RiskBased SECURITY

2020 Mid Year Report

Data Breach QuickView



Welcome



Is this the new normal, or a temporary disruption like shelves emptied of toilet paper?

If you tuned in to the Q1 Data Breach QuickView Report, you're already aware that 2020 started off as a very unusual year. If you're new to the QuickView Report, it won't take much reading to realize the six-month mark of 2020 is already unlike any previously reported mid year point.

The number of publicly reported breaches stands at its lowest point in five years, while the number of records exposed is more than four times higher than any previously reported six month time period. The striking differences between 2020 and prior years bring up many questions. Why is the breach count low compared to prior years? What is driving the growth in the number of records exposed? And perhaps most importantly, is this a permanent change in the data breach landscape?

Throughout this report we will provide our take on those questions. We'll be digging into the data to shed light on which trends we believe are anomalies, and which represent more enduring change. This mid year report covers publicly disclosed data breaches first reported between January 1, 2020 and June 30, 2020 and compares current observations to the same time period for prior years. It is our sincere hope that you find this report to be a valuable resource as well as an interesting read.

Key Highlights

- There were 2,037 publicly reported breaches through June 30th, a 52% decrease compared to the first six months of 2019 and 19% below the same time period for 2018.
- Over 27 billion records were exposed between January 1, 2020 and June 30, 2020, exceeding the total number of records exposed during the entirety of 2019 by more than 12 billion records.
- The driving force behind the number of records exposed continues to be misconfigured databases and services.
- The two largest breaches ever reported came to light during the second quarter of 2020, accounting for more than 18 billion of the 27 billion records put at risk.
- The number of payment card details exposed in the first six months of 2020 surpassed 90 million records. Despite this, there were even more Social Security / national identity numbers, financial account numbers, and dates of birth exposed during this time period.
- Four economic sectors (Information, Health Care, Finance & Insurance, and Public Administration) accounted for more than half (52.5%) of reported breaches.
- The Information sector accounted for 14.5% of reported breaches, with software providers, hosting, and other online services accounting for 86.5% of the information sector breaches.
- The healthcare sector nearly matched the information sector, accounting for 14.3% of the reported breaches.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

In This Issue

FEATURING VIEWPOINTS FROM



Inga Goddijn
Executive Vice President,
Risk Based Security

The Cyber Risk Analytics Research Team
Risk Based Security

WELCOME

Key Highlights **2**

In This Issue **3**

Viewpoints **4**

The Breach Landscape: Better, Worse, or Both? 4

Mixing Work and Play: A Dangerous Cocktail of Leaked Credentials 6

Data Breach Trends in 2020 ..... **8**

Mid Year 2020 At A Glance 10

Who Was Breached in 2020? 15

Where Did Breaches Occur in 2020? 17

In Closing **19**

Methodology and Terms 19

Data Standards and the Use of "Unknown" 19

About Risk Based Security **20**

About Cyber Risk Analytics 20

No Warranty 20

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

The Breach Landscape: Better, Worse, or Both?



Inga Goddijn, Executive Vice President, Risk Based Security

Inga found her way to information security after working for twenty years in the insurance industry. During her time managing a multi-million dollar portfolio of technology and cyber insurance coverages, Inga witnessed first-hand the impact of ineffective security program management and the financial fallout from data breach events. At Risk Based Security, she is responsible for Cyber Risk Analytics and YourCISO. Inga has presented at a variety of industry forums and has led many education sessions throughout the U.S. She currently holds a CIPP/US designation.

From a quick look at the charts on page 8, it's clear that something unusual is happening. The number of publicly disclosed data breaches is *down 52%* compared to the same period in 2019, while the number of records exposed is *nearly six times higher*. The breach and record counts stand in stark contrast to the prior year, and it also begs the question: how can the number of breaches be declining while the number of records exposed has ballooned to unprecedented levels? Both anomalies are worth closer examination.

ARE THERE REALLY FEWER BREACHES TAKING PLACE?

This question has been top of mind for our research team for the past several months. The consensus among the group is no, most likely the pace of breach activity is on par with recent years. As with many other industries, we believe that data breach reports are suffering from the all-too-familiar supply chain disruption. In this case our supply of reported data breach information. Our research focuses on publicly disclosed events, using a robust system for uncovering these disclosures. This means we rely on a degree of transparency and various outlets to actually surface the information. As we mentioned in our Q1 Data Breach QuickView Report, in early March we observed a conspicuous decline in the amount of reporting on breach events. This trend has continued into the second quarter. For comparison, in the first six months of 2019 we validated approximately 6,700 unique reports that contained information useful for documenting breach events. For the same time period this year, the number dropped to approximately 4,500. When we dig deeper into the reasons behind this decline, we see less coverage per event as well as delayed reporting from some sources. Clearly there is less information being disclosed.

