Data Breach QuickView

Third Quarter 2015 Data Breach Trends

Sponsored by:
Risk Based Security

Data Breaches - at the 3/4 pole …

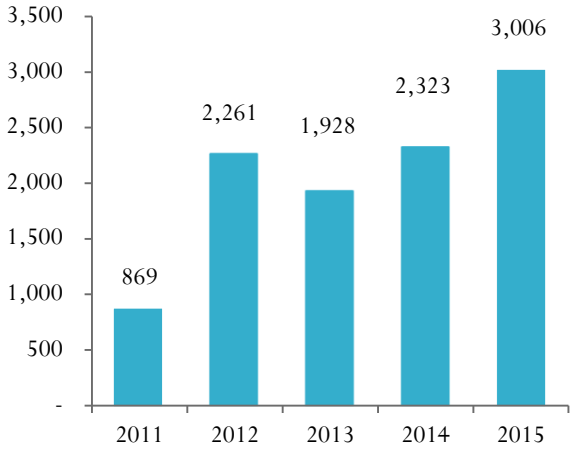
- There were 3006 incidents reported during the first nine months of 2015 exposing 366 million records.
- Six Hacking incidents alone exposed a combined 220 million records.
- A single act of Hack of Anthem Insurance Companies exposed 78.8 million records. (#15 All Time)
- The Business sector accounted for 44.9% of reported incidents, followed by Unknown (19.7%), Education (16.9%), Government (12.3%), and Medical (6.2%).
- The Business sector accounted for 58.0% of the records exposed, followed by Government (23.5%), and Unknown (15.6%).
- 66.3% of reported incidents were the result of Hacking, which accounted for 83.2% of the exposed records.
- Skimming, the number two breach type, accounted for 171 incidents but only exposed 24,973 records.
- Breaches involving U.S. entities accounted for 39.4% of the incidents and 42.5% of the exposed records.
- 40.4% of the incidents exposed between one and 100 records.
- Twenty-eight (28) incidents exposed one million or more records.
- Ninety-nine organizations reported multiple breaches in 2015.
- 78.5% of incidents involved outside the organization activity.
- 56.9% of all incidents exposed between 1 and 1,000 records.
- The number of reported incidents tracked by Risk Based Security will exceed 18,000 in 2015 and may exceed 4.0 billion exposed records.

RiskBased SECURITY

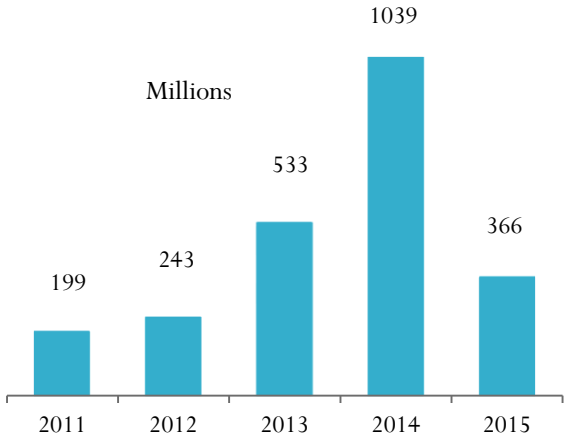
Not Just Security, the Right Security.

