RiskBased SECURITY

Not Just Security, the Right Security.

CYBER RISK ANALYTICS

RPS®
Risk Placement Services, Inc.

Data Breach QuickView Report

First Nine Months of 2018 - Data Breach Trends

Risk Based Security, Inc.

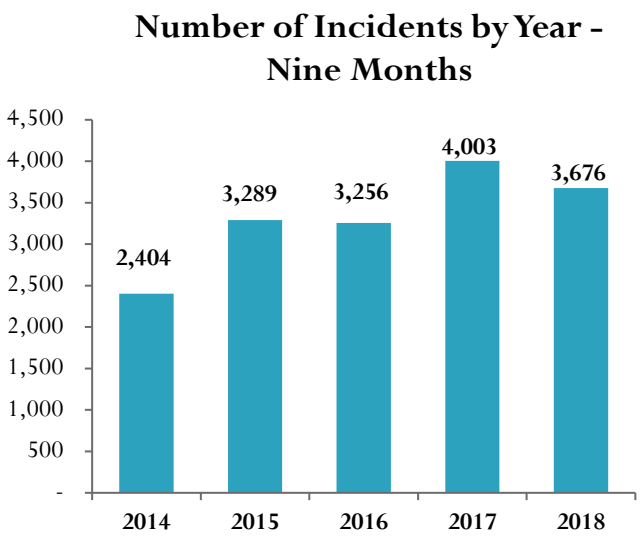
Issued on October 29, 2018
Data as of September 30, 2018

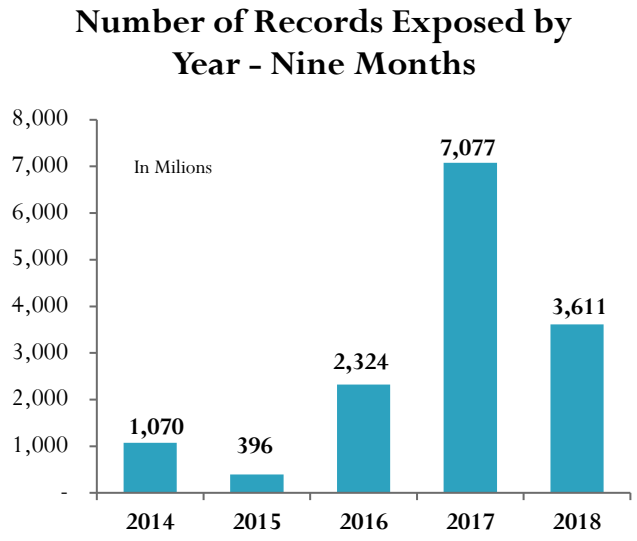
2018 is on pace to be another significant year for breach activity but will most likely fall below the high-water mark set in 2017.

- **3,676** breaches have been reported through September 30, exposing approximately **3.6 billion** records.
- Compared to the same point in 2017, the number of reported breaches is *down 8%* and the number of exposed records is *down approximately 49% from 7 billion*.
- The Business sector accounted for 38% of reported breaches, followed by Government (8.2%), Medical (7.8%) and Education (3.9%). Nearly 43% of breached organizations could not be definitively classified.
- Seven breaches exposed **100 million** or more records with the 10 largest breaches accounting for **84.5%** of the records exposed year to date.
- The Business sector accounted for 63.6% of the records exposed followed by Unclassified at 34.8% and Government at 1.4%. The pattern from 2017 and the first 2 quarters of 2018 remains the same, with the Medical and Education sectors combined accounting for less than 1% of the total records exposed year to date.
- **Fraud** remains in the top spot for the breach type compromising the most records, accounting for **35.7% of exposed records**, while **Hacking** takes the lead in number of incidents, accounting for **57.1% of reported breaches**.
- 2018 continues to be marked by a lack of transparency, with 34.5% of breached organizations unwilling or unable to disclose the number of records exposed.

Table of Contents

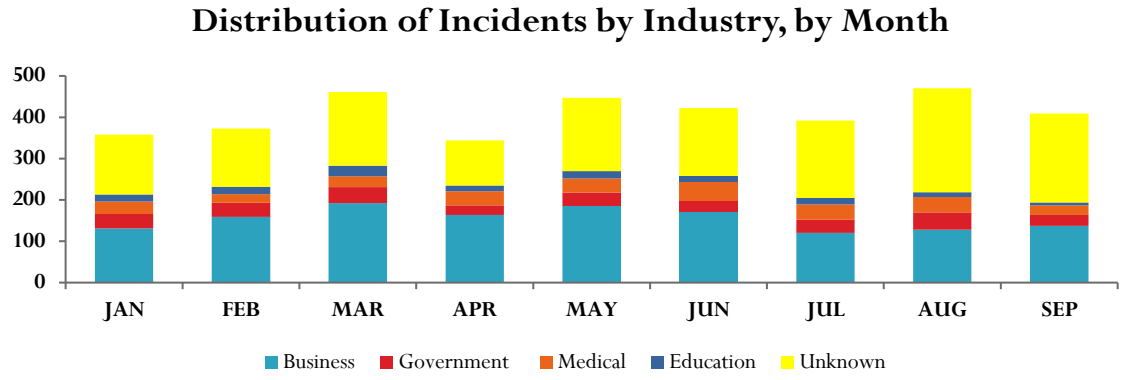
First Nine Months of 2018 Compared to Same Point in Previous Four Years

