Data Breach QuickView Report

2016 Data Breach Trends – Year In Review

Sponsored by:
Risk Based Security

Issued in January 2017

2016 Sets new records, once again …

- There were 4,149 breaches reported during 2016 exposing over 4.2 billion records – approximately 3.2 billion more records than the previous all time high exposed in 2013.
- Top 10 breaches (9 Hacks[1] and 1 Web) exposed a combined 3 billion records.
- Top 10 Severity scores averaged 9.96 out of 10.0.
- The Business sector accounted for 51% of reported breaches, followed by Unknown (23.4%), Government (11.7%), Medical (9.2%), and Education (4.7%).
- The Business sector accounted for 80.9% of the number of records exposed, followed by Unknown (13.1%), Government (5.6%), Medical (.3%), and Education < .1%.
- 53.3% of reported breaches were the result of Hacking, which accounted for 91.9% of the exposed records.
- Malware accounted for 4.5% of the reported breaches, but represented just 0.4% of the records compromised.
- Breaches involving U.S. entities accounted for 47.5% of the breaches and 68.2% of the exposed records.
- 37.2% of the breaches exposed between one and 1000 records, 50.4% of breaches exposed between one and 10,000 records.
- 256 breaches involved Third Parties.
- Ninety-four (94) breaches in 2016 exposed one million or more records.
- Six (6) 2016 breaches have taken their place on the Top 10 List of All Time Largest Breaches.
- In December 2016, Yahoo reported the single largest breach ever disclosed, impacting over 1 billion records.
- The number of reported breaches tracked by Risk Based Security has exceeded 23,700, exposing over 9.2 billion records.

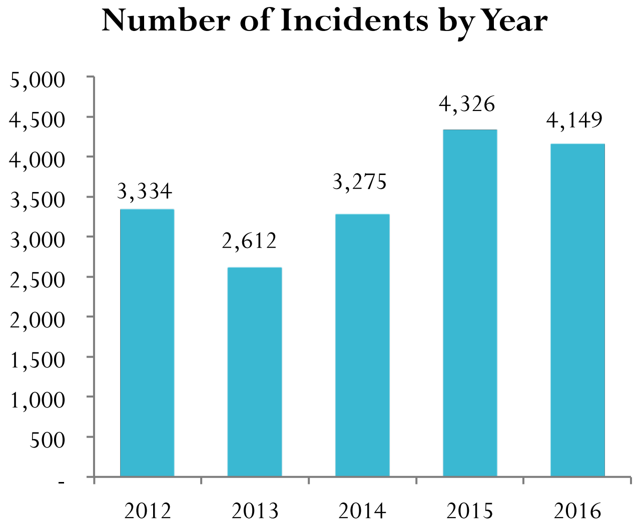
RiskBased SECURITY

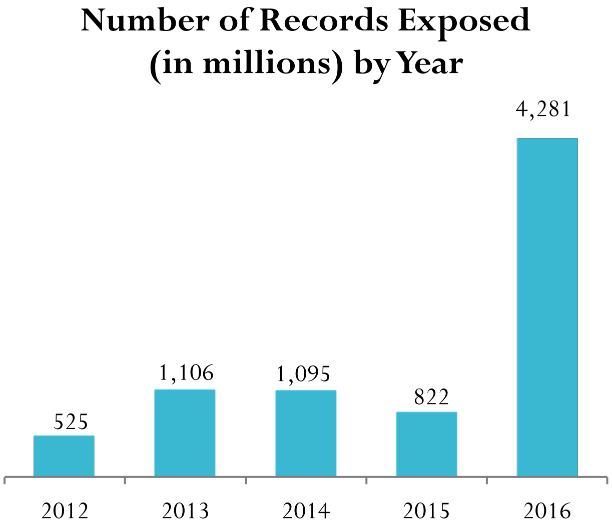
Not Just Security, the Right Security.

