Data Breach QuickView Report

Data Breach Trends - First Six Months of 2017

Sponsored by:
Risk Based Security

Issued in July 2017

Mega breaches continue while pace of disclosure shows signs of slowing

- There were 2,227 breaches reported in the first half of 2017, exposing over **6 billion** records.
- Top 10 breaches exposed 5.6 billion of the 6 billion records compromised.
- Top 10 Severity scores averaged 9.82 out of 10.0.
- The Business sector accounted for 56.5% of reported breaches, followed by Unknown (17%), Government (9.1%), Medical (9%), and Education (8.4%).
- The Business sector accounted for 93% of the total records exposed, followed by Government and Unknown (approximately 3% for each). Medical and Education sectors combined accounted for less than 1% of the total records exposed year to date.
- Web (inadvertent online disclosure) continues to be the leading cause of records compromised in 2017, accounting for 68.3% of records exposed, but only 7.1% of incidents reported so far this year.
- 41.6% of reported breaches were the result of Hacking, yet accounted for 30.6% of the exposed records.
- Breaches involving U.S. entities accounted for 61% of the breaches and approximately 30% of the exposed records.
- 29.3% of the breaches exposed between one and 1,000 records, 43.6% of breaches exposed between one and 10,000 records – virtually unchanged from Q12017.
- 121 breaches, or 5.4%, affected Third Parties.
- Fifty (50) breaches - 19 in Q2 and 31 in Q1 - exposed one million or more records.
- Four 2017 breaches are now on the Top 10 List of All Time Largest Breaches.
- The company DU Called, replaced River City Media for the top spot of the single largest breach disclosed, impacting 2 billion records.

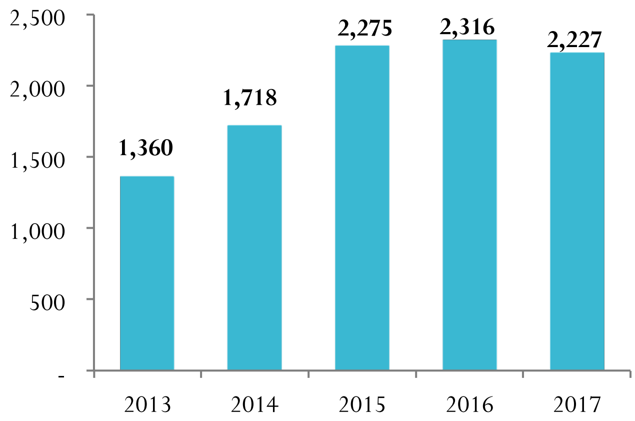
RiskBased SECURITY

Not Just Security, the Right Security.