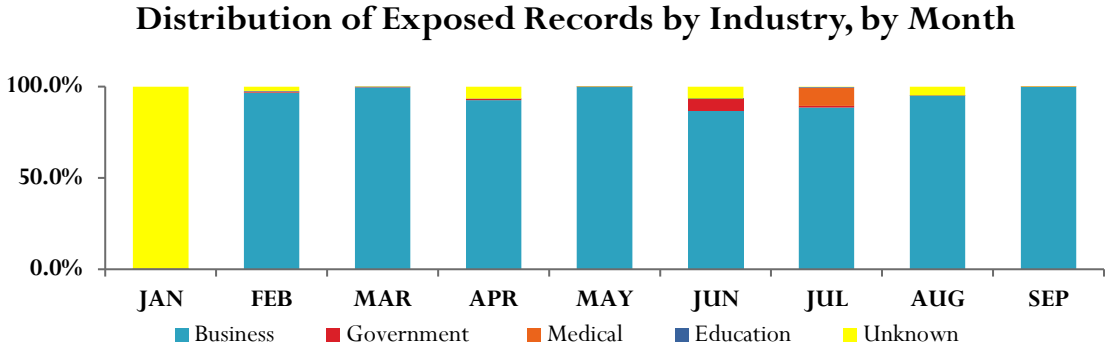




Is this good news? The number of reported breaches shows some improvement compared to 2017 and the number of records exposed dropped dramatically. But the decline from 2017 is only part of the story. 2018 is on track to have the second most reported breaches and the third most records exposed since 2005. Despite the decrease from 2017, the overall trend continues to be more breaches and more "mega breaches" impacting hundreds of millions of records at once.

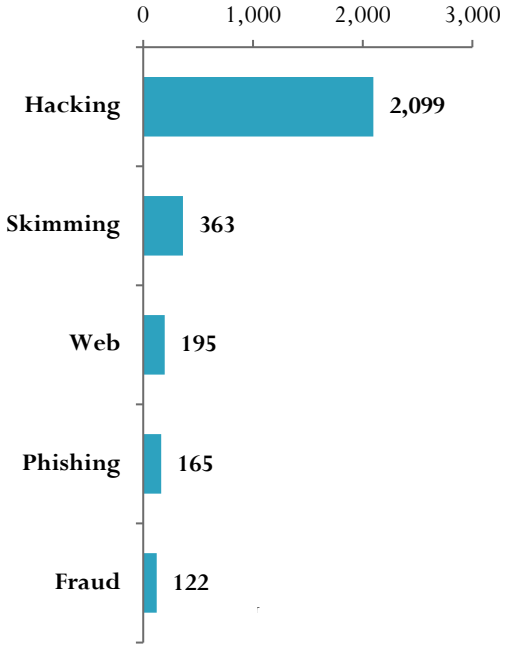
First Nine Months of 2018 Breaches by Industry, by Month





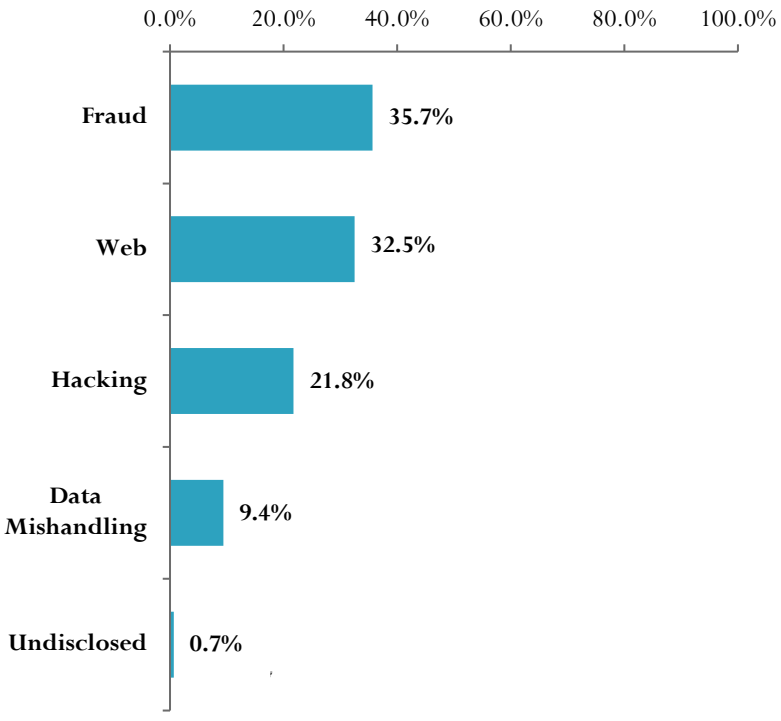
First Nine Months of 2018 Breaches by Type and Record Exposed