Third Quarter 2015 Compared to Third Quarter of the Past Four Years

Number of Incidents - Third Quarter 2015

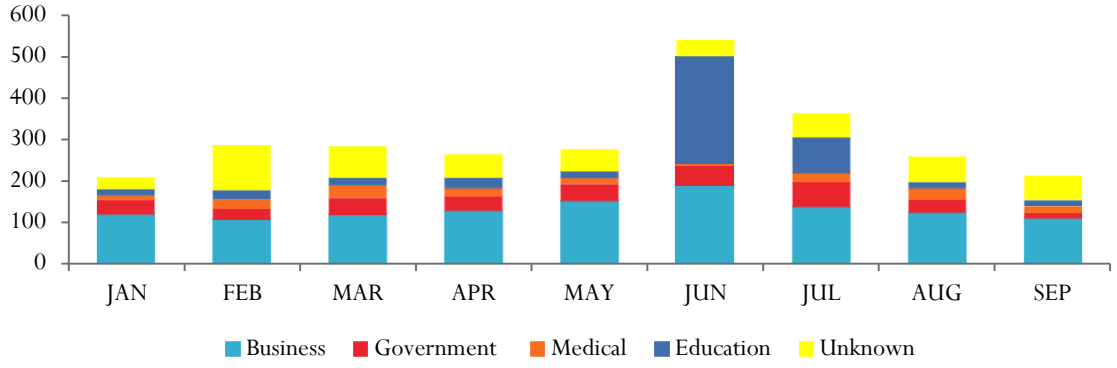


Number of Records Exposed - Third Quarter 2015

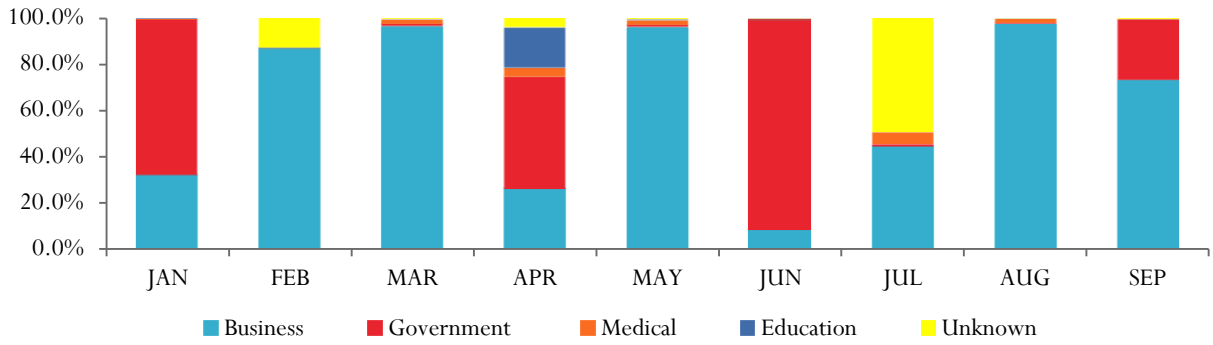


First Nine Months of 2015 by Industry by Month

Third Quarter 2015 Incidents by Industry

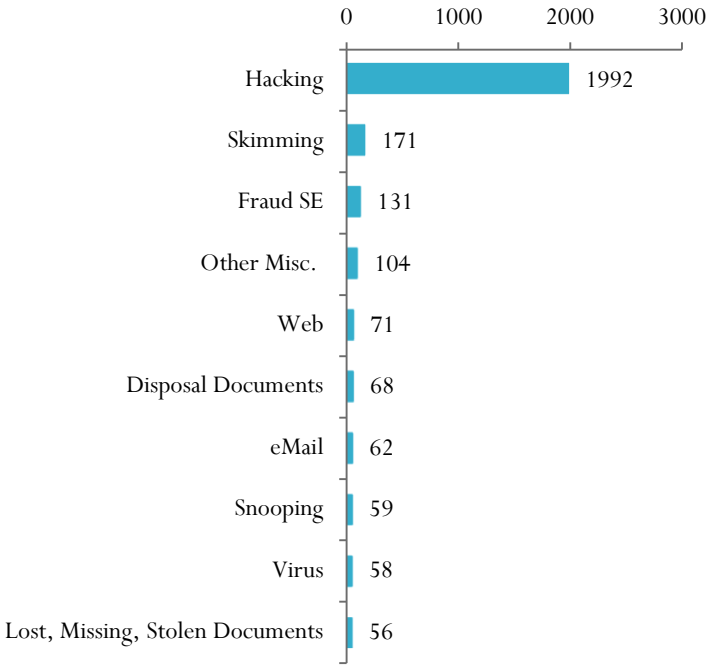


Third Quarter 2015 Exposed Records by Industry



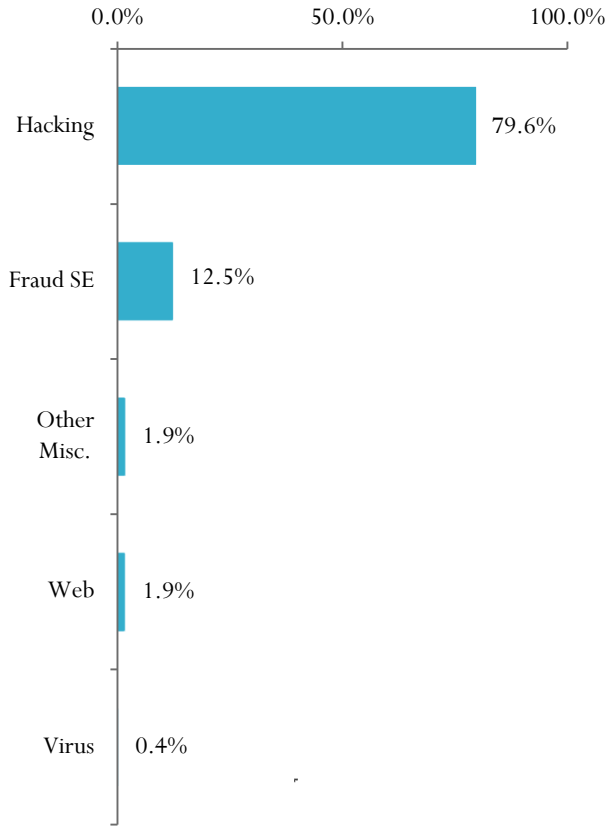
Third Quarter 2015 Analysis by Breach Type

Third Quarter 2015 Incidents - Top 10 Breach Types



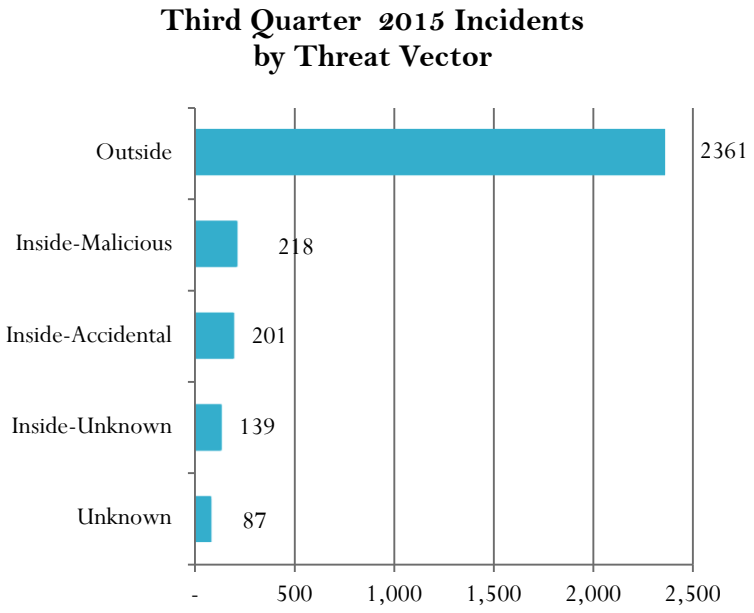
The number of breaches caused by Hacking, (66.3%), dwarfs all other breach types reported.

Third Quarter 2015 Records Exposed by Breach Type