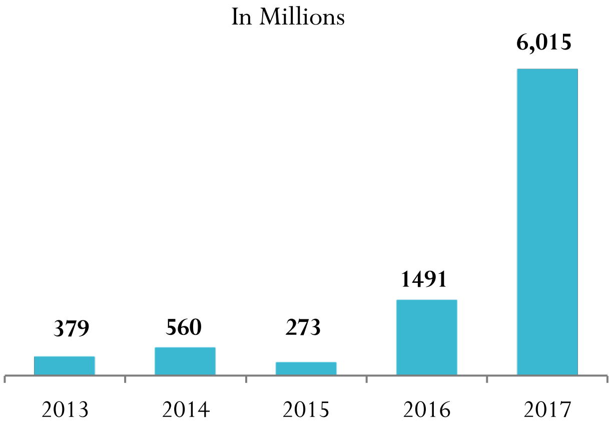
Table of Contents

Mid-Year 2017 Compared to Mid-Year of the Previous Four Years

Number of Incidents by Year - First 6 Months

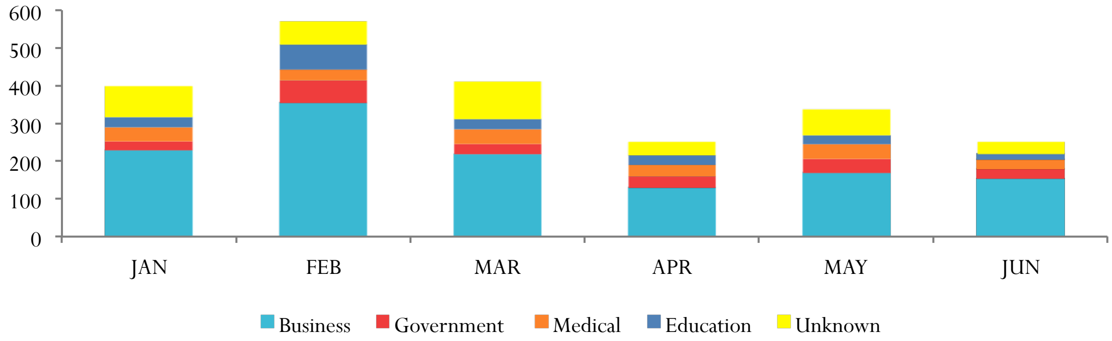


Number of Records Exposed by Year - First 6 Months

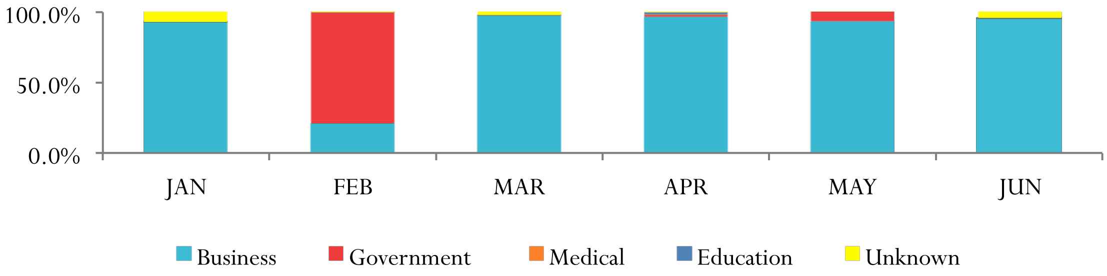


Mid-Year 2017 by Industry, by Month

Distribution of Incidents by Industry, by Month

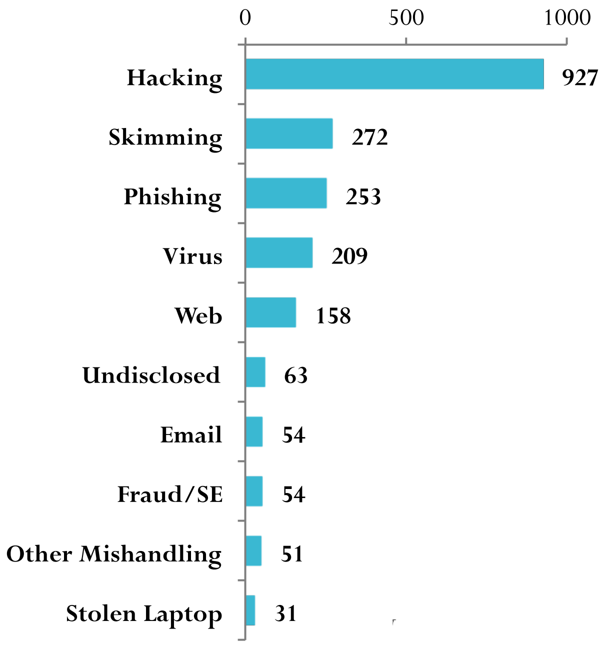


Distribution of Exposed Records by Industry, by Month



Mid-Year 2017 Analysis by Breach Type

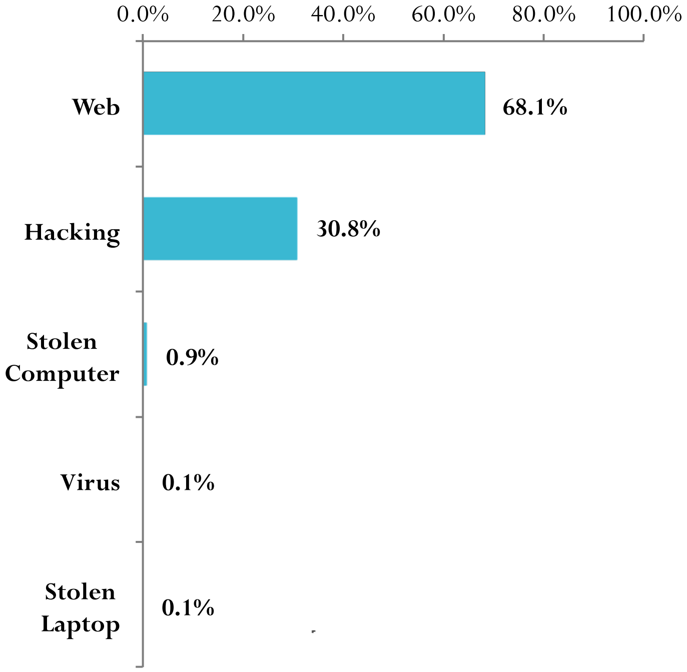
Top 10 Breach Types - First 6 Months



The number of phishing incidents started to decline once the U.S. tax season came to a close.

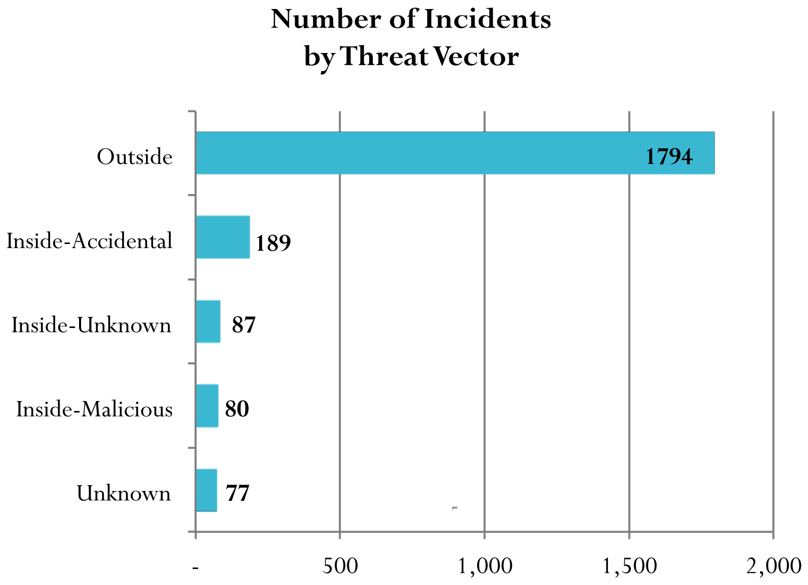
Despite being the leading cause of records exposed, Web (inadvertent online disclosure) ranked fifth on number of incidents.

Top 5 Breach Types by Records Exposed
First 6 Months



While not making the top 5 list very often, a Stolen Computer from the COMELEC (Philippines Election Commission) offices resulted in 55.1 million voter records exposed.

Mid-Year 2017 Data Breach Analysis by Threat Vector



16.0% of incidents were the result of insider activity, up slightly from 12.1% of incidents reported in Q12017.

