RiskBased SECURITY

Not Just Security, the Right Security.

CYBER RISK ANALYTICS

Better Data Matters

# Data Breach QuickView Report

## First Quarter 2019 - Data Breach Trends

**Risk Based Security, Inc.**

**Issued on April 30, 2019**
**Data as of March 31, 2019**

### 2019 starts off fueled by credential leaks and compromised email accounts

- **1,903** breaches were reported through March 31, exposing approximately **1.9 billion** records.
- Compared to Q1 2018, the number of reported breaches was ***up 56.4%*** and the number of exposed records was ***up 28.9%*** *from 1.4 billion*.
- Of the breached organizations that could be definitively classified, the Business sector accounted for 71.1% of reported breaches, followed by Medical (13.6%), Government (7.8%), and Education (6.8%).
- Already in 2019, there have been three breaches exposing **100 million** or more records. Despite this, only one new breach was added to the top twenty largest breaches of all time.
- The Business sector accounted for 85.6% of the records exposed followed by Unclassified at 12.6% and Medical at 1.5%. The Governmental and Education sectors combined accounted for 5.8 million records exposed in Q1, or less than 0.03% of the total records exposed.
- **Web** continued its reign in the top spot for the breach type exposing the most records, accounting for **67.6% of compromised records**, while **Hacking** remained firmly as the top breach type for number of incidents, accounting for **84.8% of reported breaches**.
- **14.7%** of breached organizations were unwilling or unable to disclose the number of records exposed.

# Table of Contents

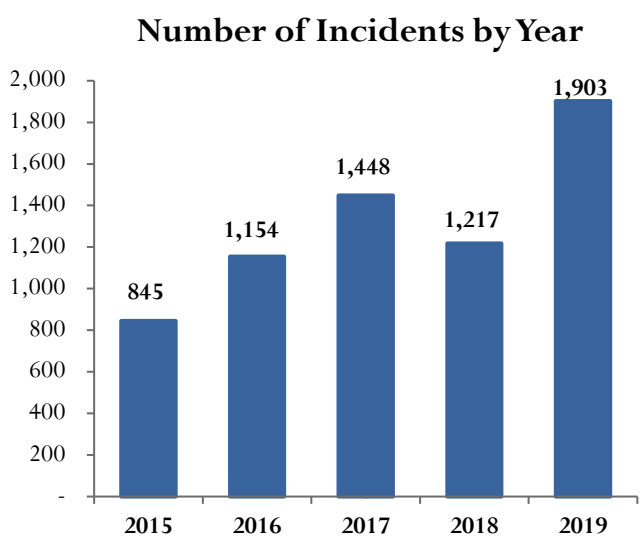
## Introduction

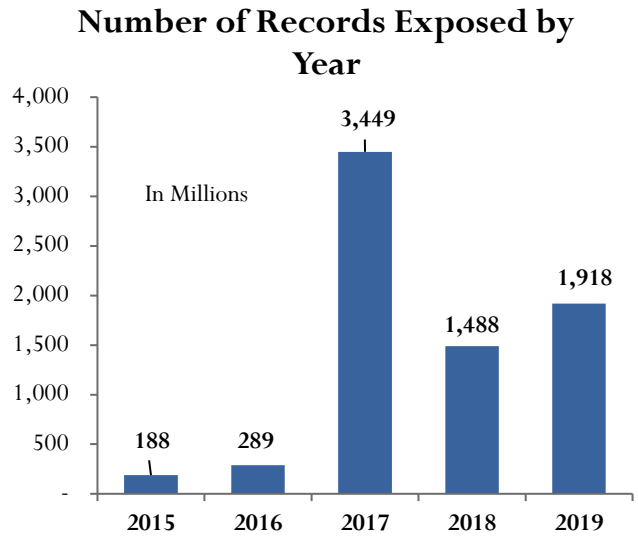
Everywhere you look today you see the concept of "*risk-based security*" being touted as the next big thing. At Risk Based Security we have been advocates of that concept for nearly a decade. We have always believed that the goal should be to know your vendors and assets, understand the threats and vulnerabilities that may impact those vendors and assets, and calculate a risk score in order to prioritize mitigation actions. This is not accomplished by a single exercise once a year. It requires a continuous assessment of your organization's risk posture as well as assessment of key vendors, suppliers, and business associates. Calculating a risk score to guide your mitigation program, while using incomplete and infrequently updated information, merely gives you a false sense of security and well-being when perhaps your true risks go unidentified. The difference is the data.

Ask yourself the questions, "What is my source of data breach information?" and "What is my source of software vulnerability information?" And then ask your service and tool providers the same questions. You'll be surprised at the lack of transparency, meaning they typically rely on sources of data that are incomplete with late reporting. After you read this report, we doubt you will find that an acceptable response.