Top Five Breach types accounted for 96.4% of all exposed records.

Third Quarter 2015 Analysis by Threat Vector



78.5% of incidents involved outside the organization activity.

Third Quarter 2015 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	303,545,259
Inside-Malicious	3,772,212
Inside-Accidental	12,433,527
Inside-Unknown	46,054,307
Unknown	399,560
Total	**366,204,865**

82.9% of the total exposed records are the result of Outside activity.

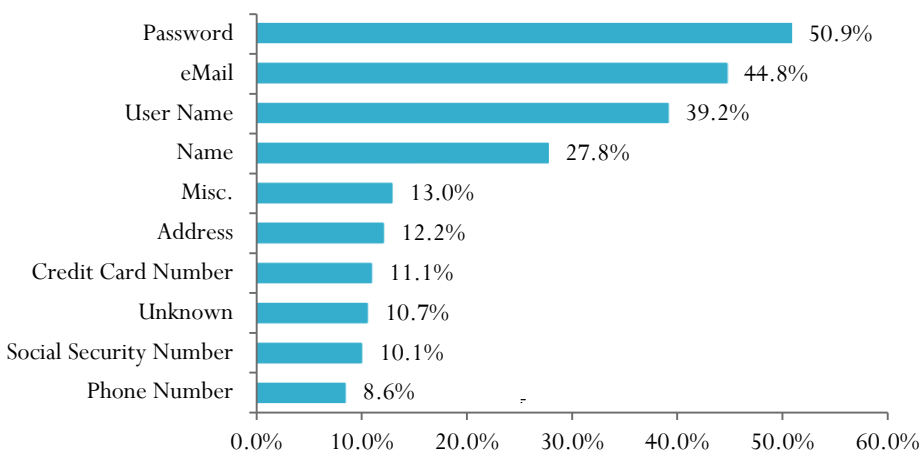
Five incidents, all Hacks, Anthem (78.8 million), Republic of Turkey (50.0 million), Unknown Organization, (44.0 million), Avid Life Media, Inc. (39 million) U.S. Office of PM, (21.5 million) accounted for 233.3 million exposed records, (63.7%).