[1] See page 16 for definitions

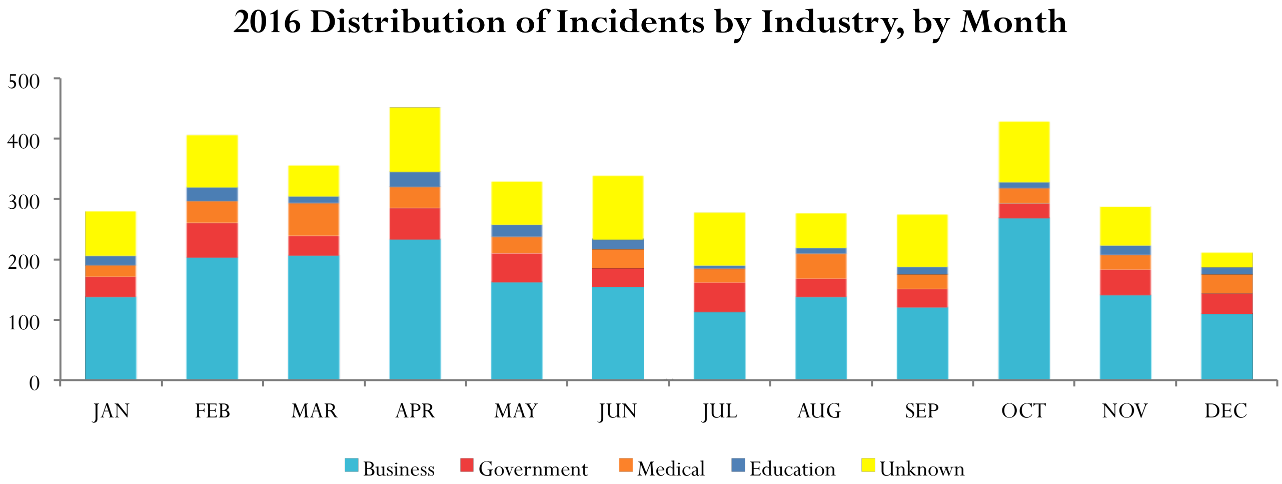
Table of Contents

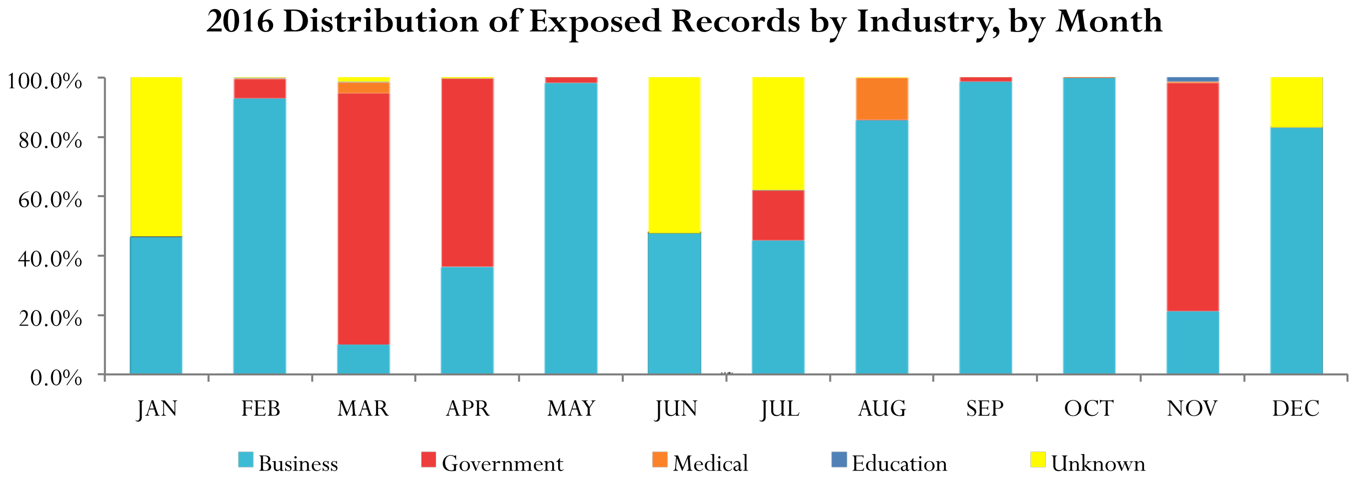
2016 Compared to the Prior Four Years


Number of Incidents by Year

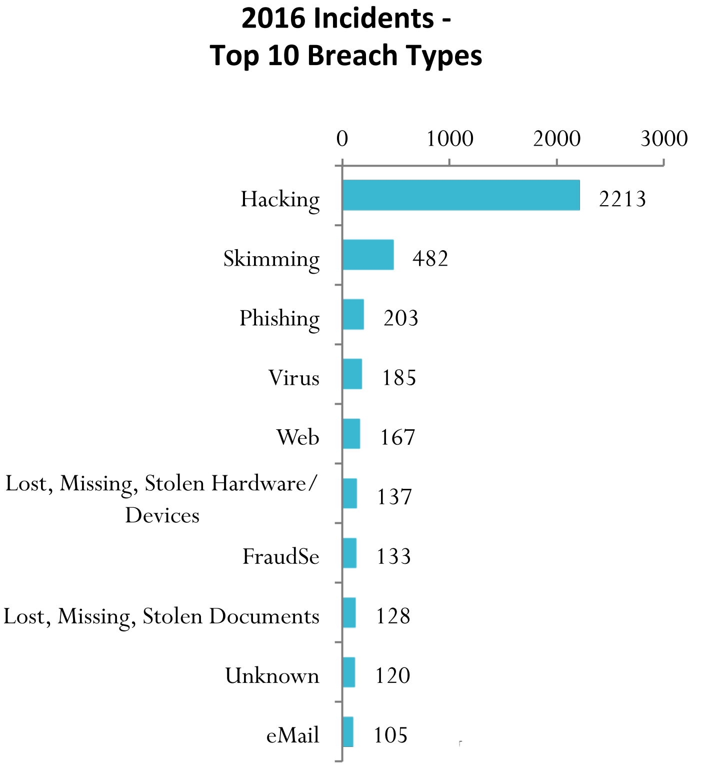

Number of Records Exposed (in millions) by Year

2016 by Industry by Month


2016 Distribution of Incidents by Industry, by Month

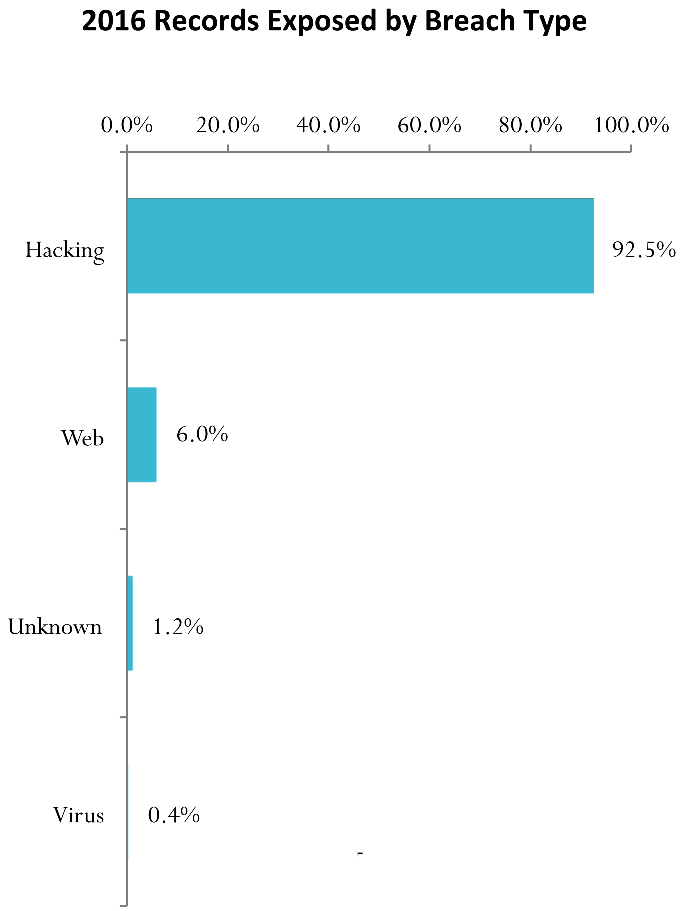

2016 Distribution of Exposed Records by Industry, by Month

2016 Analysis by Breach Type



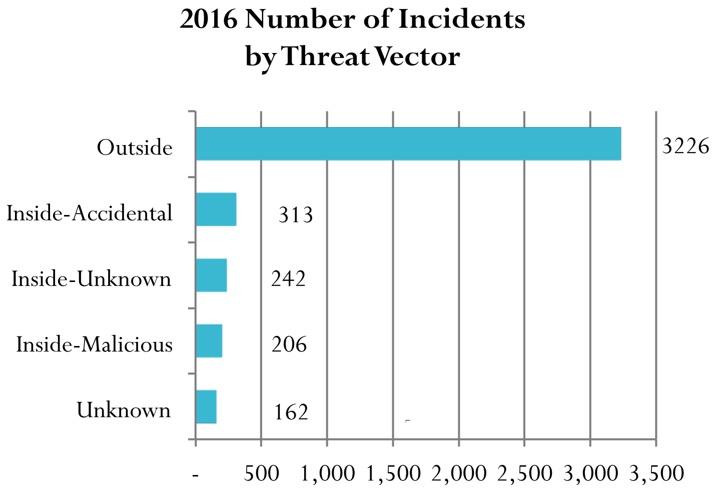
Hacking continues to dominate as the leading breach type, with SQL injection a predominant method utilized.

Stolen laptops, once a leading cause of data compromise, accounted for only 67 (1.6%) of incidents in 2016.



Misconfigured databases and other inadvertent web based disclosures exposed over 253 million records in 2016.

2016 Data Breach Analysis by Threat Vector



Only 18.3% of incidents were the result of insider activity

2016 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	3,819,637,019