Top 5 Breach Types



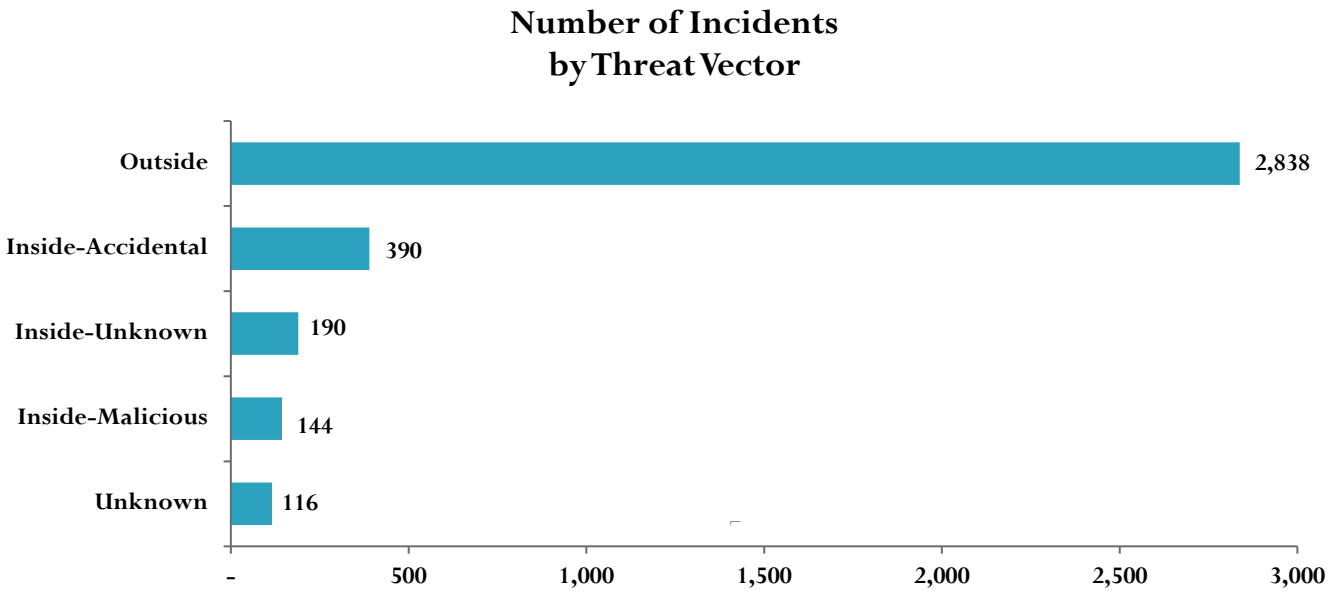
Despite the lack of headlines, skimming continues to be an issue at ATMs and for gas station operators. Approximately 53% of the skimming events were discovered at ATMs and 42% found on gas pumps.

Records Exposed by Breach Type



Programming errors and misconfigured services continue to be a major source of data exposure, with 17 such breaches compromising 1 million or records.

First Nine Months of 2018 Breaches by Threat Vector



Threat Vector	Records Exposed
Inside-Accidental	1,402,297,210
Unknown	1,248,810,176
Outside	916,953,592
Inside-Unknown	41,761,225
Inside-Malicious	1,859,916
Total	**2,692,703,003**

The real insider risk comes from the amount and type of data exposed in an insider event. Of the 51 breaches impacting intellectual property, 61% originated from inside the organization.

First Nine Months of 2018 Distribution of Breaches by Discovery Method

	Internal Discovery - Incidents	Internal Discovery - Records	External Discovery - Incidents	External Discovery - Records	Undisclosed Discovery - Incidents	Undisclosed Discovery - Records
Q1	181	2,971,012	689	1,240,717,817	322	241,354,523
Q2	148	367,110,447	664	778,978,590	401	71,748,079
Q3	154	56,885,775	818	789,404,566	299	62,511,310
Total	**483**	**426,967,234**	**2,171**	**2,809,100,973**	**1,022**	**375,613,912**

First Nine Months of 2018 Time Interval Between Discovery and Reporting

Average Number of Days Between Breach Discovery and Reporting	Q1 2018	Q1 2017	Q1 2016	Q1 2015	Q1 2014
	37.9	42.7	68.9	82.6	75.5
	Q2 2018	Q2 2017	Q2 2016	Q2 2015	Q2 2014
	55	47.8	59.2	72.5	57
	Q3 2018	Q3 2017	Q3 2016	Q3 2015	Q3 2014
	49.7	50.6	65.7	66.3	117
Average For The Year	2018	2017	2016	2015	2014
	47.5	47	64.6	73.8	83.2

Overall the gap has been closing between when a breach is first discovered by the responsible organization to when the breach is first publicly disclosed. However, looking at the averages for each of the five years, 2018 shows no improvement compared to 2017 despite mounting regulatory pressure to speed up public disclosure.

First Nine Months of 2018 10 Largest Breaches by Records Exposed[1]

Breach Type	Records Exposed	Percentage of Total Exposed	Data Type[2]	Severity Score
Fraud	1,190,000,000	33%	ADD/EMA/MISC/NAA/NUM/SSN	10
Web	445,000,000	12%	EMA/MISC/NAA	9.4
Web	340,000,000	9%	ADD/EMA/MISC/NAA/NUM	10
Other (Data Mishandling)	336,000,000	9%	PWD/USR	9.3
Hack	240,000,000	7%	ADD/EMA/FIN/MISC/NUM/PWD	10
Hack	150,000,000	4%	EMA/PWD/USR	10
Web	120,000,000	3%	DOB/MISC/NAA	9.6
Hack	92,283,889	3%	EMA/PWD	9.5
Fraud	87,000,000	2%	MISC/NAA	10
Web	50,553,664	1%	DOB/EMA/MISC/PWD/USR	8.7

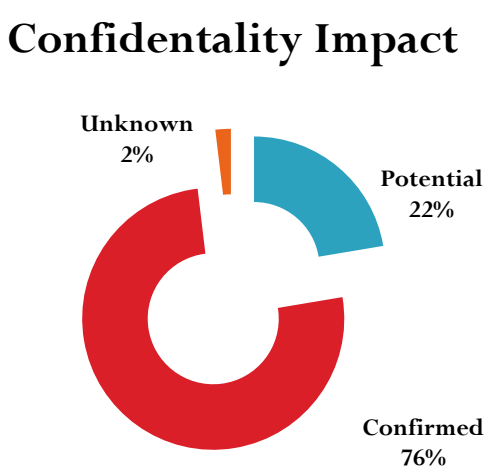
The 10 largest breaches from the first nine months of the year exposed 3,050,837,553 records, or 84.5% of the total records exposed through the end of September.