#BetterDataMatters

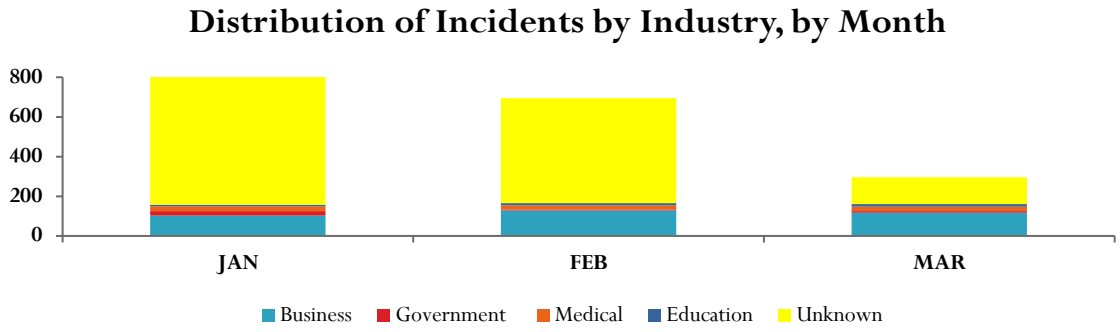
## First Three Months of 2019 Compared to Q1 of the Previous Four Years

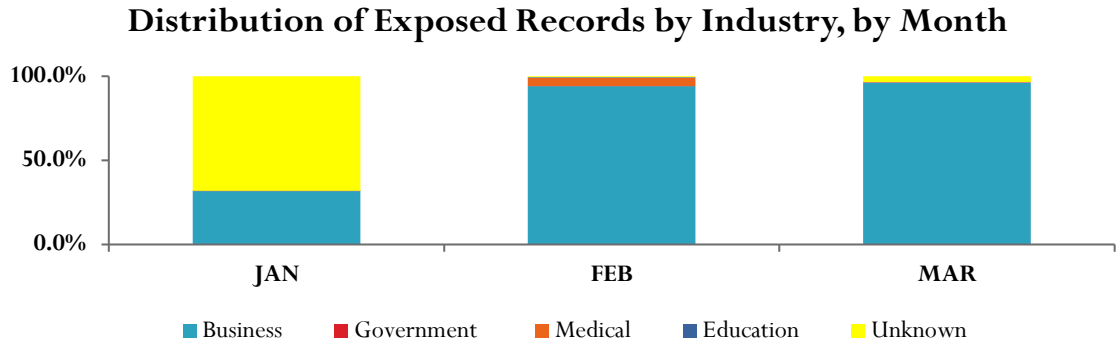



For three years in a row more than one billion records have been exposed in the first quarter of the year, whereas between 2009 and 2016, the number of records exposed in the first quarter generally fell in the 100,000,000 – 200,000,000 range, with only 2016 and 2014 exceeding 200 million. Why the shift? Two causes stand out: leaky databases and malicious actors going public with sizable data sets for sale.

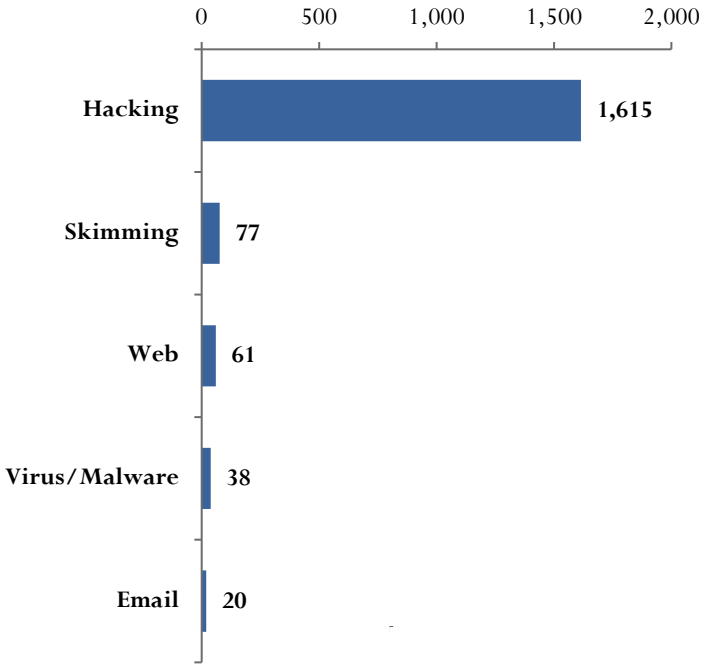
## First Three Months of 2019 Breaches by Industry, by Month



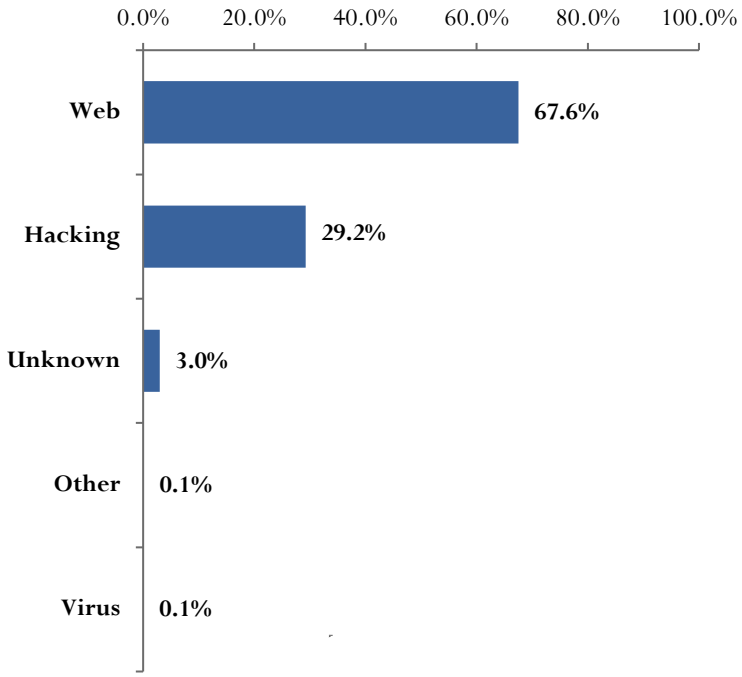
## First Three Months of 2019 Breaches by Type and Record Exposed