Inside-Accidental	87,888,518
Inside-Malicious	2,295,432
Inside-Unknown	121,425,860
Unknown	250,548,979
Total	**4,281,795,808**

56.3% of incidents originating from malicious insiders had no confirmed record count, while 39.3% of incidents originating from insider accidents had no confirmed count

Top 10 Breaches – Data Types and Severity Scores[2]

Breach Type	Records Exposed	Percentage of Total Exposed	Data Type[3]	Severity Score
Hack	1,000,000,000	23.35%	DOB/EMA/MISC/NAA/NUM/PWD	10
Hack	500,000,000	11.68%	DOB/EMA/MISC/NAA/NUM/PWD	10
Hack	412,214,295	9.63%	EMA/IP/MISC/PWD/USR	10
Hack	360,213,024	8.41%	EMA/PWD/USR	10
Hack	203,419,083	4.75%	ADD/DOB/FIN/MISC/NAA/NUM	10
Hack	154,000,000	3.60%	ADD/EMA/MISC/NAA/NUM	10
Hack	127,343,437	2.97%	DOB/EMA/NAA/PWD/USR	9.70
Hack	98,167,935	2.29%	EMA/MISC/PWD/USR	9.59
Web	93,424,710	2.18%	ADD/DOB/MISC/NAA	9.82
Hack	93,338,602	2.18%	EMA/NAA/NUM/PWD	10
The top 10 breaches exposed 3,042,121,086 records, or 71% of the total records exposed in 2016				