Third Quarter 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	3Q2015	3Q2015	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.

Third Quarter 2015 Analysis by Data Type – Percentage of Incidents



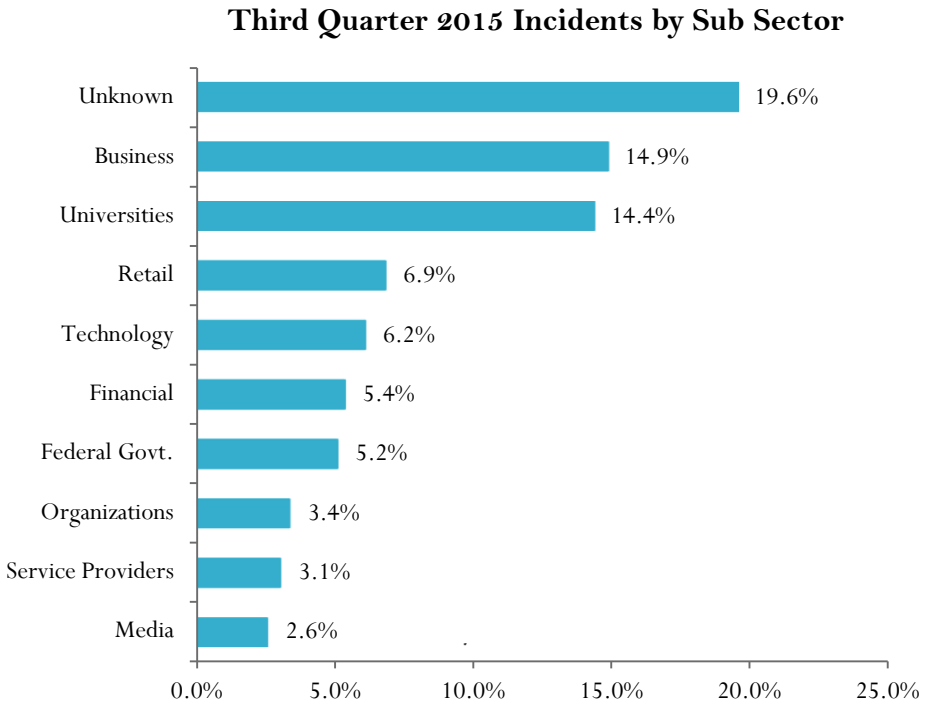
Third Quarter 2015 Percentage of Incidents Exposing Data Types vs. 2014

Data Type	3Q2015	2014
Password	50.9%	57.4%
eMail	44.8%	47.5%
User Name	39.2%	48.9%
Name	27.8%	31.8%

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

- Percentage of incidents exposing Passwords shows a slight decline
- Percentage of incidents exposing User Names also has declined YTD

Third Quarter 2015 Analysis by Industry Sub Type



- The Insurance sector accounted for 27.4% of the exposed records followed by the Federal Governments at a close 21.9%.
- Universities move into the #3 spot in number of incidents accounting for 14.4%.

Of the 433 incidents occuring at colleges and universities during the first nine months of 2015, 397, 91.7% were due to Hacking. The Average number of records exposed equaled

1,626, 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 (62.6%), User Names (57.9%), and eMail Addresses (47.3%). 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 attackers see user names and passwords as prize targets.

