.ru forums.	9.78
JumpStart Games, Inc.	(Hacking) 70,000,000 usernames, email addresses, genders, countries and states, and dates of birth taken sometime prior to 2014 and sold online.	9.75
Republic of the Philippines Commission on Elections	(Hacking) 55,000,000 voter registration details, including 1,300,000 passport numbers with expiry dates, 15,800,000 fingerprints, and the database schema, leaked on the Internet.	9.74
Badoo Trading Limited dba Badoo.com	(Hacking) 127,343,437 user email addresses, usernames, MD5 hashed passwords with no salts, names, and dates of birth stolen and sold on the Internet.	9.71

Top 20 Breaches All Time (Exposed Records Count)

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Highest All Time 9/22/2016	Hack exposes user names, email addresses, phone numbers, dates of birth, hashed passwords and security questions and associated answers.	500 Million	Yahoo	Business - Technology	United States
Number 2 5/27/2016	Hack exposes user account records containing SHA1 encrypted passwords, email addresses.	360 Million	MySpace	Business	United States
Number 3 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 4 10/19/2013	Fraudulent account created gaining access to credit card numbers, social security numbers, names, and financial account numbers.	200 Million	Court Ventures, Inc.	Business - Data	United States
Number 5 12/28/2015	Mis-configured database exposes voter names, dates of birth, addresses, phone numbers, political party affiliations, and genders.	191 Million	Organization's Name has not been reported	Unknown	United States
Number 6 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 7 6/23/2016	Hack exposes USA voter information.	154 Million	Organization's Name has not been reported	Unknown	United States
Number 8 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 9 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 10 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

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Number 11 6/8/2013	North Korean Hackers expose email addresses and identification numbers	140 Million	Organization's Name has not been reported	Unknown	South Korea
Number 12 1/20/2009	Hack/Malicious Software exposes credit cards at processor	130 Million	Heartland Payment Systems	Business - Finance	United States
Number 13 6/2/2016	Hack exposes user names, email addresses, hashed passwords, names, dates of birth and sold on Internet.	127 Million	Badoo Trading Limited	Business	United Kingdom
Number 14 6/2/2016	Hack exposes email addresses and password hashes and offered or sale on the Internet.	117 Million	LinkedIn Corporation	Business - Technology	United States
Number 15 12/18/2013	Hack exposed customer PII, 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 16 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 17 1/20/2014	Fraud exposes credit card numbers, social security numbers, and phone numbers.	104 Million	Korea Credit Bureau	Business - Financial	South Korea
Number 18 9/6/2016	Hack exposes email addresses, user names and passwords.	98 Million	Rambler	Business - Media	Russian Federation
Number 19 1/17/2007	Hack exposes credit card numbers and transaction details	94 Million	TJX Companies Inc.	Retail	United States
Number 20 4/22/2016	Unsecured cloud server exposes addresses, dates of birth, names, occupations and voting credentials.	93 Million	Movimiento Ciudadano	Government - Organization	Mexico

Methodology & Terms

Risk Based Security's proprietary application crawls the Internet 24x7 to capture and aggregate data breach breaches 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

Data Type Definitions

Abbreviation	Description
CCN	Credit Card Numbers
SSN	Social Security Numbers (or Non-US Equivalent)
NAA	Names
EMA	Email Addresses
MISC	Miscellaneous
MED	Medical
ACC	Account Information
DOB	Date of Birth
FIN	Financial Information
UNK	Unknown
PWD	Passwords
ADD	Addresses
USR	User Name
NUM	Phone Number
IP	Intellectual Property

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