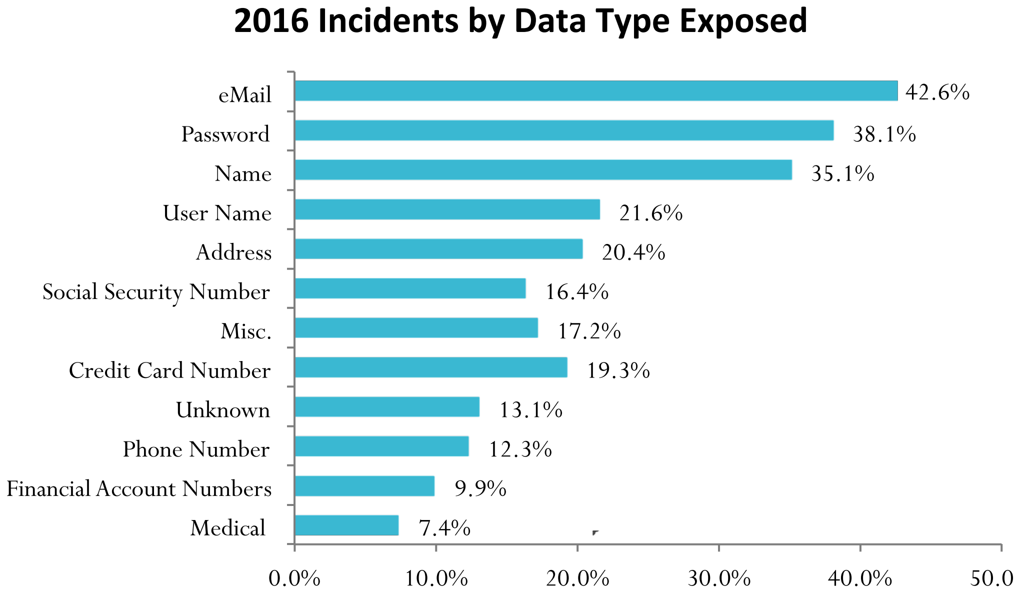
[2] See page 13 for additional detail on these incidents.
[3] See page 17 for a description of abbreviations.

2016 Analysis by Data Family

	Percentage of Total Breaches	Percentage of Total Exposed Records	Percentage of Total Breaches	Percentage of Total Exposed Records
Data Family	**2015**	**2015**	**2016**	**2016**
Electronic	89.5%	99.6%	90.9%	99.9%
Physical	7.1%	<0.15%	6%	<.1%
Unknown	3.0%	< 0.15%	2.7%	<.1%

While the vast majority of breaches impact electronic data, regulators in both the United States and the U.K. have demonstrated an interest in pursuing actions against organizations for mishandling documents. On August 10th, 2016, the UK's Information Commission's Office fined the Hampshire County Council £100,00 for leaving confidential records behind in a vacated building. In the U.S., on March 1st, Health and Human Services Office of Civil Rights fined Lincare Holdings a total of $239,800 after a manager moved out of her house, leaving behind confidential medical files containing protected health information.

2016 Analysis by Data Type – Percentage of Breaches



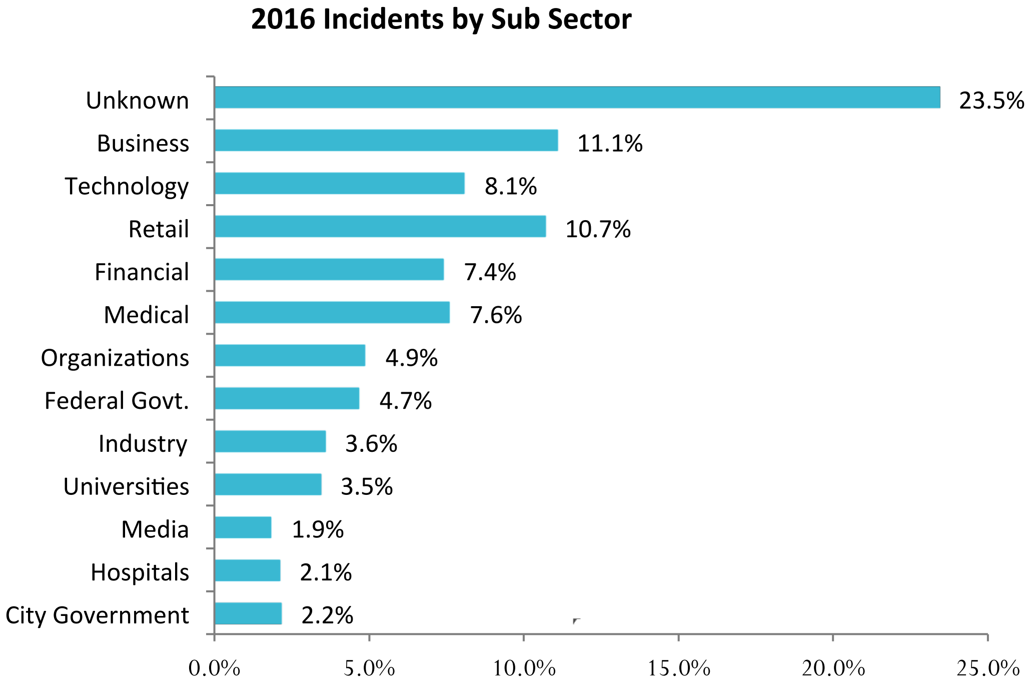
42.6% of data breaches exposed eMail Addresses. Passwords and eMail Addresses remain a prize target.