Mid-Year 2017 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	2,227,842,612
Inside-Unknown	2,001,248,057
Inside-Accidental	1,739,943,232
Unknown	45,540,090
Inside-Malicious	567,571
Total	**6,015,141,562**

A single insider incident exposed Two billion records.

Mid-Year 2017 – Breach Discovery Method

	Internal Discovery - Incidents	Internal Discovery - Records	External Discovery - Incidents	External Discovery - Records	Undisclosed Discovery - Incidents	Undisclosed Discovery - Records
Q1	221	65,173,264	783	3,345,957,501	376	17,670,845
Q2	222	2,966,956	314	486,285,236	311	2,097,077,760
YTD	443	68,140,220	1,097	3,832,242,737	687	2,114,748,605

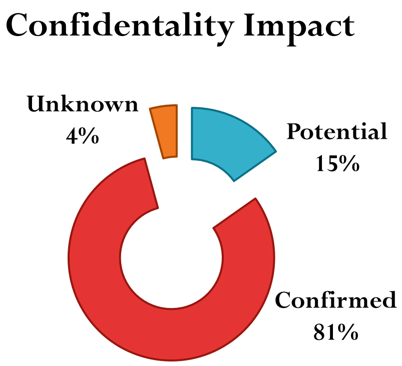
Mid-Year 2017 Top 10 Breaches Data Types and Severity Scores[1]

Breach Type	Records Exposed	Percentage of Total Exposed	Data Type[2]	Severity Score
Web	2,000,000,000	33.2%	ADD/NAA/NUM	10.0
Web	1,374,159,612	22.8%	ADD/EMA/FIN/MISC/NAA	10.0
Hack	1,221,893,767	20.3%	EMA/PWD	10.0
Web	267,693,854	4.5%	EMA/NUM	9.80
Web	198,000,000	3.3%	ADD/DOB/MISC/NAA/NUM	10.0
Web	135,000,000	2.2%	ADD/FIN/MISC/NAA/NUM/SSN	9.68
Hack	129,696,449	2.2%	EMA/PWD	9.71
Hack	126,761,168	2.1%	ADD/NAA/NUM	9.40
Hack	91,890,110	1.5%	EMA/PWD/USR	9.56
Hack	77,000,000	1.3%	EMA/PWD/USR	9.96
The top 10 breaches exposed 5,622,094,960 records, or 93.4% of the total records exposed in the first 6 months				

Mid-Year 2017 Analysis by Data Family

	Percentage of Total Breaches	Percentage of Total Exposed Records	Percentage of Total Breaches	Percentage of Total Exposed Records
Data Family	**Mid-Year 2016**	**Mid-Year 2016**	**Mid-Year 2017**	**Mid-Year 2017**
Electronic	90.18%	99.98%	93.22%	99.98%
Physical	6.75%	<1%	4.62%	<1%
Unknown	3.07%	<1%	2.16%	<1%

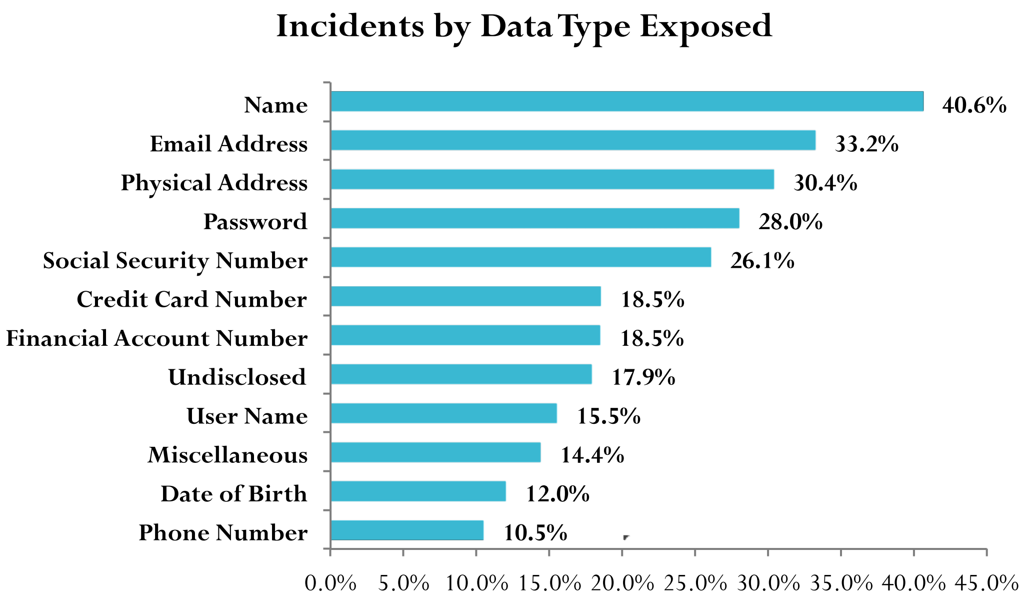
Mid-Year 2017 Confidentiality Impact



The majority of breaches continue to result in confirmed unauthorized access to sensitive data

[1] See page 13 for additional detail on these incidents.
[2] See page 17 for a description of abbreviations.

Mid-Year 2017 Analysis by Data Type - Percentage of Breaches



Compared to the same time period in 2016, the percentage of breaches impacting Social Security numbers increased from 17.6% in 2016 to 26.1% in 2017. Likewise, the percentage of breaches impacting Names increased from 36.1% to 40.6% and the percentage impacting physical addresses increased from 21.6% to 30.4%. Research indicates this effect is attributable to the steady rise of successful phishing campaigns targeting W-2 data during the first 4 months of the year.