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

First Nine Months of 2018 Analysis by Data Family

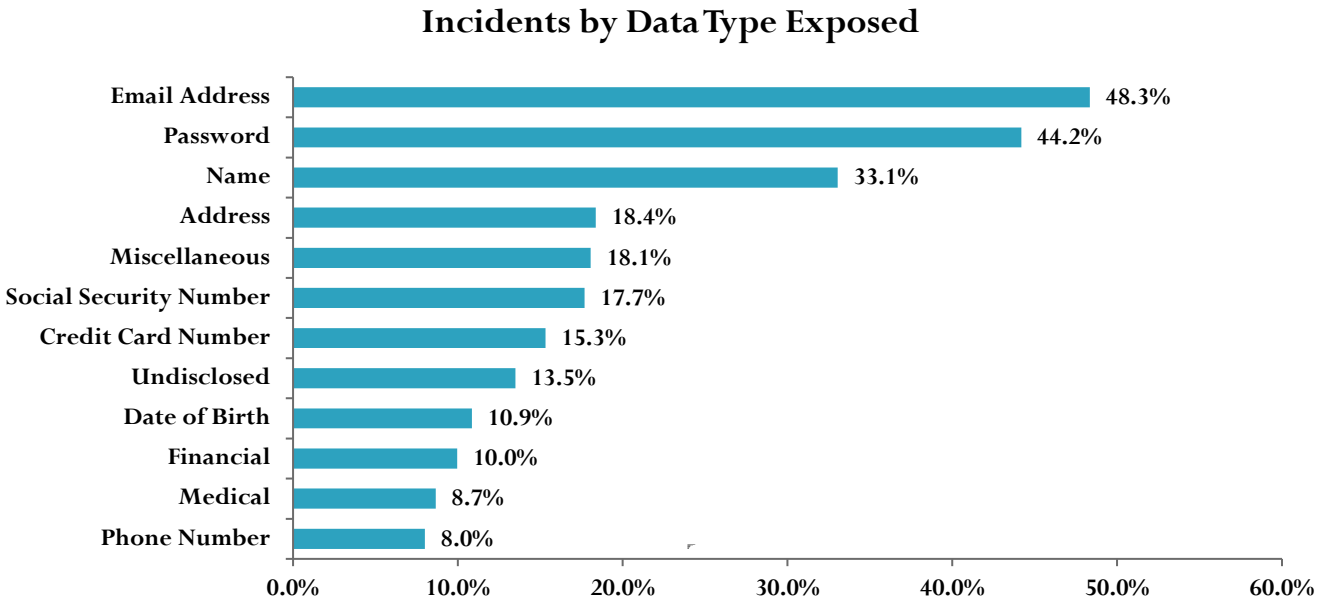
	Percentage of Total Breaches	Percentage of Total Exposed Records	Percentage of Total Breaches	Percentage of Total Exposed Records
Data Family	**2017**	**2017**	**2018**	**2018**
Electronic	93.24%	99.98%	93.06%	99.97%
Physical	4.53%	<1%	4.76%	<1%
Unknown	2.23%	<1%	2.18%	<1%

First Nine Months of 2018 Impact on Data Confidentiality



The percentage of breaches with confirmed unauthorized access to sensitive data has been slowly rising from 68% in Q1 but remains below year end 2017's 83%.

First Nine Months of 2018 Breach Analysis by Data Type



Percentage of Breaches Exposing Top Four Data Types – Nine Months 2018 vs. Prior Years			
Data Type	**9 Months 2018**	**9 Months 2017**	**9 Months 2016**
Email Address	48.2%	43.4%	44.1%
Password	44.2%	38.9%	40.6%
Name	33.1%	33.7%	35.5%
Physical Address	18.4%	23.8%	21.1%

First Nine Months of 2018 Analysis of Records Compromised Per Breach

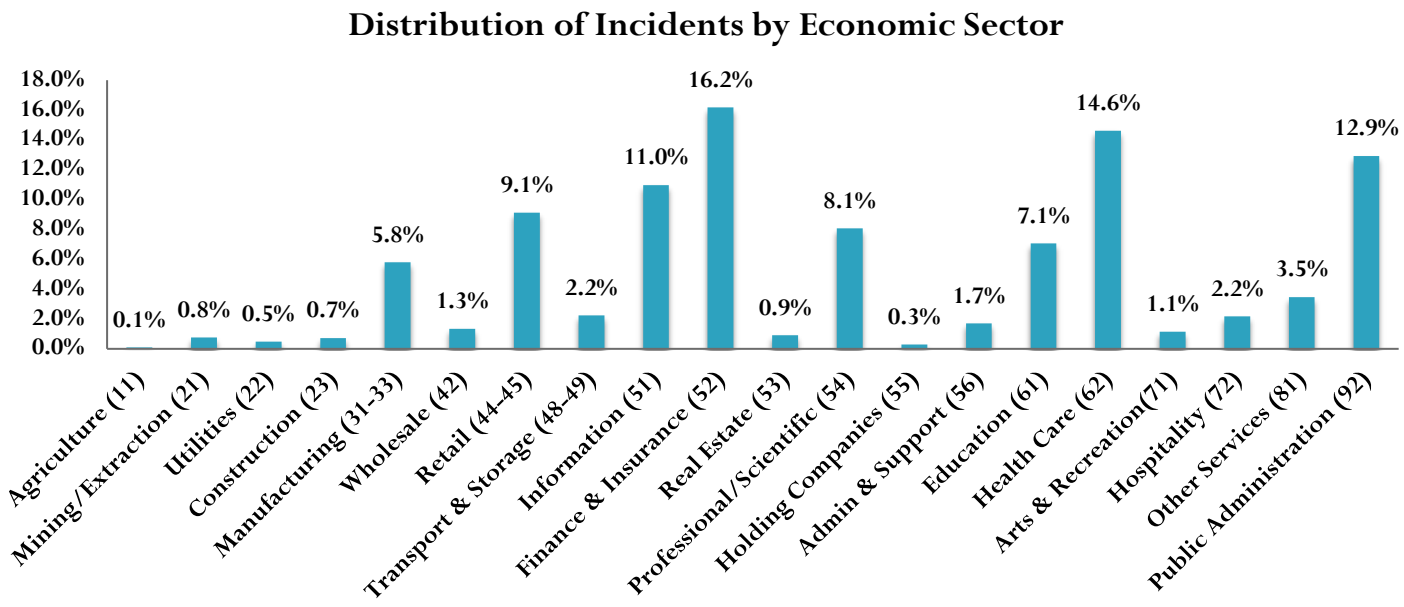
Exposed Records	Number of Breaches	Percent of Total
Unknown/Undisclosed	1,265	34.4%
1 to 100	1,060	28.8%
101 to 1,000	718	19.5%
1,001 to 10,000	323	8.8%
10,001 to 100,000	182	5.0%
100,001 to 500,000	54	1.5%
500,001 to 999,999	18	0.5%
1 M to 10 M	29	0.8%
> 10 M	27	0.7%