2016 Percentage of Breaches Exposing Data Types vs. 2015

Data Type	2015	2016
Password	49.9%	38.1%
eMail	45.5%	42.6%
User Name	37.7%	21.6%
Name	29.4%	35.1%

Although the number of incidents impacting access credentials declined in 2016, the number of passwords impacted skyrocketed, from 151 million in 2015 to over 3.2 billion in 2016

2016 Analysis by Industry Sub Business Type



- Unknown[4] and Business sub types remain in the top two spots with Retail coming in at number three in number of breaches.
- Looking ahead to 2017, Industry sub types will be updated to align with NAICS Economic Sectors

2016 Analysis of Records per Breach

Exposed Records	Number of Breaches	Percent of Total
Unknown	1606	38.7%
1 to 100	769	18.5%
101 to 1,000	777	18.7%
1,001 to 10,000	546	13.2%
10,001 to 100,000	230	5.5%
100,001 to 500,000	101	2.4%
500,001 to 999,999	24	0.6%
1 M to 10 M	58	1.4%
> 10 M	36	0.9%

In 2016, the number of breaches exposing more than 10 million records increased 125% over 2015.

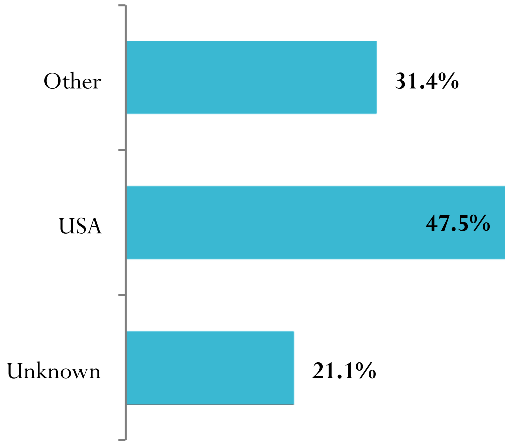
[4] In certain situations, the party responsible for the breach cannot be identified with certainty. When this happens, the marker “Unknown Organization” is used and the associated business type and sub-type are also “Unknown”.

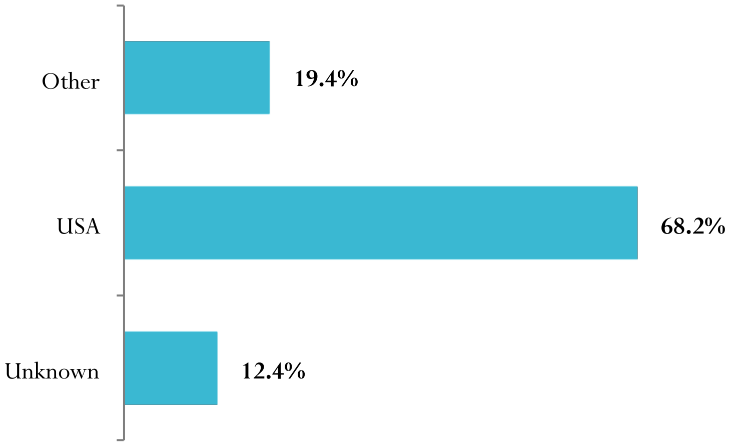
2016 - Breach Types/Records Exposed – Top 5

Breach Category	Number of Breaches	Number of Records Exposed	Average Records per Breach	Percent of Total Records Exposed
Hacking	2213	3,915,227,460	1,769,195	91.44%
Web	167	253,355,867	1,517,101	5.92%
Unknown	120	50,901,084	424,176	1.19%
Virus	185	15,794,286	85,375	0.37%
All Other	1464	46,517,116	31,774	1.09%

Breaches taking place at FriendFinder Networks, Myspace and Yahoo - all classified as hacking incidents - accounted for more than 2.2 billion records compromised.