Third Quarter 2015 Analysis of Records per Incident

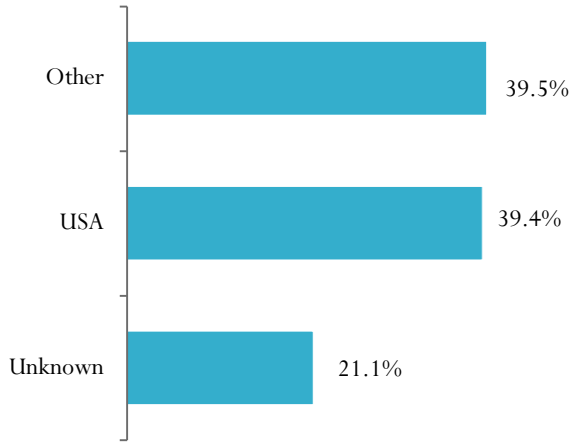
Exposed Records	Number of Incidents	Percent of Total
Unknown	847	28.2%
1 to 100	1197	39.8%
101 to 1,000	514	17.1%
1,001 to 10,000	306	10.2%
10,001 to 100,000	82	2.7%
100,001 to 500,000	23	0.8%
500,001 to 999,999	9	0.3%
1 M to 10 M	20	0.7%
> 10 M	8	0.3%

The number of incidents with exposed records reported as "Unknown" is 28.2% for 3Q2015 – an increase over 2014's 19.2%.

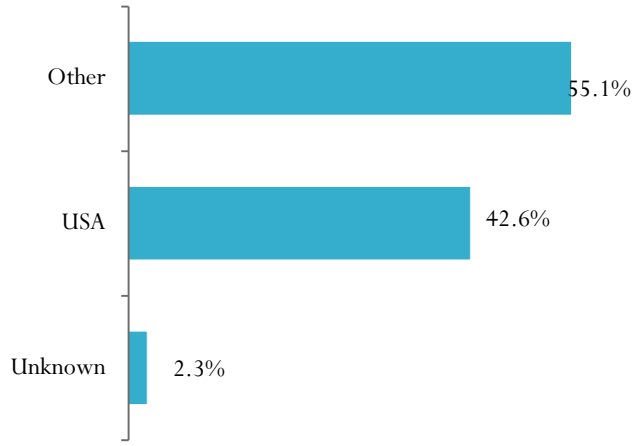
- 56.9% of incidents exposed between 1 and 1000 records

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

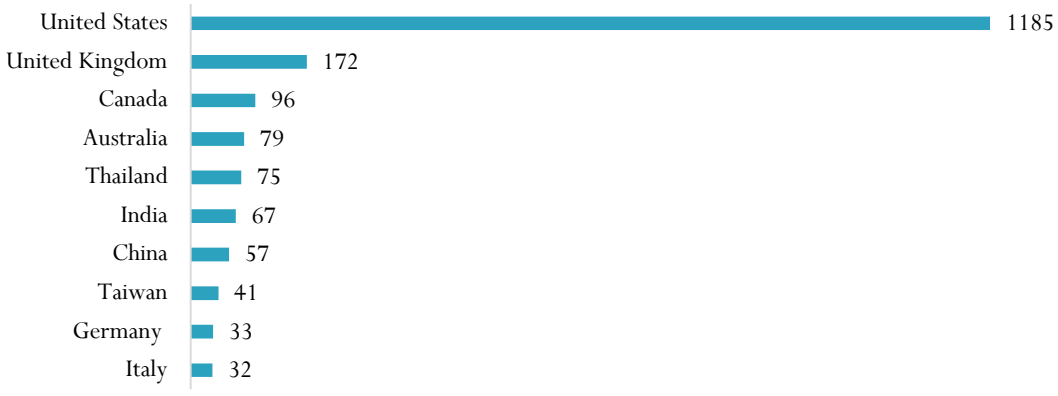
Third Quarter 2015 Incidents by Location