ARE BREACHES REALLY GETTING WORSE IN TERMS OF THE NUMBER OF RECORDS EXPOSED?

For the past few years, misconfigured databases and services have been the key driver behind the growing number of records exposed. It is easy to understand why. When entire databases are left open and freely accessible, a considerable amount of data is put at risk. It is a small handful of these events in Q2 that are responsible for the explosion in the number of records exposed.

Setting aside the mega leaks, there are signals that breach events are trending toward increased severity. Two data points stand out supporting this trend: the median number of records exposed, and the percentage of breaches exposing between one and 9,999 records. Focusing on the breaches where the record count is confirmed, we observed:

- Median number of records exposed in the first six months of 2020: **219**
- Median number of records exposed in the first six months of 2019: **125**
- Percentage of breaches exposing less than 10,000 records in the first six months of 2020: **74%**
- Percentage of breaches exposing less than 10,000 records in the first six months of 2019: **92%**

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

The Data Breach QuickView report is powered by

Cyber Risk Analytics

The standard for actionable data breach intelligence, risk ratings and supply chain monitoring.

- ☑ Cyber Insurance
- ☑ Security & Vulnerability Management
- ☑ Vendor Risk Management
- ☑ Procurement
- ☑ Governance & Management



REQUEST A DEMO
sales@riskbasedsecurity.com

LEARN MORE

Mixing Work and Play: A Dangerous Cocktail of Leaked Credentials

The Cyber Risk Analytics Research Team, Risk Based Security

Since 2011, the Cyber Risk Analytics (CRA) research team has provided organizations with the most comprehensive threat intelligence solution on the market, providing details about the number of data breaches, records exposed, industry type, threat vectors, and much more. The CRA research team has analyzed over 47,500 breaches exposing 69 billion records and monitors over 104,000 organizations.



In the second quarter of 2020, over 350 million passwords along with email addresses or usernames were compromised by malicious actors. The breaches ranged in size from the very small, exposing fewer than 50 records, to the very large, with tens of millions of access credentials exposed at once. Most passwords were hashed, although many were weakly protected, with outdated hashing algorithms, and easily decrypted. As is often the case, several larger breaches - or the full extent of previously reported breaches - came to light only *after* the pilfered data began circulating online.

Much has been written about the perils of reusing passwords as well as just how prevalent the problem is. The Cyber Risk Analytics research team actively monitors for leaked credentials, and can attest to the fact that underground hacking forums are awash with stolen credentials. From time to time the team shares details of some of the more interesting finds like the Quidd leak, the breach at MobiFriends, and the extortion-turned-leak incident at Preen.Me.

There is no shortage of password hygiene advice available, and best practices for password management are included in most information security frameworks. However, what is largely missing from the conversation is the point of view of the researchers that uncover and analyze these data sets. From our experience, two overlooked factors stand out.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

IS THAT ACCOUNT REALLY WORK RELATED?



When a dating application like MobiFriends is compromised, it may be tempting to think that the exposed credentials would be largely tied to consumer email domains such as gmail.com or yahoo.com. Unfortunately, that's not the case. Nearly five years after the notorious Ashley Madison breach, employees are still using workplace email addresses for personal use for a wide variety of services including potentially sensitive sites. We observed this trend across several incidents in Q2 including breaches at gaming sites, sports media companies, and recreation equipment dealers. Stronger policies around the use of business email accounts for personal purposes can help reduce the risk of third-party breaches potentially exposing employees' access credentials, as well as the risk of phishing campaigns targeting employee interests.

HELP ME HELP YOU

There is nothing quite like the frustration of knowing an entity has been compromised, but having no clear path for alerting the victim organization. Even casual followers of the news about misconfigured databases can sense the frustration of the researchers as they struggle to get the attention of the staff that can address the issue. That same holds true when trying to report an as-yet-undisclosed breach. Efforts to reach out are often met with silence, and in rare cases mistrust or outright hostility. Offering a mechanism to report security issues, even if it's as simple as a security@ email inbox, can go a long way toward facilitating the conversation. If it is a reputable source reaching out, chances are that news of the incident will eventually surface. No one wants to hear that they have a problem, but it's much better to know and respond *before* the event makes headlines. Perhaps it's time to look at the lessons learned from the software vulnerability coordination process. The leading software vendors have a mechanism allowing "potential" vulnerabilities in their products to be reported to them. Why not replicate something similar for potential exposes that could lead to a breach?