### Top 5 Breach Types



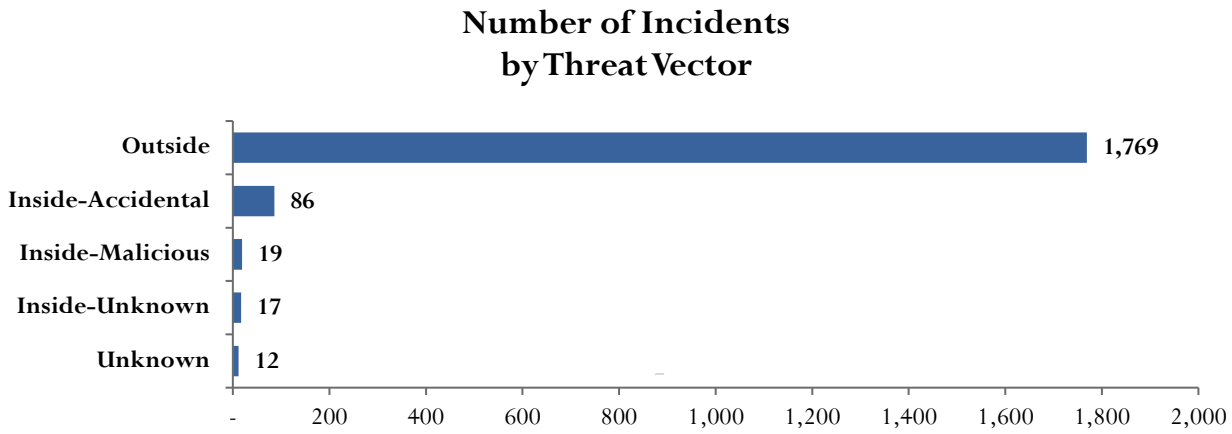

Regular readers of the QuickView Report will recognize a consistent theme here, with unauthorized access into services or systems ("hacking") taking the top spot for breach type.

### Records Exposed by Breach Type




Another consistent theme, exposure of sensitive data on the Internet ("web") remains the number one contributor to the total number of records exposed, which is unfortunate as preventing this is largely within the organization's control.

## First Three Months of 2019 Breaches by Threat Vector




Going hand-in-glove with Hacking as the top breach type, incidents originating outside of the compromised organization are, by far, the largest threat vector. A particularly popular attack method evident in recent quarters is targeting user email accounts. Malicious actors typically phish employees or use leaked credentials to access email services. Although pilfering sensitive data is not always the attackers' objective, such access can trigger lengthy investigations and give rise to a string of regulatory obligations.

| Threat Vector | Records Exposed |
|---|---|
| Inside-Accidental | 1,262,020,967 |
| Outside | 620,107,852 |
| Inside-Unknown | 36,453,278 |
| Unknown | 112,920 |
| Inside-Malicious | 71,071 |
| **Total** | **1,918,766,088** |

## First Three Months of 2019 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 2019 | 87 | 4,194,268 | 1,580 | 1,823,324,010 | 236 | 91,245,675 |

This outcome closely mirrors prior quarters with the majority of breaches discovered via external sources such as notification by law enforcement, fraud monitoring, actor disclosure, security researchers or notification from customers themselves.

## First Three Months of 2019 Time Interval Between Discovery and Reporting

| | Q1 2019 | Q1 2018 | Q1 2017 | Q1 2016 | Q1 2015 |
|---|---|---|---|---|---|
| Average Number of Days Between Breach Discovery and Reporting | 54.0 | 37.9 | 42.7 | 68.9 | 82.6 |
| Average For The Year | 2019 | 2018 | 2017 | 2016 | 2015 |
| | TBD | 49.6 | 48.6 | 60.9 | 70.1 |

In the 2018 Year End QuickView Report we posed this question: could there be a correlation between discovery method and the average number of days it takes to disclose the breach? It seemed likely the organizations that were able to discover their breaches would also be better prepared to respond, resulting in a shorter number of days between discovery and reporting. Analysis of Q1 2019 does ***not*** support this assumption. In fact, organizations that learned of the breach from external sources disclosed the incident much more quickly than organizations that learned of the breach through internal sources.

For Q1 2019, the average number of days between discovery and disclosure was 43 days when the breach came to light via external sources. However, it was a stunning 74 days for organizations that learned of the breach via internal sources. The median number of days between discovery and disclosure was equally surprising, with a median of 8 days for external discovery compared to a median of 46 days for internal discovery.

Is this a random outcome? Tune in to the QuickView Report throughout the year as we continue to track the data.