The number of breaches impacting between 1 and 10,000 records has been around the 55% mark since 2016. In 2015, it was 67% and in 2014 it was 71%. The shift in 2016 coincides with an increase in the percentage of Unknown.

First Nine Months of 2018 Records Exposed For Top 5 Breach Types

Breach Category	Number of Breaches	Number of Records Exposed	Average Records per Breach	Percent of Total Records Exposed
Hacking	2,099	780,262,761	371,731	21.60%
Skimming	363	3,629	10	-
Web	195	1,165,546,624	5,977,162	32.27%
Phishing	165	1,154,974	7,000	0.03%
Fraud	122	1,278,549,029	10,479,910	35.40%

First Nine Months of 2018 Analysis of Incidents by NAICS Economic Sector



*Where known. Organizations that could not be definitively classified have been removed from results

First Nine Months of 2018 Top 3 Business Groups For Top 3 Economic Sectors

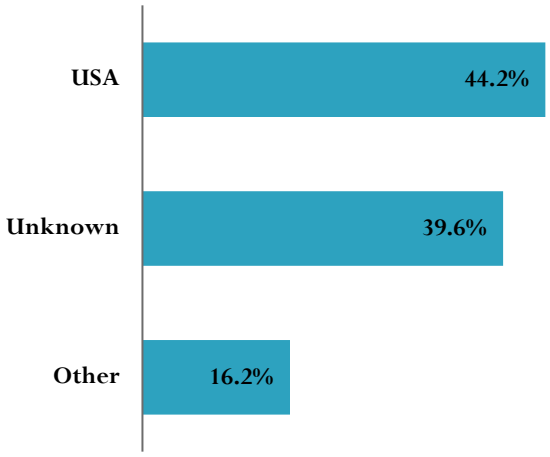
Economic Sector	Business Group	Percentage of Breaches Within Economic Sector
Finance & Insurance* (52)	Financial	80.6%
	Insurance	19.4%
Health Care (62)	Practitioners Offices	37%
	Hospitals	36%
	Medical Facilities	18.5%
Public Administration (92)	Cities	22.8%
	Federal Government	26.5%
	State	19.5%

*Note, the Finance & Insurance sector is made of two Business Groups. As such, the entire sector is represented.

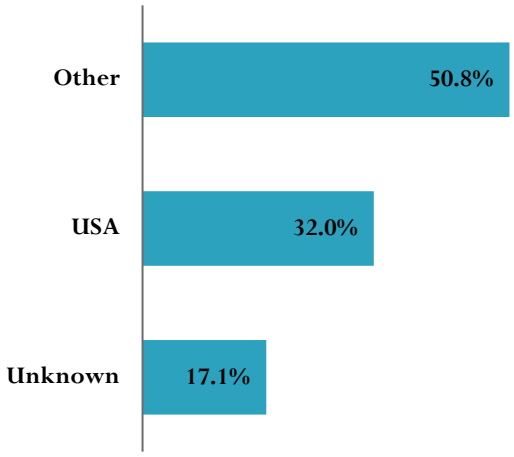
35% of the breaches in the Financial Business Group are due to skimming at ATM machines.

First Nine Months of 2018 Analysis of Breaches by Location

Incidents by Location



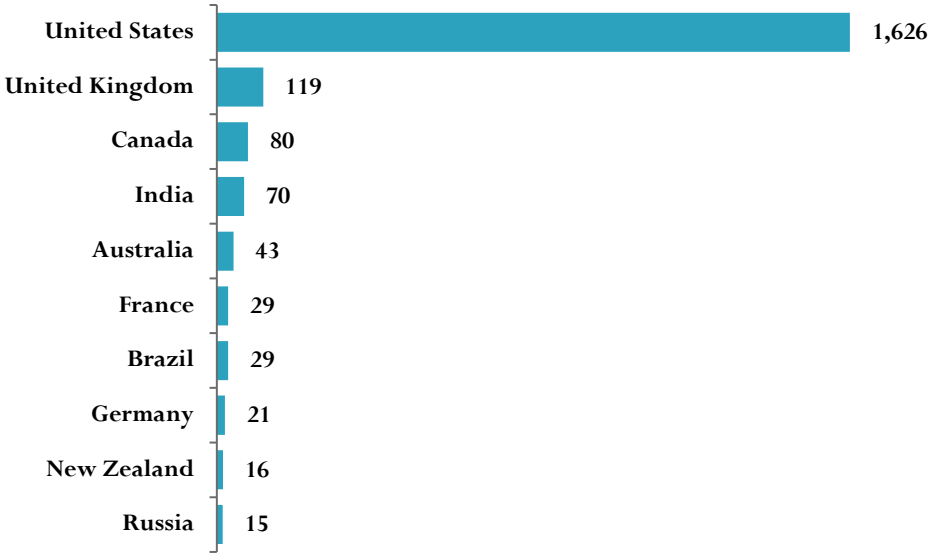
Records Exposed by Location



While nearly 40% of the breaches cannot be tied to a location, these account for only 17% of the total number of records exposed. These breaches are often data leaks from unknown organizations or breaches at nebulous website operators.