Percentage of Breaches Exposing Data Types YTD 2017 vs. Prior Years

Data Type	First 6 Months 2017	First 6 Months 2016	First 6 Months 2015
Name	40.6%	36.1%	27.8%
Email Address	33.2%	42.9%	45.5%
Physical Address	30.4%	21.6%	12.3%
Password	28%	39.8%	52.2%

The "W-2 phishing effect" is more evident when comparing the percentage of breaches impacting 2017's top four data types over time. Access credentials in the form of username / email address and password remain popular targets, but the overall number of breaches impacting these records has steadily declined during the first half of 2017 as attention turns to data more directly useful for tax fraud.

Mid-Year 2017 Analysis of Records per Breach

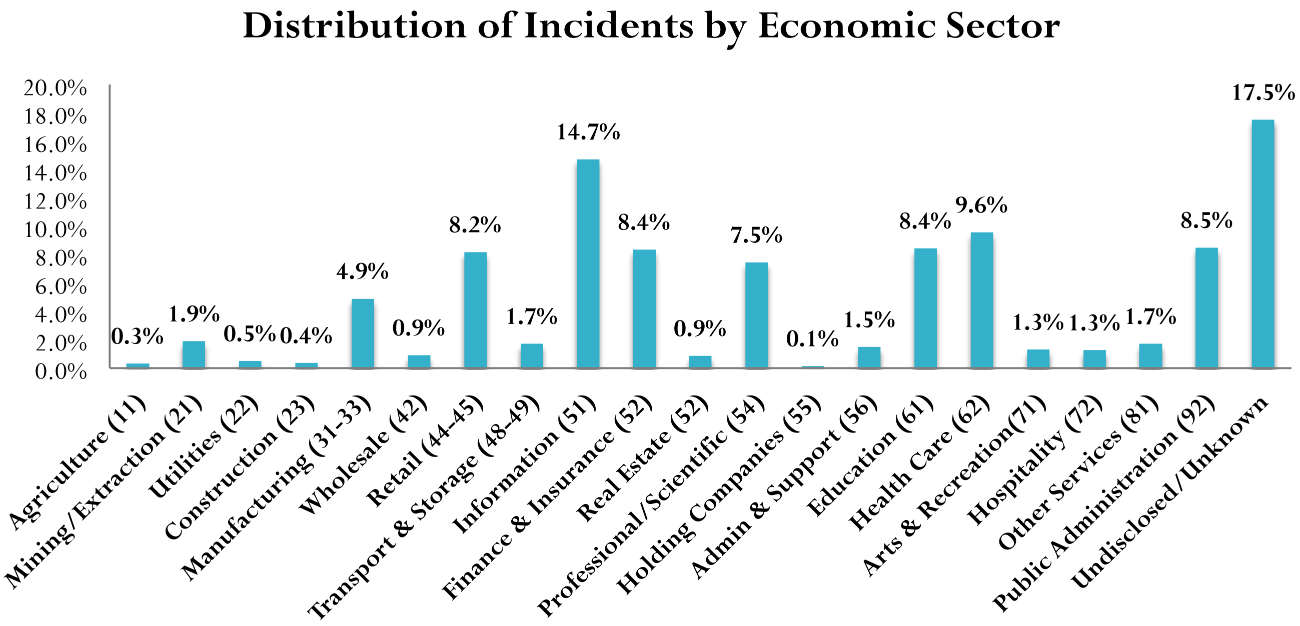
Exposed Records	Number of Breaches	Percent of Total
Unknown/Undisclosed	1024	46.0%
1 to 100	317	14.2%
101 to 1,000	336	15.1%
1,001 to 10,000	320	14.4%
10,001 to 100,000	132	5.9%
100,001 to 500,000	36	1.6%
500,001 to 999,999	12	0.5%
1 M to 10 M	30	1.3%
> 10 M	20	0.9%

For the third year in a row, the number of incidents with exposed records either unknown or unreported increased. At this point in 2015, it was 27.6%; in 2016, it was 35.4%.

Mid-Year 2017 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	927	1,839,750,699	1,984,629	30.59%
Skimming	272	4,874	18	0.00%
Phishing	253	458,964	1,814	0.01%
Virus/Malware	209	6,918,120	33,101	0.12%
Web	158	4,069,836,698	25,758,460	67.67%

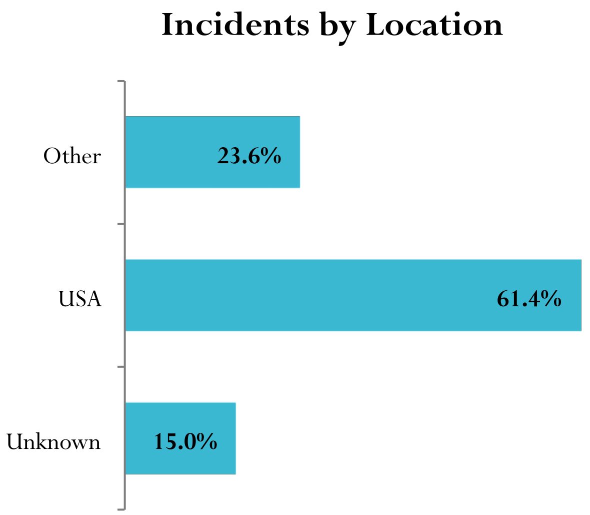
Mid-Year 2017 Analysis of Incidents by NAICS Economic Sector