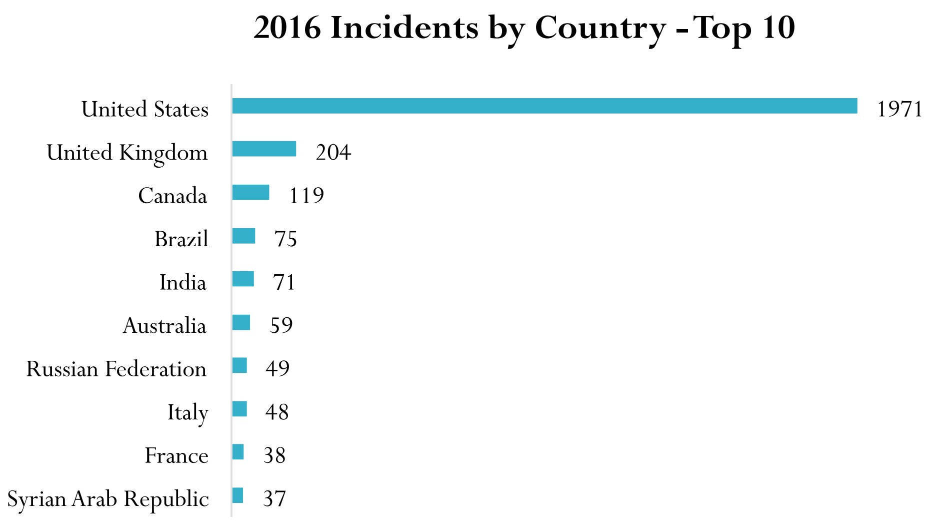
2016 Analysis by Country


2016 Incidents by Location


2016 Records Exposed by Location

- There were 102 countries reporting at least one data breach in 2016.
- The Top 10 countries accounted for 64.4% of the breaches.
- Disclosed breach events in Brazil jumped 92.3% in 2016 compared to 2015, with 72% of the incidents taking place prior to the summer Olympics.

2016 Analysis by Country – Top 10



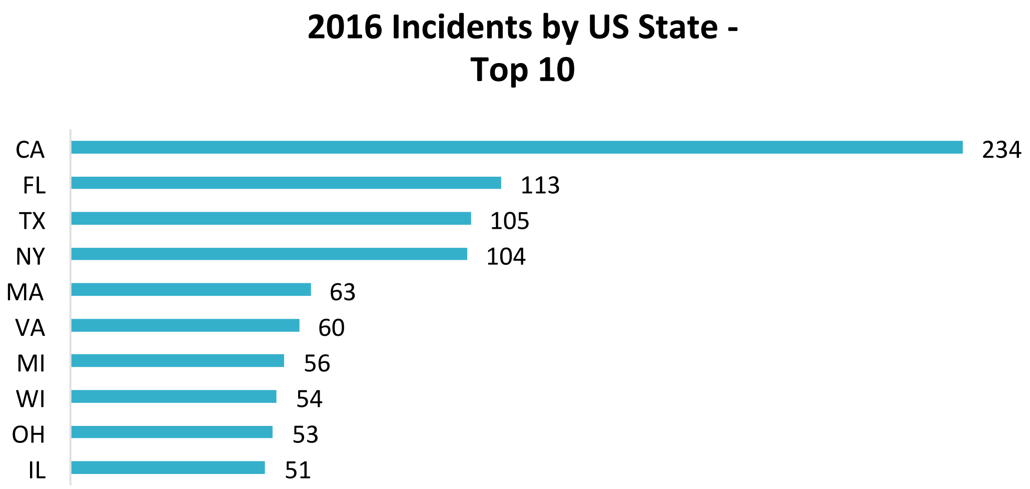
USA and UK account for 52.4% of breaches.

2016 Exposed Records by Country – Top 10

Exposed Records Ranking	Number of Breaches	Country	Total Exposed Records	Average Records per Breach	Median Number of Records	Percentage of Exposed Records
1	1971	United States	2,919,677,558	1,956,888	1,224	68.19%
2	49	Russian Federation	259,738,619	5,300,788	533	6.07%
3	9	Mexico	93,427,863	10,380,874	554	2.18%
4	38	France	86,337,303	2,272,034	359	2.02%
5	11	Philippines	75,306,058	6,846,005	37	1.76%
6	119	Canada	73,083,967	614,151	86	1.71%
7	19	China	54,885,226	2,888,696	5,116	1.28%
8	13	Japan	43,017,377	3,309,029	149,006	1.00%
9	19	Iran	35,333,504	1,859,658	13	0.83%
10	7	Taiwan	30,033,018	4,290,431	16,483	0.70%

Ten breaches in the United States accounted for roughly 2.7 billion of the 2.9 billion records exposed. The median number of records lost – derived from breaches with a confirmed record count - bolsters the findings in the Analysis of Records Per Breach table with 50.4% of breaches exposing between 1 and 10,000 records and 37.2% of breaches expose between 1 and 1,000 records.

2016 Analysis of US State Rankings



The top 10 states represent 52.1% of US incidents.

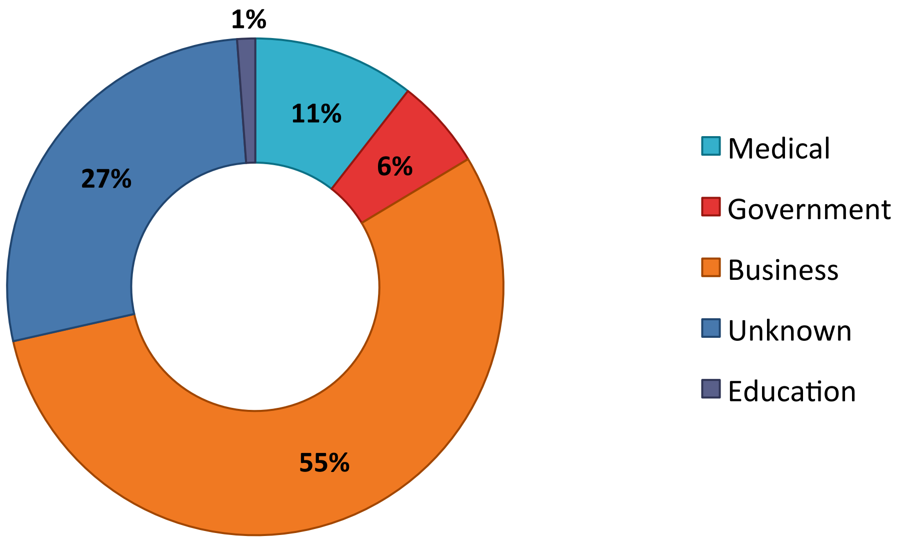
- Indiana and Pennsylvania just missed making the Top Ten list, with 49 and 46 breaches respectively.