Third Quarter 2015 Records by Location



Third Quarter 2015 Incidents by Country - Top 10

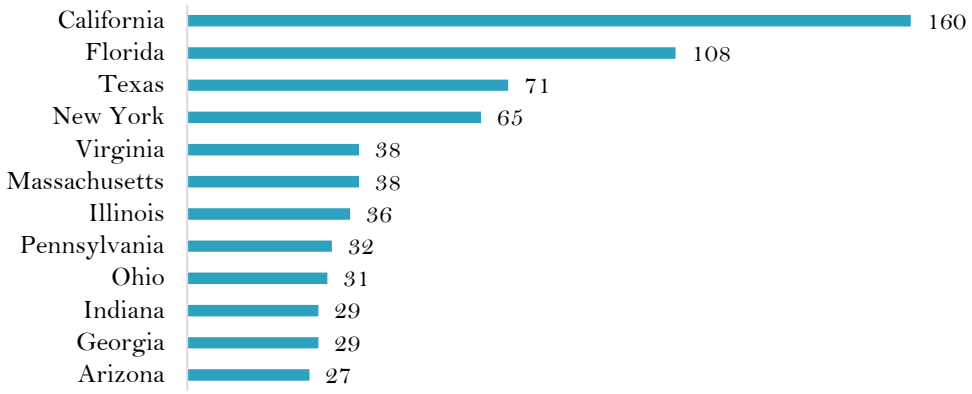


Third Quarter 2015 Exposed Records by Country – Top 10

Exposed Records Ranking	Country	Total Exposed Records	Average Records per Breach	Percentage of Exposed Records
1	United States	155,740,256	131,426.38	42.53%
2	Republic of Turkey	50,000,910	2,941,230	13.65%
3	Canada	45,127,473	470,078	12.32%
4	South Korea	44,168,680	1,766,747	12.06%
5	Russian Federation	26,720,955	1,571,821	7.30%
6	United Kingdom	10,523,386	1,169,265	2.87%
7	Pakistan	10,050,929	13,158	2.74%
8	Japan	9,124,268	608,285	2.49%
9	China	2,263,126	17,736	0.62%
10	India	1,010,971	150,014	0.28%

Third Quarter 2015 Analysis of US State Rankings

Third Quarter 2015 Incidents by US State - Top 10



Top 10 represent 56.0% of US incidents.

Exposed Records Ranking	US State	Total Exposed Records	Percentage of USA Exposed Records
1	Indiana	83,185,997	53.41%
2	District of	21,954,713	14.10%
3	California	14,812,496	9.51%
4	New York	11,462,758	7.36%
5	Alaska	11,001,023	7.06%
6	Unknown	10,790,781	6.93%
7	Colorado	4,598,027	2.95%
8	Washington	1,507,200	0.97%
9	Maryland	1,133,253	0.73%
10	Virginia	1,017,447	0.65%

Top three states represent 77.0% of exposed US records.

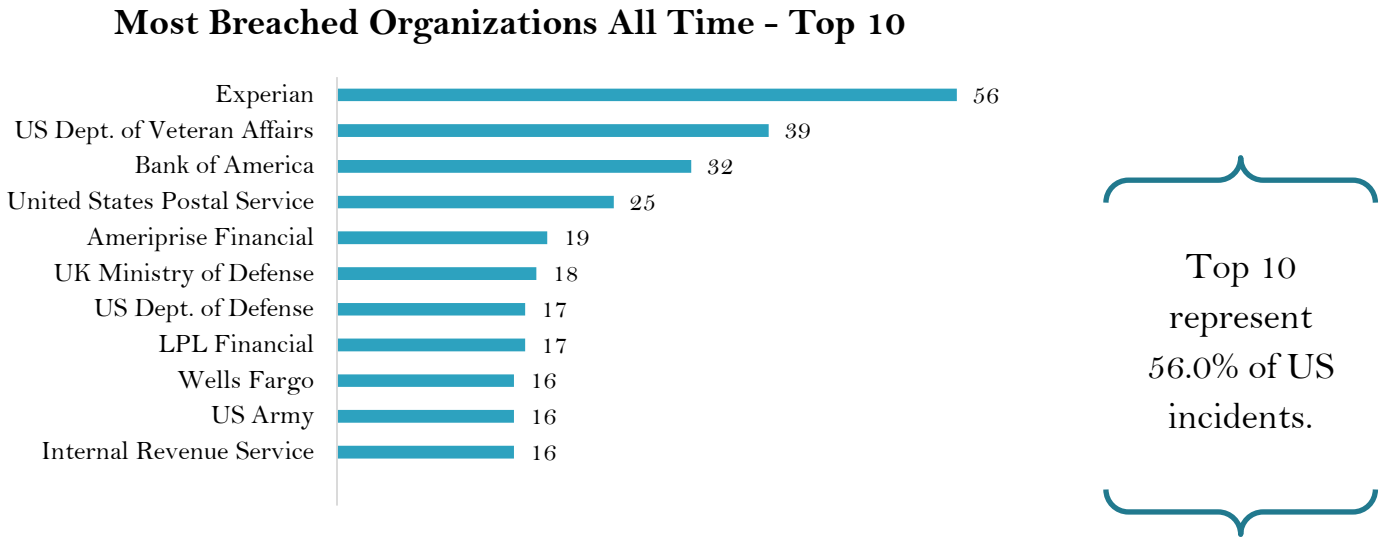
Third Quarter 2015 Analysis of Business Types