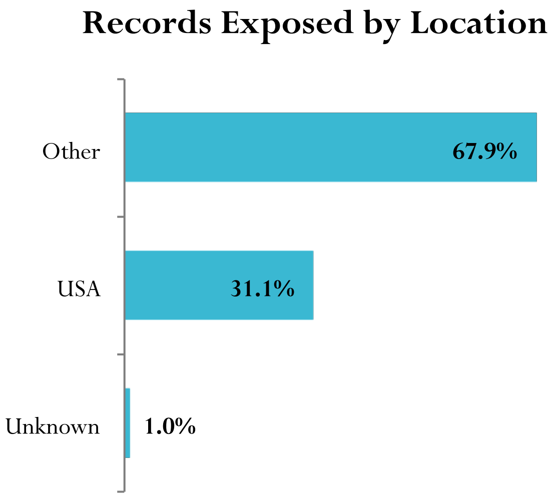


Distribtuion of Business Groups Within Economic Sectors – Top 3

Economic Sector	Business Group	Percentage of Breaches Within Economic Sector
Information (51)	Software / Web Services	79.9%
	Mass Media	11.2%
	Telecommunications	7.3%
HealthCare (62)	Non-Hospital Facilities	33.3%
	Hospitals	29.5%
	Practitioner Offices	29.5%
Public Sector (92)	Federal	33.8%
	State	20.6%
	Cities	19.5%

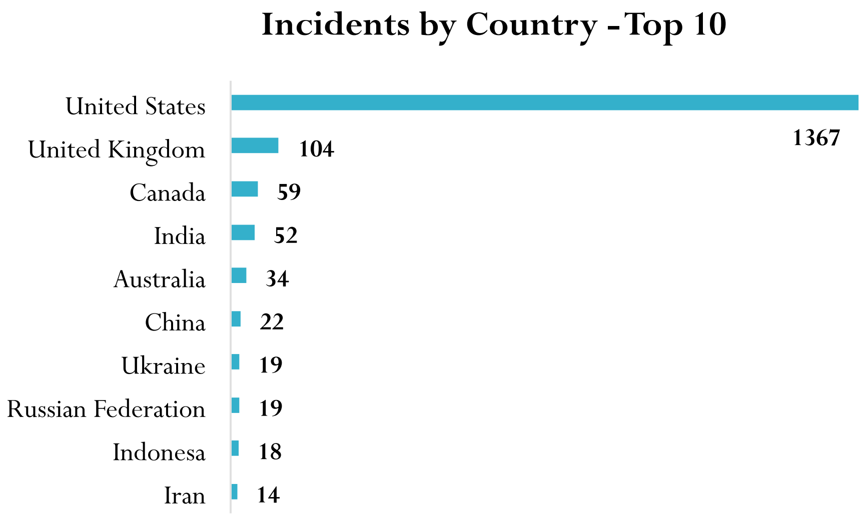
Mid-Year 2017 Analysis by Country





The Top 10 countries accounted for 1,708, or 76.6% of the breaches reported and 97.7% of the records compromised.

Mid-Year 2017 Analysis by Country – Top 10



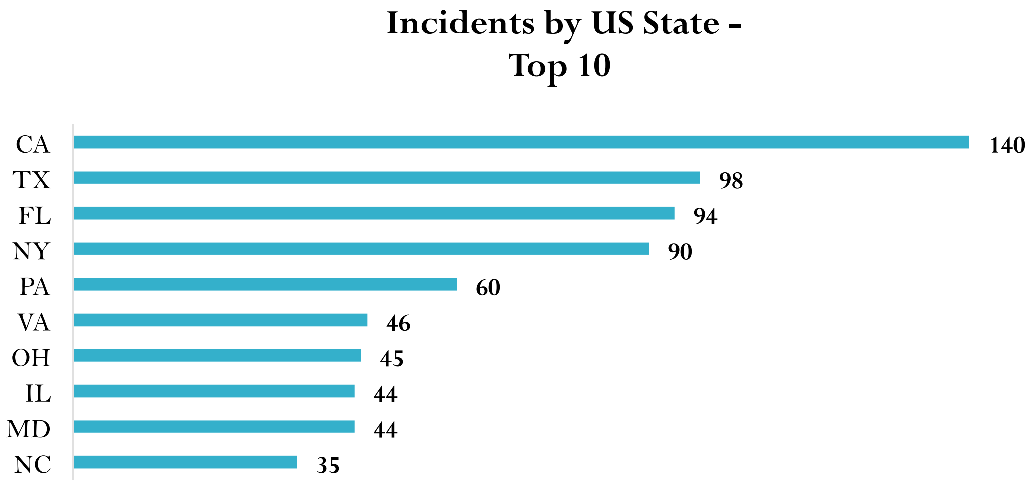
North America accounted for 64.2% of breaches

Mid-Year 2017 Exposed Records by Country

Ranking	Number of Breaches	Country	Total Exposed Records	Average Records per Breach	Median Number of Records	Percentage of Exposed Records
1	22	China	3,822,024,257	173,728,375	3,371,754	48.83%
2	1367	United States	3,746,193,334	2,740,449	1,700	47.86%
3	52	India	179,055,018	3,443,366	308	2.29%
4	2	Philippines	55,254,020	27,627,010	-	0.71%
5	7	Hong Kong	12,041,792	1,720,256	1,890,876	0.15%
6	4	South Africa	6,700,000	1,675,000	-	0.09%
7	104	United Kingdom	2,401,829	23,095	669	0.03%
8	59	Canada	2,107,262	35,716	503	0.03%
9	2	Finland	1,100,023	550,012	-	0.01%
10	7	Japan	722,096	103,157	121	0.01%

Large breaches affecting 1,000,000 or more records heavily influences the average number of records lost in certain countries. The median number of records lost in the five countries reporting the most breaches ranges between 308 and 1,700, with Australia coming in at 872.