Exposed Records Ranking	US State	Total Exposed Records	Number of Breaches	Exposed Records/Breach	Percentage of USA Exposed Records
1	CA	2,349,731,591	234	10,041,588	80.48%
2	NY	142,802,652	104	1,373,102	4.89%
3	TX	60,374,939	105	574,999	2.07%
4	VA	49,966,475	60	832,774	1.71%
5	DE	33,407,985	4	8,351,996	1.14%
6	LA	10,265,379	12	855,448	0.35%
7	NC	8,287,075	37	223,975	0.28%
8	WA	6,438,745	39	165,096	0.22%
9	AZ	4,896,525	41	119,427	0.17%
10	OH	4,398,316	53	82,987	0.15%

- California alone accounted for 54.9% of the total records compromised in 2016.
- Top Ten states represent 91.47% of records exposed in the USA.

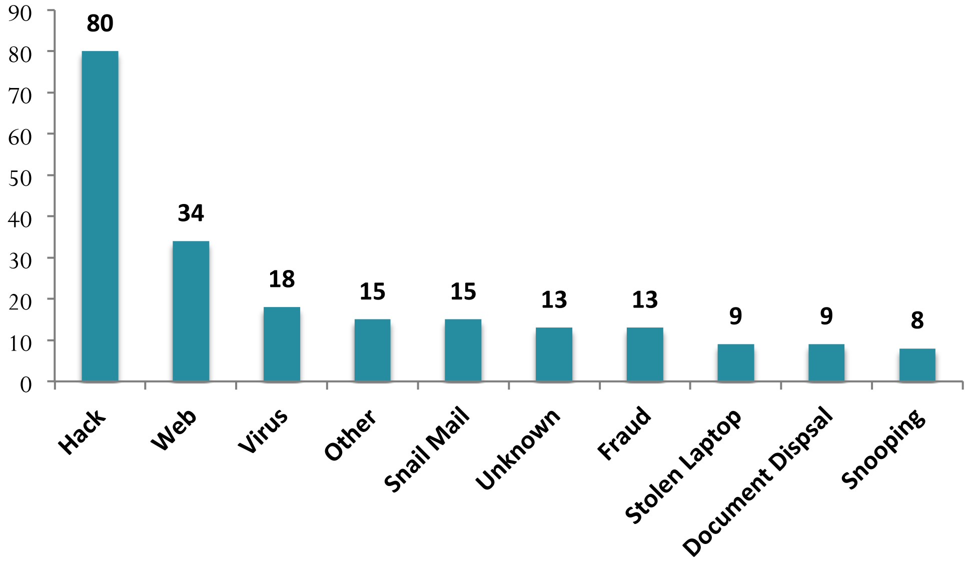
2016 Breaches Involving Third Parties

2016 Third Party Breaches by Business Type



- Business organizations account for more than half of the 3rd Party breaches
- Hacking is the dominate breach type impacting 3rd Parties

2016 Third Party Breaches by Breach Type - Top 10



2016 Repeat Offenders

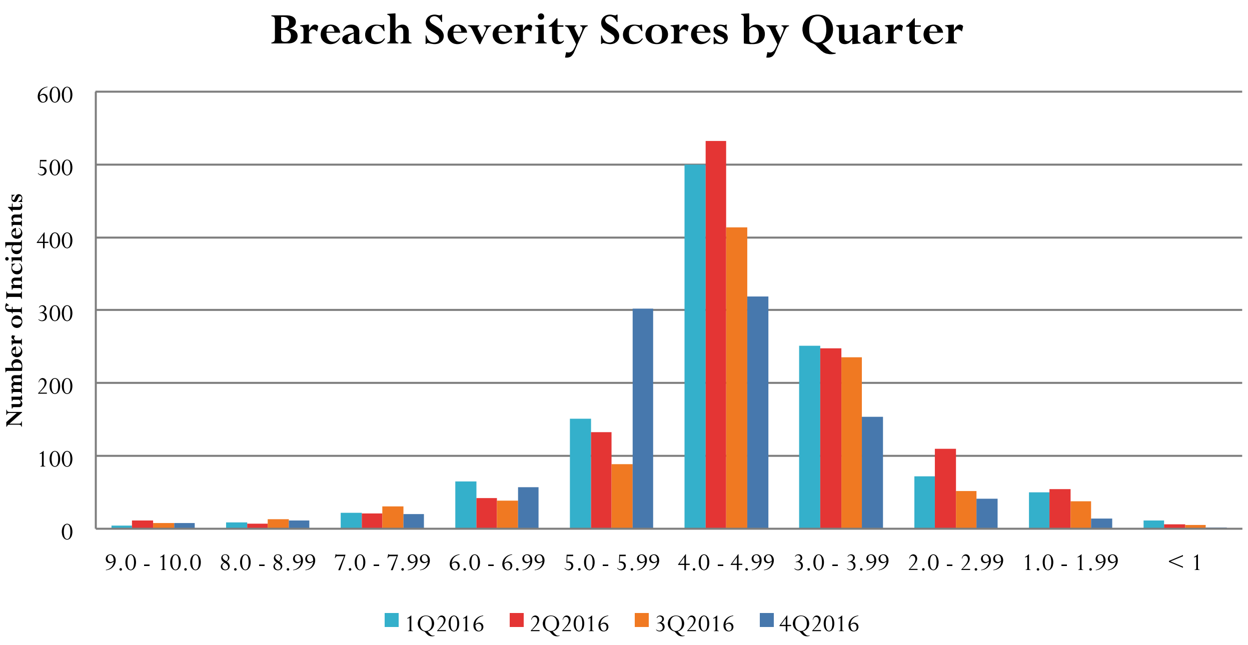
One hundred twenty three (123) organizations reported multiple data breaches in 2016