First Nine Months of 2018 Breaches by Country

Incidents By Country - Top 10

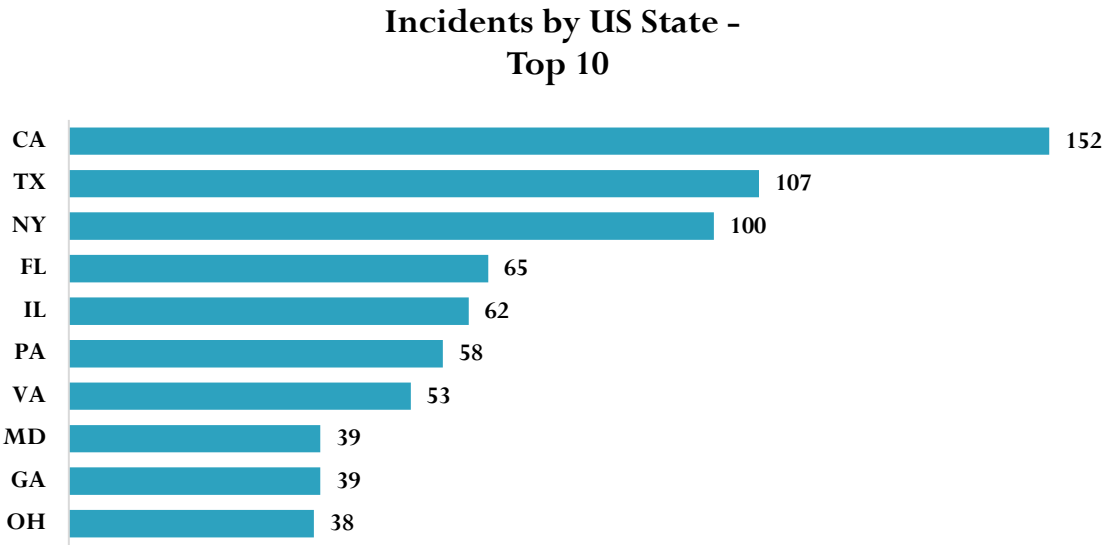


First Nine Months of 2018 Exposed Records by Country

Ranking	Number of Breaches	Country	Total Exposed Records	Average Records per Breach	Median Records Exposed	Percentage of Exposed Records
1	70	India	1,267,975,805	28,117,056	20,000	35.11%
2	1626	United States	1,157,019,617	959,281	1,541	32.04%
3	9	China	302,493,665	8,007,125	5,950,000	8.38%
4	21	Germany	121,797,967	24,853,850	516	3.37%
5	2	Vietnam	24,853,852	834,833	N/A	0.69%
6	43	Australia	20,120,586	6,173,825	651	0.56%
7	119	United Kingdom	18,970,305	6,027,394	258	0.53%
8	3	Ukraine	18,521,476	3,500,141	9,260,738	0.51%
9	6	Philippines	18,082,408	261,491	213	0.50%
10	5	Egypt	14,000,564	1,705,714	281	0.39%
Total	1,904		2,963,836,245	1,556,637		82%

While the top ten countries accounted for 82% of records exposed this period, the same countries accounted for roughly half, or 51.8%, of reported incidents. Setting aside large breaches in China and the Ukraine, the median number of records exposed remains relatively low for all countries except India, indicating a pattern of larger breaches taking place in that country. For comparison, in the first 9 months of 2018, 7% of breaches reported in India impacted 1 million or more records while only 1% of breaches reported in the United States impacted 1 million or more records.

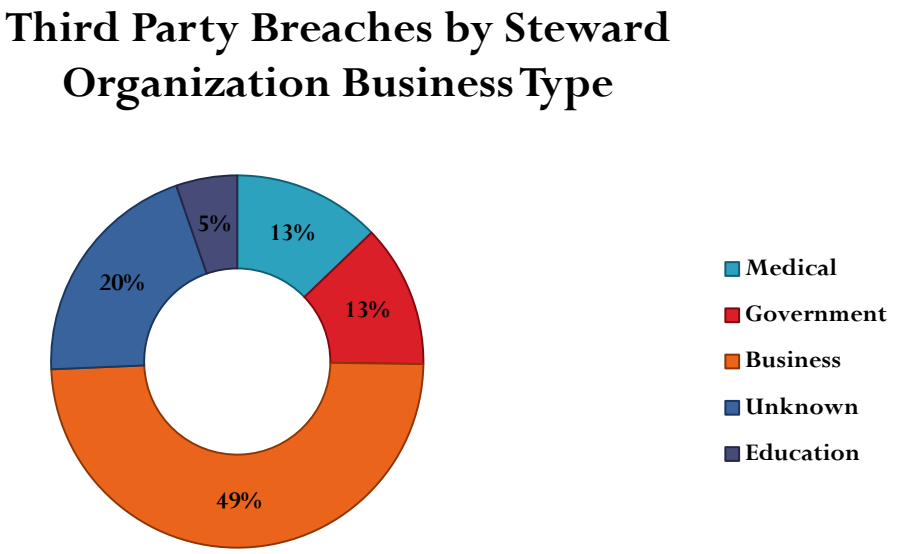
First Nine Months of 2018 Distribution of Breach Location By State