Mid-Year 2017 Distribution of Breaches By State

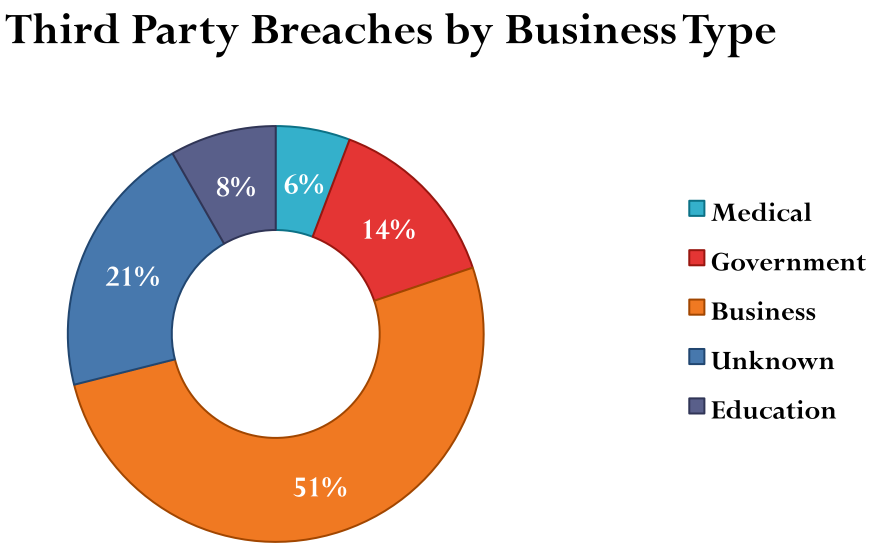


The top 10 states represent 51% of US breaches.

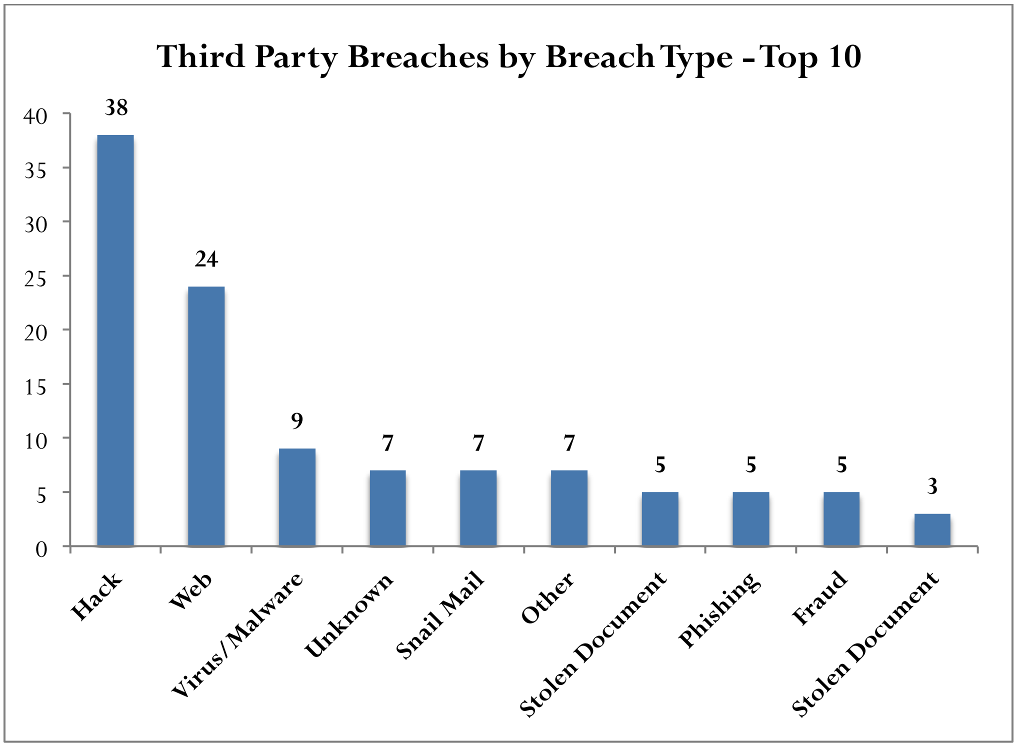
Mid-Year 2017 Analysis of US State Rankings- Exposed Records

Exposed Records Ranking	US State	Total Exposed Records	Number of Breaches	Exposed Records/Breach	Percentage of USA Exposed Records
1	WA	1,375,336,881	27	50,938,403	73.42%
2	NJ	33,724,579	29	1,162,917	1.31%
3	CA	10,690,370	140	76,360	0.31%
4	NY	8,163,474	90	90,705	0.19%
5	AR	4,890,000	7	698,571	0.16%
6	TX	4,777,984	98	48,755	0.15%
7	GA	3,798,732	23	165,162	0.10%
8	MD	2,674,211	44	60,778	0.09%
9	MI	2,426,296	22	110,286	0.07%
10	FL	1,519,843	94	16,169	0.02%