123 organizations reported two or more breaches during the year, with 37% of those organizations reporting three or more breaches. It is always challenging to draw definitive conclusions as to why some organizations experience multiple data loss events in a relatively short period of time. However, events in 2016 made it clear that once an investigation is underway, organizations should be prepared for the possibility of additional breach discoveries. Events at Yahoo and Mossack Fonseca serve as useful examples of this. After the damaging leak of millions of documents containing details of clients' sensitive financial affairs, Mossack Fonseca launched into an extensive investigation of the breach. Within two months, the investigation had identified a second, unrelated incident of malicious insider activity. Events at Yahoo unfolded in much the same way. It seemed unlikely the September disclosure that 500 million user details had been compromised would ultimately lead to a much larger breach. Unfortunately for Yahoo, the breach investigation uncovered the largest incident ever reported, impacting over 1 billion user accounts as well as indicating proprietary code had been compromised and used in the attack.

2016 – Breach Severity 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. 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, we have implemented a system indicating the relative severity of each breach in our database. Our Severity Scores range from .1 to 10.0.

2016 – Breach Severity Scores



2016 – Breach Severity Scores – Top 10

Organization	Top 10 Summary	Score
Yahoo	(Hacking) Over 1,000,000,000 customer names, email addresses, phone numbers, dates of birth, and hashed passwords, as well as an unknown number of security questions and answers stolen by hackers using stolen proprietary code	10
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
FriendFinder Networks, Inc.	(Hacking) 412,214,295 member email addresses, usernames, and encrypted passwords, as well as roughly 30,000,000 member IP addresses and membership statuses, an unknown amount of source code, and an unknown number of employee names, home IP addresses, and VPN server access keys stolen by hackers exploiting a Local File Inclusion vulnerability	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) 203,419,083 customer names, addresses, genders, phone numbers, dates of birth, ethnicities, religions, primary languages, marital statuses, income details, credit ratings, and other assorted personal and financial details stolen and put of for sale on the dark web by hackers incorrectly labeling it as coming from Experian	10
Unknown Organization / L2, Inc.	(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 / VK	(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
Republic of the Philippines Commission on Elections (COMELEC)	(Hacking) 75M voter names, dates of birth, email address, genders, addresses, precinct numbers, disabilities, identification numbers, and registration record numbers, as well as 1.3M passport numbers with expiry dates, 15.8M fingerprints, and the database schema, leaked on the Internet	9.87
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

Top 20 Breaches All Time (Exposed Records Count)

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
Highest All Time 12/14/2016	While investigating the #2 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 2 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 3 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	United States
Number 4 5/27/2016	Hack exposes user account records containing SHA1 encrypted passwords, email addresses.	360 Million	MySpace	Business	United States
Number 5 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 6 12/3/2016	Hackers offer for sale a database containing names, addresses, genders, phone numbers, dates of birth, ethnicities, religions, primary languages, marital statuses, income details, credit ratings, and other assorted personal and financial details.	203 Million	Organization's Name has not been reported	Unknown	Unknown
Number 7 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 8 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

Breach Reported Date	Summary	Records Exposed	Organization’s Name	Industry-Sector	Breach Location
Number 9 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 10 6/23/2016	Hack exposes USA voter information.	154 Million	Organization’s Name has not been reported	Unknown	United States
Number 11 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 12 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 13 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 14 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 15 1/20/2009	Hack/Malicious Software exposes credit cards at processor	130 Million	Heartland Payment Systems	Business - Finance	United States
Number 16 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 17 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 18 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 19 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 20 1/20/2014	Fraud exposes credit card numbers, social security numbers, and phone numbers.	104 Million	Korea Credit Bureau	Business - Financial	South Korea

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

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 Ratings and Vulnerability Intelligence. Our products, Cyber Risk Analytics (CRA) and VulnDB, provide organizations 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 threat intelligence about organizations that have had a data breach or leaked credentials. 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.