First Nine Months of 2018 Analysis of US State Rankings, Exposed Records

Exposed Records Ranking	US State	Total Exposed Records	Number of Breaches	Exposed Records/Breach	Percentage of Records Exposed in USA
1	CA	547,771,268	152	3,603,758	47.34%
2	FL	341,569,901	65	5,254,922	29.52%
3	MD	150,591,747	39	3,861,327	13.02%
4	WA	48,013,062	29	1,655,623	4.15%
5	NY	21,626,031	100	216,260.31	1.87%
6	IN	14,055,942	21	669,330.57	1.21%
7	IL	2,450,127	62	39,518.18	0.21%
8	MO	1,620,875	33	49,117	0.14%
9	IA	1,500,334	23	65,232	0.13%
10	MA	1,130,315	38	29,745	0.10%

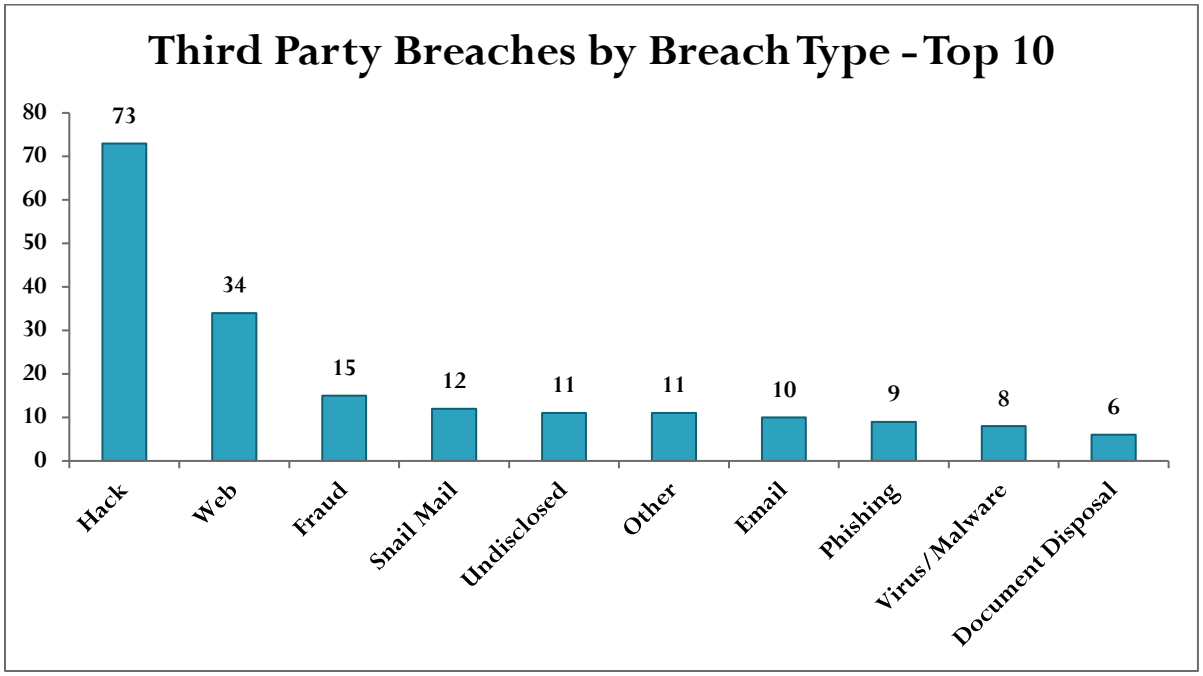
First Nine Months of 2018 Breaches Impacting Third Party Organizations



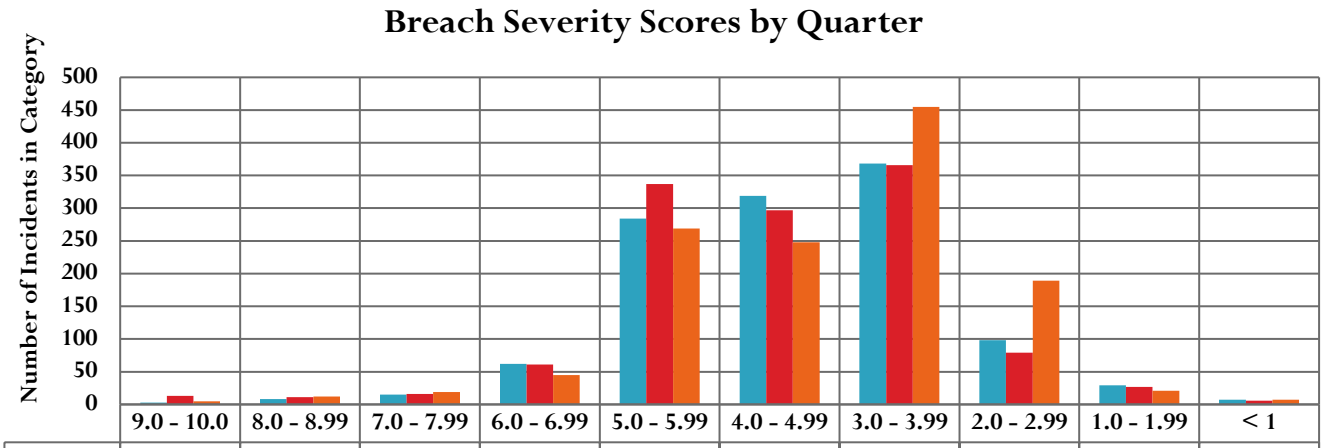
6.2% percent of the breaches reported in the first nine months 2018 directly impacted a third party organization. This is relatively unchanged from the mid-year point.