## First Three Months of 2019 Ten Largest Breaches by Records Exposed[1]

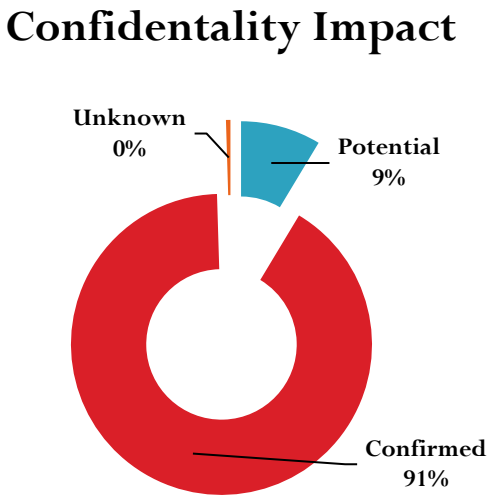
| Breach Type | Records Exposed | Percentage of Total Exposed | Data Type[2] | Severity Score |
|---|---|---|---|---|
| Web | 982,864,972 | 51.2% | ADD/DOB/EMA/FIN/MISC/NAA/NUM/PWD | 10 |
| Web | 202,730,434 | 10.6% | ADD/DOB/EMA/MISC/NAA/NUM | 9.39 |
| Hack | 161,549,210 | 8.4% | EMA/MISC/NAA/PWD/USR | 9.81 |
| Hack | 60,800,000 | 3.2% | EMA/MISC/PWD | 9.39 |
| Hack | 57,000,000 | 3.0% | ADD/EMA/MISC/PWD/USR | 9.36 |
| Hack | 41,028,098 | 2.1% | DOB/EMA/MISC/NAA/PWD/USR | 9.52 |
| Hack | 40,000,000 | 2.1% | EMA/MISC/NAA | 9.20 |
| Web | 33,000,000 | 1.7% | ADD/EMA/MISC/NUM/USR | 8.77 |
| Hack | 28,510,450 | 1.5% | EMA/NAA/PWD | 9.06 |
| Web | 24,300,000 | 1.3% | ADD/DOB/FIN/MISC/NAA/SSN | 9.16 |

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

## First Three Months of 2019 Analysis by Data Family

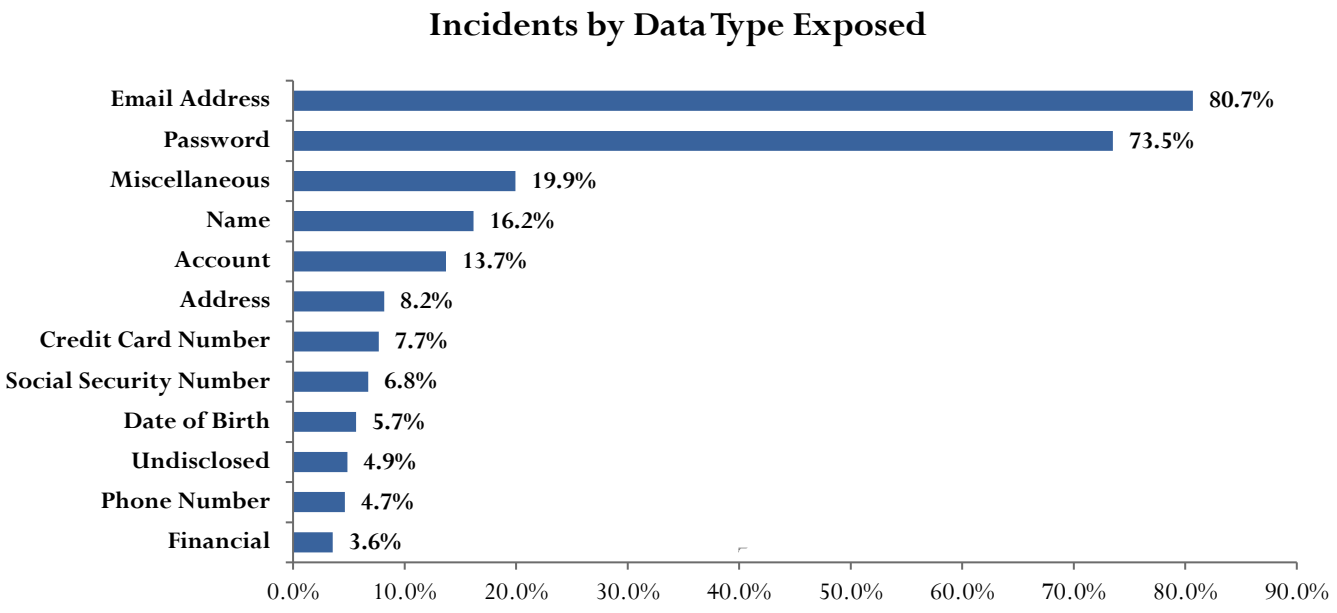
| | Percentage of Total Breaches | Percentage of Total Exposed Records | Percentage of Total Breaches | Percentage of Total Exposed Records |
|---|---|---|---|---|
| **Data Family** | **2018** | **2018** | **2019** | **2019** |
| **Electronic** | 92.03% | 99.98% | 98.12% | 100.00% |
| **Physical** | 5.34% | <1% | 1.57% | N/A |
| **Unknown** | 0.49% | <1% | <1% | N/A |

## First Three Months of 2019 Impact on Data Confidentiality




Q1 of 2018 saw the number of incidents with confirmed data exposure drop to 68%. Throughout 2018 and now into Q1 of 2019, confidentiality impact has returned to a more typical distribution.