Mid-Year 2017 Breaches Involving Third Parties



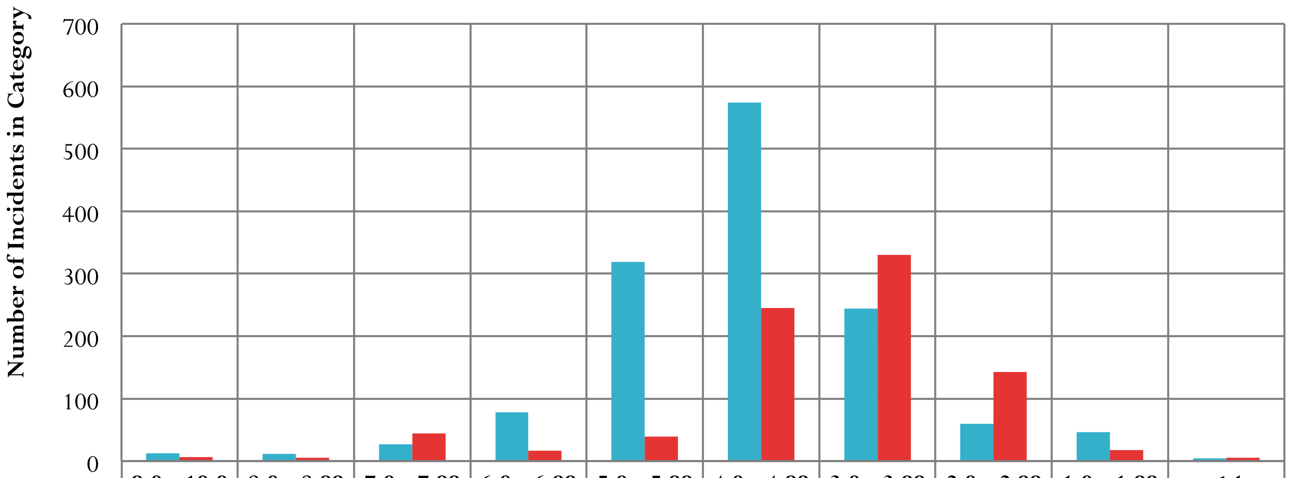
- Organizations classified in the business sector account for more than 50% of the breaches impacting data belonging to customers, clients or other 3rd parties.
- Three of the largest breaches reported in the first six months impacted 3rd parties.
- Hacking remains the dominant breach type for incidents impacting 3rd Parties, with regard to both the number of breaches and the number of records compromised.



Mid-Year 2017 – Breach Severity Scores & Scoring

We can all readily agree that not all data breaches are created equal. Where disagreement arises is when we attempt to rate the ‘severity’ or ‘impact’ 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.

Breach Severity Scores by Quarter



	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
🟦 1Q2017	12	11	27	78	319	574	244	60	46	4
🟥 2Q2017	6	5	44	17	39	245	330	143	18	5

On a positive note, breach severity scores declined in the second quarter of 2107. 58.2% of breaches reported in Q2 scored 3 or below while 25.7% of Q1 reported breaches scored 3 or below.

Mid-Year 2017 – Breach Severity Scores – Top 10

Score	Reported	Organization	Top 10 Summary
10	Q2	DU Group dba DU Caller	(Web) 2,000,000,000 user phone numbers, names and addresses inappropriately made accessible in an uncensored public directory
10	Q1	NetEase, Inc. dba 163.com	(Hacking) 1,221,893,767 email addresses and passwords stolen by hackers and sold on the Dark Web by DoubleFlag
10	Q1	River City Media, LLC	(Web) 1,374,159,612 names, addresses, IP addresses, and email addresses, as well as an undisclosed number of financial documents, chat logs, and backups exposed by faulty `rsync` backup
10	Q2	Deep Root Analytics	(Web) Approximately 198,000,000 voter names, addresses, dates of birth, phone numbers, political party affiliations, and other demographic information exposed in an unsecured Amazon S3 bucket

Score	Reported	Organization	Top 10 Summary
9.96	Q2	Edmodo	(Hacking) 77,000,000 user email addresses, usernames, and bcrypt hashed passwords with salts stolen by hackers through undisclosed means
9.80	Q1	EmailCar	(Web) 267,693,854 email addresses and phone numbers exposed in an unsecure MongoDB installation and later dumped on the Internet
9.71	Q1	Tencent Holdings Ltd dba QQ.com	(Hacking) 129,696,449 email addresses and passwords stolen by hackers and sold on the Dark Web by DoubleFlag
9.68	Q2	National Social Assistance Programme (India)	(Web) Roughly 135,000,000 Aadhaar numbers and 100,000,000 linked bank account numbers, as well as names, caste, religion, addresses, phone numbers, photographs, and assorted financial details leaked on government web portals
9.56	Q2	Youku	(Hacking) 91,890,110 user accounts with usernames, email addresses and MD5 encrypted passwords compromised by hackers and offered for sale
9.45	Q1	Yahoo Japan	(Hacking) 23,590,165 email addresses and passwords stolen by hackers and sold on the Dark Web by DoubleFlag

Top 20 Largest Breaches All Time (Exposed Records Count)

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Highest All Time **5/13/2017**	User phone numbers, names and addresses inappropriately made accessible in an uncensored public directory	2 Billion	DU Caller Group (DU Caller)	Business - Technology	China
Number 2 **3/3/2017**	Names, addresses, IP addresses, and email addresses, as well as an undisclosed number of financial documents, chat logs, and backups, exposed by faulty rsync backup.	1.3 Billion	River City Media, LLC	Business - Technology	United States
Number 3 **1/25/2017**	A database holding email addresses and passwords stolen by hackers and offered for sale on the dark web.	1.2 Billion	NetEase, Inc. dba 163.com	Business – Technology	China