Notable third party breaches reported in the first nine months of 2018 include:

- Typeform: Undisclosed Records Exposed
  Customer data from as many as 233,000 accounts exposed
- FastHealth Corp: 657,529 Records Exposed
  Customer data from at least 8 organizations exposed
- PageUp: Undisclosed Records Exposed
  Customer data from at least 10 organizations exposed
- Nuance Communications: 45,000 Records Exposed
  Customer data from at least 6 organizations exposed
- 24[7].ai: 938,449 Records Exposed
  Customer data from at least 4 organizations exposed
- Orbitz, LLC: 880,000 Records Exposed
  Customer data from at least 7 organizations exposed



First Nine Months of 2018 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
1Q2018	3	8	15	62	284	319	368	98	29	7
2Q2018	13	11	16	61	337	297	366	79	27	6
3Q2018	5	12	19	45	269	248	455	189	21	7

First Nine Months of 2018 Top 10 Breaches By Severity Score

Score	Reported	Organization (Third Party)	Top 10 Summary
10	Q1	Facebook	(Fraud) 87,000,000 user profile details obtained by a third party application without clear authorization for redistribution and in violation of platform guidelines
10	Q3	Facebook	(Hacking) 30,000,000 user details accessed by hackers exploiting flaw in the "View As" feature
10	Q1	Undisclosed (UIDAI)	(Fraud) 1,190,000,000 names, Aadhaar numbers, addresses, phone numbers, email addresses, postal codes, and photographs of Indian citizens made available to unauthorized users
10	Q1	Under Amour	(Hacking) 150,000,000 email addresses, usernames, and hashed passwords belonging to users of the MyFitnessPal app accessed by a hacker
10	Q2	Exactis	(Web) 230,000,000 personal details of adults as well as information on 110 million business contacts exposed on the Internet due to a misconfigured marketing database
10	Q3	Huazhu Hotel Group	(Hacking) 240,000,000 records containing personal information on 130 million individuals stolen by hackers
9.71	Q2	Ticketfly, LLC	(Hacking) 26,151,608 customer and employee details taken by hackers and later leaked online
9.65	Q2	Hudson's Bay Company	(Hacking) Up to 5,000,000 customers' credit card details stolen from point of sale system by hackers

Score	Reported	Organization (Third Party)	Top 10 Summary
9.63	Q2	Social Sweethearts (Nametests.com)	(Web) 120,000,000 Facebook user IDs, names, dates of birth, languages, genders, photos, devices used, and post details leaked to unauthorized third parties due to programming flaw
9.56	Q2	MyHeritage Ltd	(Hacking) 92,283,889 user email addresses and hashed passwords stolen by hackers through undisclosed means

Top 20 Largest Breaches All Time (By Records Exposed)

Reported Date	Summary	Records Exposed	Organization	Industry-Sector	Breach Location
All Time Highest 12/14/2016	Recent revelations around the 2013 intrusion into Yahoo's systems moves this event back into the top spot	3 Billion	Yahoo	Business - Technology	United States
Number 2 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 3 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 4 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
Number 5 1/3/2018	Village-level enterprise operators sell access to the Aadhaar database	1.1 Billion	Unknown	Unknown	India
Number 6 1/3/2017	Email addresses, passwords, and SMTP credentials exposed on the Internet due to a misconfigured spambot database	711 Million	Unknown	Unknown	Netherlands
Number 7 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 8 9/11/2018	Misconfigured database exposes up to 445 million customer details including names, email addresses and IP addresses	445 Million	Veeam Software	Business - Technology	Switzerland

Reported Date	Summary	Records Exposed	Organization	Industry-Sector	Breach Location
Number 9 10/18/2016	Hackers compromise member email addresses, usernames, and encrypted passwords, IP addresses and statuses.	412 Million	FriendFinder Networks, Inc	Business - Technology	United States
Number 10 12/5/2017	Misconfigured MongoDB exposes over 400 million names, phone numbers, email addresses and other customer information	404 Million	Ai.type	Business - Technology	Israel
Number 11 5/27/2016	Hack exposes user accounts containing SHA1 encrypted passwords, email addresses.	360 Million	MySpace	Business - Technology	United States
Number 12 6/27/2018	Misconfigured marketing database exposes 230 million personal details as well as 110 million business contact records	340 Million	Exactis	Business – Professional Services	United States
Number 13 5/3/2018	Usernames and clear text passwords accidentally captured in an unprotected internal log	336 Million	Twitter	Business - Technology	United States
Number 14 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 15 8/28/2018	Customer contact details as well as bank account numbers stolen by hackers	240 Million	Huazhu Hotel Group	Business - Hotel	China
Number 16 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 17 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 18 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 19 6/19/2017	Unsecured Amazon S3 bucket exposes voter names, addresses, dates of birth, contact information and preferences.	198 Million	Deep Root Analytics	Business / Business	United States
Number 20 12/28/2015	Misconfigured 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

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 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 arising primarily from data mishandling
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 devices (such as a 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 for unauthorized purposes
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)

Name	Description
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 (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 / Undisclosed
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 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.

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.

For more information, please visit:
https://www.riskbasedsecurity.com/
Or call 855-RBS- RISK.

About Risk Placement Services

Risk Placement Services, Inc. (RPS), one of the nation's largest intermediaries, offers valuable solutions in wholesale brokerage, binding authority, programs and standard lines. Headquartered in Rolling Meadows, Illinois, RPS has more than 80 branch office and satellite locations, creating a coast-to-coast network of offices with retailer needs in mind. RPS places well over $3.1 billion in premium annually, demonstrating the company's strength and market presence. RPS leverages local knowledge, regional expertise and national relationships to deliver winning proposals to each retail broker partner and provide knowledge-based coverage solutions for each situation.

The RPS Executive Lines division specializes in protecting individuals and their companies against a wide range of executive risks and other professional liabilities. Market-leading specialists in public, private, and nonprofit Directors & Officers (D&O), Errors & Omissions (E&O), Fiduciary, Crime, and Kidnap & Ransom insurance products, RPS Executive Lines provides total management insurance solutions via 100 different insurance markets. Additionally, they help clients pinpoint hidden exposures to loss and fortify them against vulnerabilities, ultimately improving their risk profile.