## First Three Months of 2019 Breach Analysis by Data Type



| Percentage of Breaches Exposing Top Four Data Types – 2019 vs. Prior Years | | | |
|---|---|---|---|
| **Data Type** | **2019** | **2018** | **2017** |
| **Email Address** | 80.7% | 44.7% | 39.4% |
| **Password** | 73.5% | 40.7% | 34.5% |
| **Miscellaneous** | 19.9% | 16.5% | 13.4% |
| **Name** | 16.2% | 35% | 40.7% |

## First Three Months of 2019 Analysis of Records Compromised Per Breach

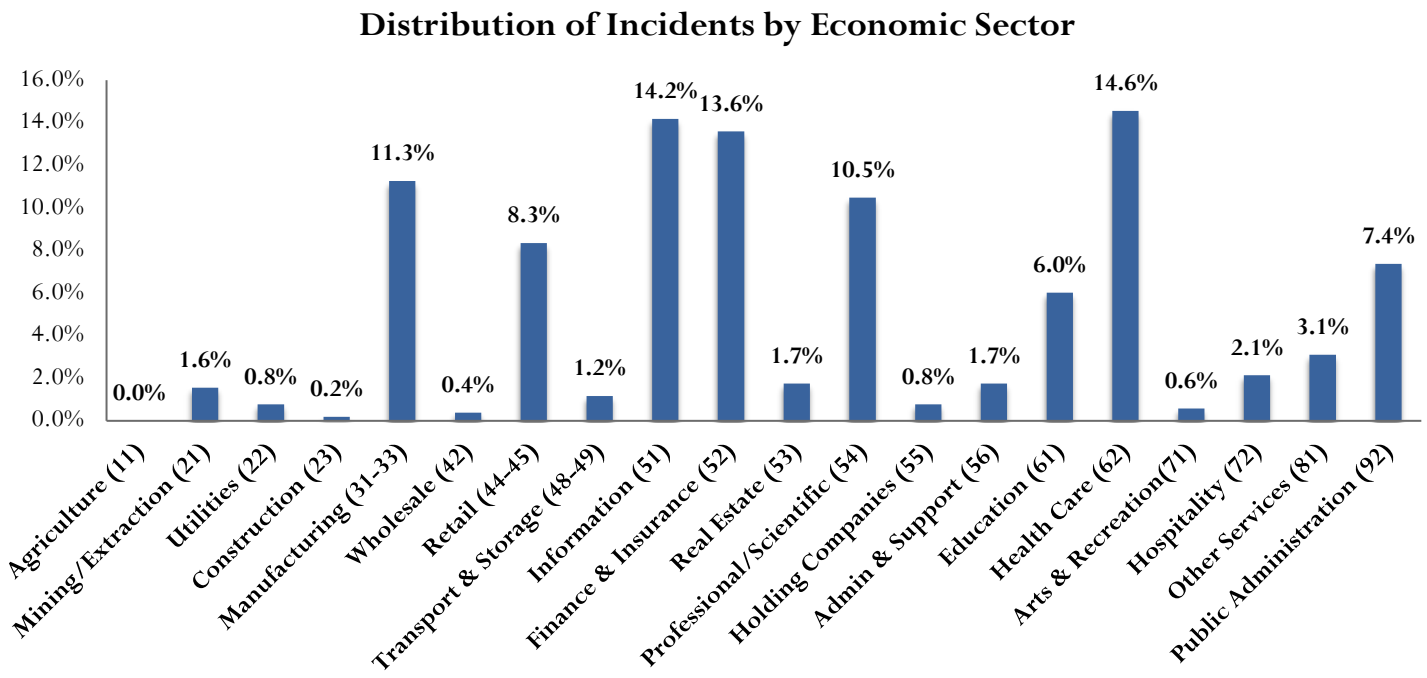
| Exposed Records | Number of Breaches | Percent of Total |
|---|---|---|
| Unknown/Undisclosed | 280 | 14.7% |
| 1 to 100 | 799 | 42.0% |
| 101 to 1,000 | 596 | 31.3% |
| 1,001 to 10,000 | 113 | 5.9% |
| 10,001 to 100,000 | 47 | 2.5% |
| 100,001 to 500,000 | 13 | 0.7% |
| 500,001 to 999,999 | 5 | 0.3% |
| 1 M to 10 M | 30 | 1.6% |
| > 10 M | 20 | 1.1% |

Despite 50 breaches exposing one million or more records, 79% of breaches expose between 1 and 10,000 records.

## First Three Months of 2019 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 | 1,615 | 560,596,868 | 347,118 | 29.2% |
| Skimming | 77 | 611 | 7 | <1% |
| Web | 61 | 1,295,803,481 | 21,242,680 | 67.6% |
| Malware/Virus | 38 | 2,253,989 | 59,315 | <1% |
| Email | 20 | 68,019 | 3,400 | <1% |

## First Three Months of 2019 Analysis of Incidents by NAICS Economic Sector



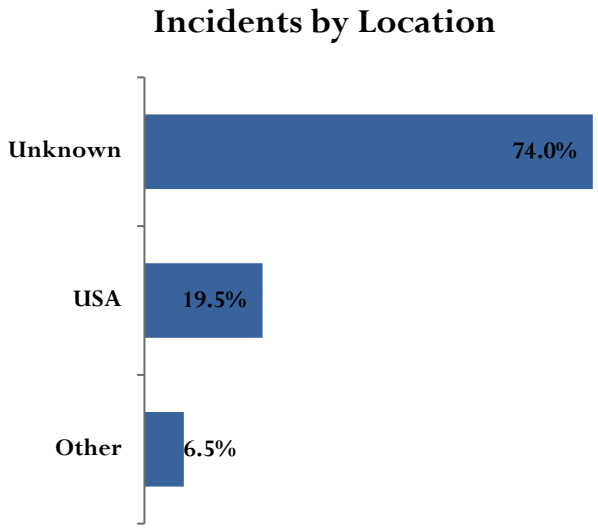

*Where known. Organizations that could not be definitively classified have been removed from results