Breach Reported Date	Summary	Records Exposed	Organization’s Name	Industry-Sector	Breach Location
Number 4 12/14/2016	While investigating the #4 incident on this list, a second hacking event was discovered targeting user names, email addresses, phone numbers, dates of birth, hashed passwords and security questions and associated answers.	1 Billion	Yahoo	Business - Technology	United States
Number 5 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 6 10/18/2016	Hackers exploit a Local File Inclusion vulnerability, compromising member email addresses, usernames, and encrypted passwords, IP addresses and membership statuses.	412 Million	FriendFinder Networks, Inc	Business - Technology	United States
Number 7 5/27/2016	Hack exposes user account records containing SHA1 encrypted passwords, email addresses.	360 Million	MySpace	Business - Technology	United States
Number 8 1/1/2017	Email addresses and phone numbers were exposed in an unsecure MongoDB installation, which was later downloaded and dumped on the Internet	267 Million	EmailCar	Business - Technology	China
Number 9 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 10 12/3/2016	Hackers offer for sale a database containing a variety of personal and financial details.	203 Million	Organization’s Name has not been reported	Unknown	Unknown
Number 11 10/19/2013	Fraudulent account used to gain access to credit card numbers, social security numbers, names, and financial account numbers.	200 Million	Court Ventures, Inc.	Business - Data	United States
Number 12 6/19/2017	Unsecured Amazon S3 bucket exposes voter names, addresses, dates of birth, contact information and voter preferences.	198 Million	Deep Root Analytics	Business / Business	United States

Breach Reported Date	Summary	Records Exposed	Organization’s Name	Industry-Sector	Breach Location
Number 13 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 14 6/21/2014	Hack exposes trip details of customers after cracking MD5 hashes	173 Million	NYC Taxi & Limousine Commission	Government - City	United States
Number 15 6/23/2016	Hack exposes USA voter information.	154 Million	Organization’s Name has not been reported	Unknown	United States
Number 16 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 17 3/17/2012	Firm may have illegally bought and sold customers' information.	150 Million	Shanghai Roadway D&B Marketing Services Co.	Business - Data	China
Number 18 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 19 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 20 5/2/2017	Leaky governmental websites expose Aadhaar numbers, banking details, names and other personal information.	135 Million	National Social Assistance Programme	Government - Federal	India

Methodology & Terms

Risk Based Security's research methods include automated processes coupled with traditional human research and analysis. Our proprietary applications crawl the Internet 24x7 to capture and aggregate potential data breach breaches for our researchers to analyze. In addition, the research team manually verifies news feeds, blogs, and other sources looking for new data breaches as well as new information on previously disclosed incidents. The database also includes information obtained through Freedom of Information Act (FOIA) requests, seeking breach notification documentation from various state and federal agencies in the United States. The research team extends our heartfelt thanks to the individuals and agencies that assist with fulfilling our requests for information.

Data Standards and the use of "Unknown"

In order for any data point to be associated with a breach entry, Risk Based Security requires a high degree of confidence in the accuracy of the information reported as well as the ability to reference a public source for the information. In short, the research team does not guess at the facts. For this reason the term "Unknown" is used when the item cannot be verified in accordance with our data validation requirements. This can occur when the breached organization cannot be identified but leaked data is confirmed to be valid or when the breached organization is unwilling or unable to provide sufficient clarity to the data point.

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
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

Name	Description
Stolen Mobile	Stolen mobile phone or device such as tablets, etc.
Stolen Tape	Stolen backup tapes
Unknown	Unknown or unreported breach type
Virus (Malware)	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

NO WARRANTY.

Risk Based Security, Inc. makes this report available on an "As-is" basis and offers no warranty as to its accuracy, completeness or that it includes all the latest data breach breaches. The information contained in this report is general in nature and should not be used to address specific security issues. Opinions and conclusions presented reflect judgment at the time of publication and are subject to change without notice. Any use of the information contained in this report is solely at the risk of the user. Risk Based Security, Inc. assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. If you have specific security concerns please contact Risk Based security, Inc. for more detailed data loss analysis and security consulting services.

About Risk Based Security

Risk Based Security (RBS) provides detailed information and analysis on Data Breaches, Vendor Risk Scores and Vulnerability Intelligence. Our products, Cyber Risk Analytics (CRA) and VulnDB, provide organizations with access to the most comprehensive threat intelligence knowledge bases available, including advanced search capabilities, access to raw data via API, and email alerting to assist organizations in taking the right actions in a timely manner. In addition, our YourCISO offering provides organizations with on-demand access to high quality security and information risk management resources in one, easy to use web portal.

VulnDB is the most comprehensive and timely vulnerability intelligence available and provides actionable information about the latest in security vulnerabilities via an easy-to-use SaaS Portal, or a RESTful API for easy integration into GRC tools and ticketing systems. VulnDB allows organizations to search on and be alerted to the latest vulnerabilities, both in end-user software and the third-party libraries or dependencies that help build applications. A subscription to VulnDB provides organizations with simple to understand ratings and metrics on their vendors and products, and how each contributes to the organization's risk-profile and cost of ownership.

Cyber Risk Analytics (CRA) provides actionable security ratings and threat intelligence on a wide variety of organizations. This enables organizations to reduce exposure to the threats most likely to impact them and their vendor base. In addition, our PreBreach vendor risk rating, the result of a deep-view into the metrics driving cyber exposures, are used to better understand the digital hygiene of an organization and the likelihood of a future data breach. The integration of PreBreach ratings into security processes, vendor management programs, cyber insurance processes and risk management tools allows organizations to avoid costly risk assessments, while enabling businesses to understand its risk posture, act quickly and appropriately to proactively protect its most critical information assets.

YourCISO provides organizations with on-demand access to high quality security and information risk management resources in one, easy to use web portal. YourCISO provides organization ready access to a senior executives and highly skilled technical security experts with a proven track record, matched specifically to your needs. The YourCISO service is designed to be an affordable long term solution for addressing information security risks. YourCISO brings together all the elements an organization needs to develop, document and manage a comprehensive information security program.

For more information, please visit:

https://www.riskbasedsecurity.com/
https://vulndb.cyberriskanalytics.com/
https://www.cyberriskanalytics.com/
https://www.yourciso.com/

Or call 855-RBS- RISK.