Business Type	Incidents	Exposed Records	Average Records per Breach	#1 Breach Type (Incidents)	#2 Breach Type (Incidents)
Business	1345	212,460,142	157,963	Hack (65.6%)	Skimming (10.9%)
Education	506	768,274	1,518	Hack (86.0%)	Web (2.8%)
Medical	186	9,546,015	51,323	Hack (13.4%)	Snooping (12.4%)
Government	370	86,193,867	232,956	Hack (88.2%)	Missing Drive (7.0%)
Unknown	599	57,236,567	95,554	Hack (82.5%)	Fraud SE (4.4%)

Business Type	#1 Sector (Incidents)	#2 Sector (Incidents)	#1 Exposed Record	#2 Exposed Record	#1 Sector (Records)	#2 Sector (Records)	#1 Breach Type (Records)
Business	Retail (15.3%)	Technology (13.2%)	Passwords (52.2%)	User Names (43.2%)	Insurance (47.3%)	Technology (23.1%)	Hack (92.6%)
Education	University (85.4%)	High School (4.5%)	Passwords (58.3%)	User Names (53.8%)	University (91.5%)	High School (2.5%)	Web (48.2%)
Medical	Provider (49.5%)	Hospital (23.7%)	Name (66.7%)	Medical Info. (57.5%)	Provider (52.8%)	Technology (40.9%)	Hack (90.6%)
Government	Federal (41.2%)	City (19.2%)	Name (35.1%)	Password (30.1%)	Federal (91.8%)	State (7.1%)	Hack (88.2%)
Unknown	N/A	N/A	eMail (75.6%)	Password (66.3%)	N/A	N/A	Fraud SE (77.5%)

Repeat Offenders [Back by Popular Demand]

Over fourteen-hundred organizations have multiple reported data breaches



Note: Experian was involved in an additional 49 breaches reported by other organizations.

A Break-down of Repeat Offenders

Number of Reported Data Breaches	Number of Organizations Reporting
> 50 Reported Breaches	1
> 40 Reported Breaches	1
> 30 Reported Breaches	3
> 20 Reported Breaches	4
> 10 Reported Breaches	32
> 5 Reported Breaches	94
> 4 Reported Breaches	153
> 3 Reported Breaches	259
2 or more Reported Breaches	1413

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.

So far in 2015, ninety-nine organizations reported multiple incidents, with one organization reporting as many as twelve incidents.

Government agencies top the 2015 list with 21 multiple incident organizations. The education sector, primarily universities, comes in second with 20 incidents followed by financials (12), energy (9) and medical (8).

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 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

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 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 19 7/2/2013	Unauthorized access to a website database exposed user names, email addresses and encrypted passwords	58 Million	Ubisoft	Technology	United States
Tied for Number 20 8/27/2008	Six people arrested for stealing records with personal information from government agencies, state firms, telecom companies and a TV shopping network	50 Million	Organization's Name has not been reported	Unknown	Taiwan

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Tied for Number 20 3/2/2013	Hackers gained access to usernames, email addresses and encrypted (hashed & salted) passwords	50 Million	Evernote	Technology	United States
Tied for Number 20 4/26/2013	Hackers gained access to customer names, emails, birthdates and hashed and salted passwords	50 Million	Living Social Inc.	Business	United States
Tied for Number 20 1/12/2015	Hackers gained access to various state agency servers exposing identification numbers	50 Million	Republic of Turkey	Federal Government	Turkey

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.)

Name	Description
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
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