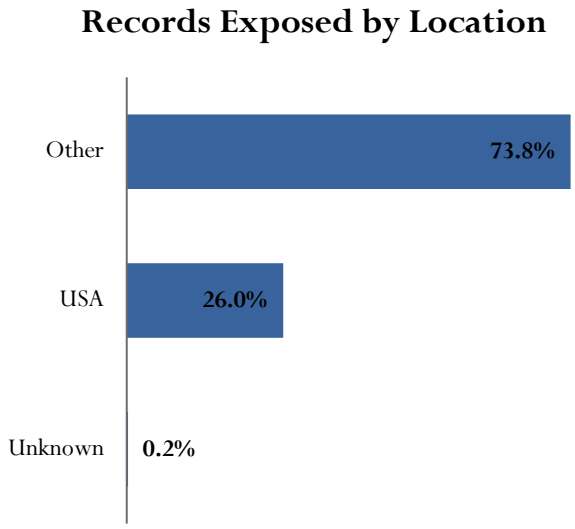
## First Three Months of 2019 Top Business Groups For Top 3 Economic Sectors

| Economic Sector | Business Group | Percentage of Breaches Within Economic Sector |
|---|---|---|
| Health Care (62) | Practitioner Offices | 37% |
| | Hospitals | 28% |
| | Medical Facilities | 26% |
| Information (51) | Software / Websites | 84% |
| | Telecommunications | 11% |
| | Mass Media | 5% |
| Finance & Insurance (52)* | Financial | 70% |
| | Insurance | 30% |

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

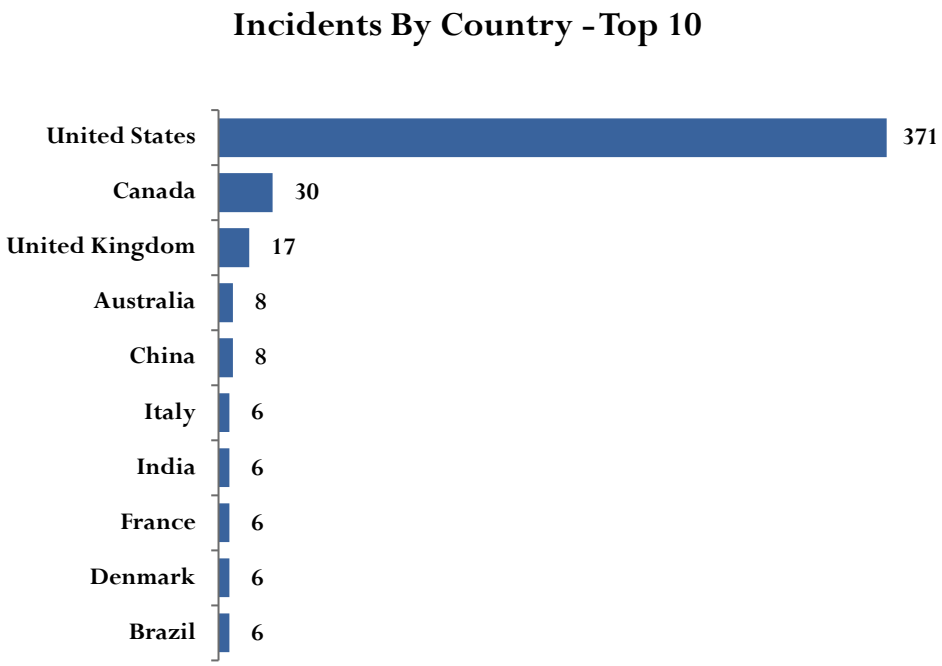
## First Three Months of 2019 Analysis of Breaches by Location




A significant number of smaller credential leaks were detected in Q1. This accounts for the high percentage of breaches where the origin of the event could not be definitively identified coupled with a low percentage of records attributed to an unknown location.

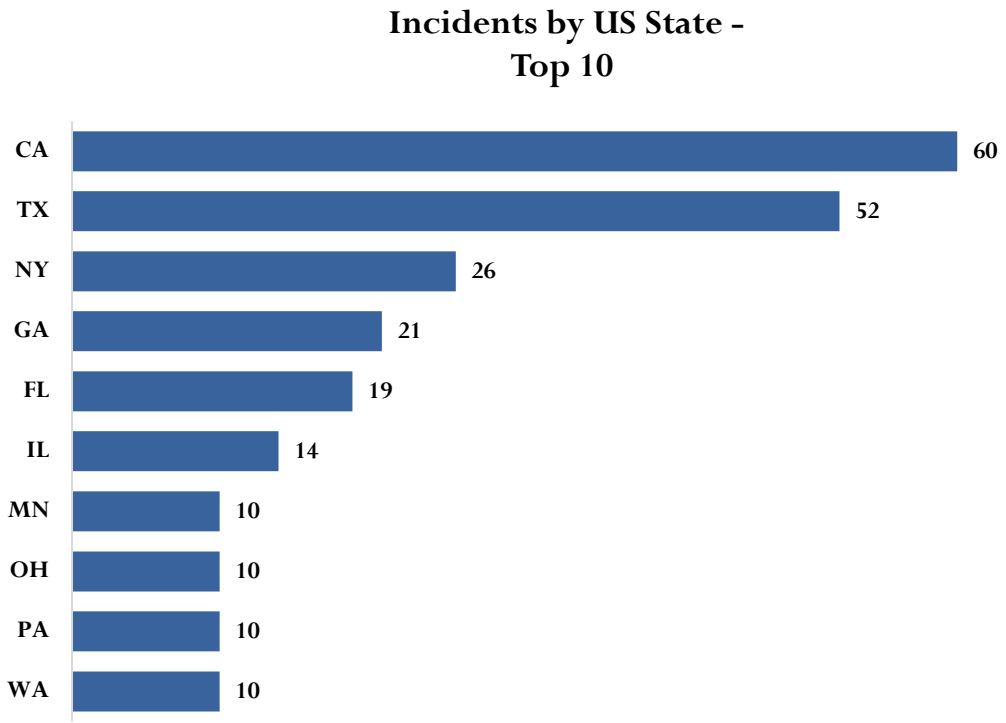
## First Three Months of 2019 Year Breaches by Country



## First Three Months of 2019 Exposed Records by Country

| Ranking | Number of Breaches | Country | Total Exposed Records | Average Records per Breach | Median Records Exposed | Percentage of Exposed Records |
|---|---|---|---|---|---|---|
| 1 | 1 | Estonia | 982,864,972 | N/A | N/A | 51.22% |
| 2 | 371 | United States | 498,772,695 | 1,344,401 | 9,000 | 25.99% |
| 3 | 8 | China | 245,466,459 | 30,683,307 | 2,182,862 | 12.79% |
| 4 | 3 | Germany | 42,451,432 | 14,150,477 | 21,270,716 | 2.21% |
| 5 | 2 | Sweden | 27,460,000 | 13,730,000 | 13,730,000 | 1.43% |
| 6 | 2 | Spain | 27,000,000 | 13,500,000 | 13,500,000 | 1.41% |
| 7 | 6 | India | 24,957,200 | 4,159,533 | 6,791,200 | 1.30% |
| 8 | 30 | Canada | 19,008,013 | 633,600 | 50 | 0.99% |
| 9 | 1 | Indonesia | 13,000,000 | N/A | N/A | 0.68% |
| 10 | 3 | Japan | 8,460,000 | 2,820,000 | 3,100,000 | 0.44% |
| Total | 427 | | 1,899,440,771 | 4,424,920 | | 98% |

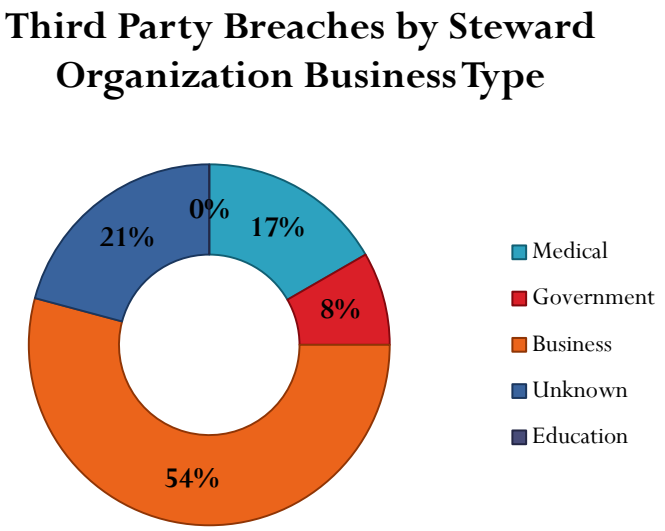
## First Three Months of 2019 Distribution of Breach Location By State



## First Three Months of 2019 Analysis of US State Rankings, Exposed Records

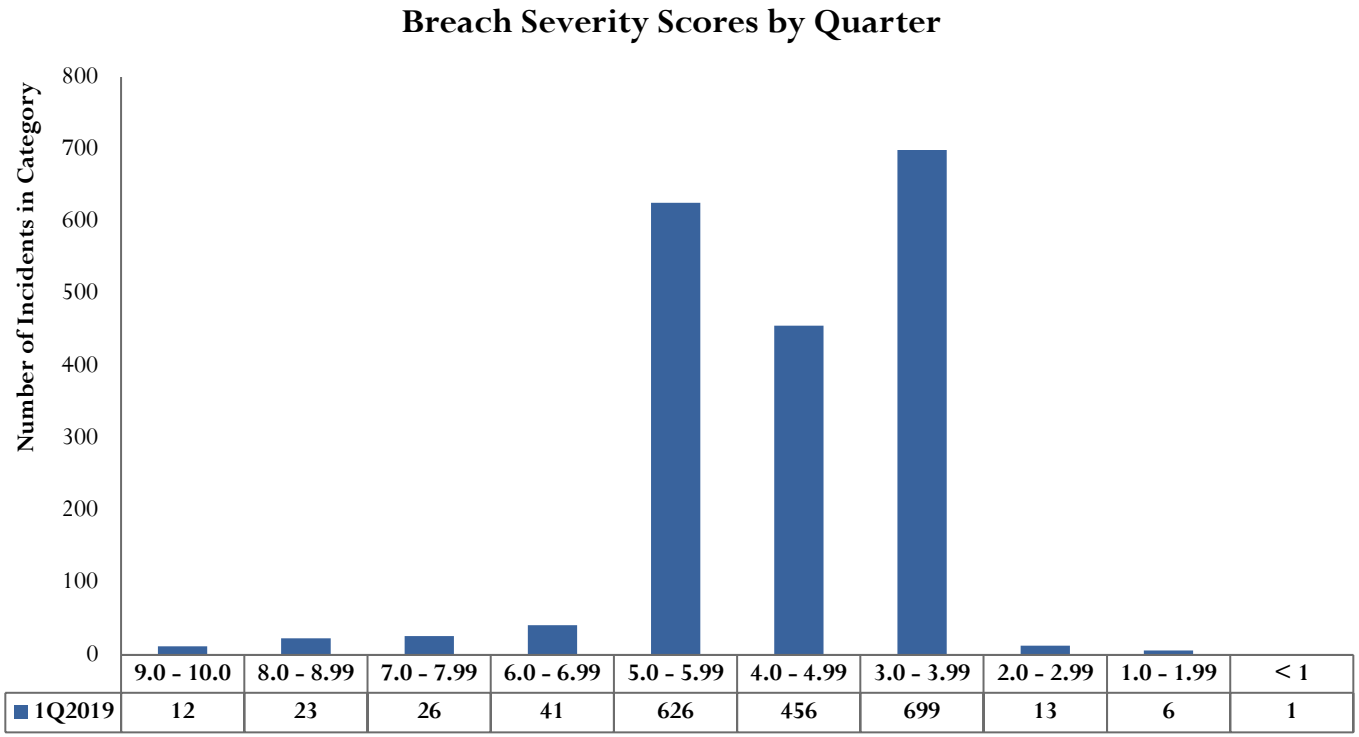
| Exposed Records Ranking | US State | Total Exposed Records | Number of Breaches | Exposed Records/Breach | Percentage of Records Exposed in USA |
|---|---|---|---|---|---|
| 1 | NY | 235,460,373 | 26 | 9,056,168 | 47.21% |
| 2 | CA | 212,740,111 | 60 | 3,545,669 | 42.65% |
| 3 | WA | 19,151,276 | 10 | 1,915,128 | 3.84% |
| 4 | TX | 9,340,004 | 52 | 179,615 | 1.87% |
| 5 | OR | 8,027,643 | 6 | 1,337,941 | 1.61% |
| 6 | KS | 4,083,473 | 6 | 680,579 | 0.82% |
| 7 | FL | 2,207,906 | 19 | 116,206 | 0.44% |
| 8 | GA | 375,811 | 21 | 17,896 | 0.08% |
| 9 | CT | 352,237 | 5 | 70,447 | 0.07% |
| 10 | SC | 91,242 | 4 | 22,811 | 0.02% |

## First Three Months of 2019 Breaches Exposing Third Party Data




Vendors, suppliers, and key service providers can hold or process terabytes of sensitive data on behalf of their customers. When such service providers expose data, it can trigger a cascading effect whereby one event impacts the data of multiple organizations. There were 49 such incidents reported in the first quarter of 2019, ranging from events such as the breach at Toyota Tokyo Sales Holdings, which exposed customer records at subsidiary operations as well as affiliated dealerships, to a Point of Sale (POS) solutions provider that exposed payment card details of the customers of at least 15 different companies.

## First Three Months of 2019 Breach Severity Scores




## First Three Months of 2019 Top 5 Breaches By Severity Score

| Score | Reported | Organization (Third Party) | Top 10 Summary |
|---|---|---|---|
| 10 | March | Verifications.io | (Web) 982,864,972 names, email & IP addresses, dates of birth, contact information, personal mortgage amounts, and FTP server credentials exposed on the Internet due to a misconfigured database |
| 9.81 | February | Dubsmash, Inc. | (Hacking) 161,549,210 users' names, IDs, email addresses, usernames, SHA256-hashed passwords, languages, and countries stolen by hackers |
| 9.51 | February | ShareThis Inc. | (Hacking) 41,028,098 users' names, usernames, email addresses, DES-hashed passwords, genders, and dates of birth stolen by hackers |
| 9.50 | March | Earl Enterprises | (Malware) 2,150,000 customer names, and credit or debit card numbers with expiration dates stolen by hackers employing malware |
| 9.38 | January | Undisclosed | (Web) 202,730,434 job applicants' personal details exposed on the Internet due to a misconfigured database |

## 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 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 |
| **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 |

| Reported Date | Summary | Records Exposed | Organization | Industry-Sector | Breach Location |
|---|---|---|---|---|---|
| **Number 11** 11/30/2018 | Hackers compromise loyalty program database, exposing names, addresses, reservation details, passport numbers | 383 Million | Starwood (Marriott) | Business – Hotels | United States |
| **Number 12** 5/27/2016 | Hack exposes user accounts containing SHA1 encrypted passwords, email addresses | 360 Million | MySpace | Business - Technology | United States |
| **Number 13** 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 14** 5/3/2018 | Usernames and clear text passwords accidentally captured in an unprotected internal log | 336 Million | Twitter | Business - Technology | United States |
| **Number 15** 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 16** 8/28/2018 | Customer contact details as well as bank account numbers stolen by hackers | 240 Million | Huazhu Hotel Group | Business - Hotel | China |
| **Number 17** 10/11/2018 | Customer names, contact details, dates of birth and other personal information exposed by misconfigured database | 236 Million | FitMetrix, Inc | Business - Technology | United States |
| **Number 18** 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 19** 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 20** 1/10/2019 | Job applicants personal details are exposed to the Internet due to a misconfigured database | 202 Million | Organization's Name has not been reported | Unknown | China |

# 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.