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Data Breach Trends in 2020

The unusual start to the year we observed in the first quarter continued as we closed in on the mid year point. Perhaps the most striking trend of the year to date is the significant damage inflicted by ransomware. In many ways, the incident at Travelex that kicked off 2020 stands out as an inflection point for ransomware operators, where the data exfiltration and lost revenue from disrupted operations has emerged as the more painful aspects of these events. This trend, as well as the larger themes observed over recent years, are discussed in more detail throughout this report.

Mid Year 2020 At A Glance

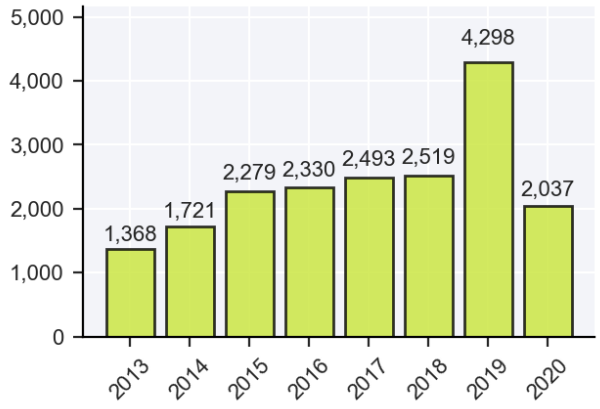


Figure 1: Number of breaches reported by Q2 each year

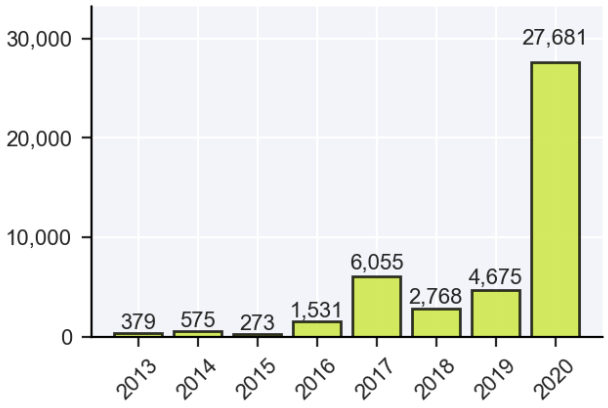


Figure 2: Number of records lost (in millions) reported by Q2 each year

As noted in the Key Findings, there was a 52% decrease in the number of breaches reported compared to the first six months of 2019. In the Q1 report we reflected on why the number of publicly disclosed breaches dropped so dramatically compared to Q1 of the previous year. We shared a combination of two factors that were impacting the numbers: a spike in illicit data leaks, coupled with a slow down in breach reporting. The slow pace of reporting observed in Q1 has continued into the second quarter and has yet to recover to pre-pandemic levels. It is interesting to note that, compared to 2018, the number of disclosed breaches is down by approximately 19%. This is roughly in line with the decline in the number of verified unique reports used to support breach research, which declined by 16% for the same period. For the record, RBS' research team does not believe the number of data breaches has truly declined, only the public reporting of the breaches.

The explosion in the number of records exposed is driven by three large breaches, which together accounted for 23.3 billion or approximately 84%, of the number records compromised. These three breaches were the result of misconfigured databases and services.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

A consistent theme from recent reports continues into 2020, with “Hacking”, or unauthorized access to systems or services, the primary driver behind the number of breaches, while online disclosures, classified as “Web”, were responsible for the number of records exposed.

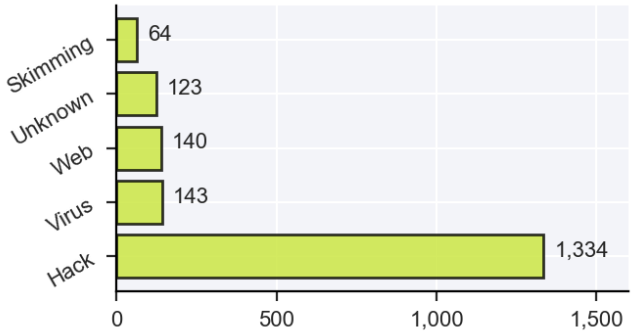


Figure 3: Number of breaches by breach type, reported by Q2 2020

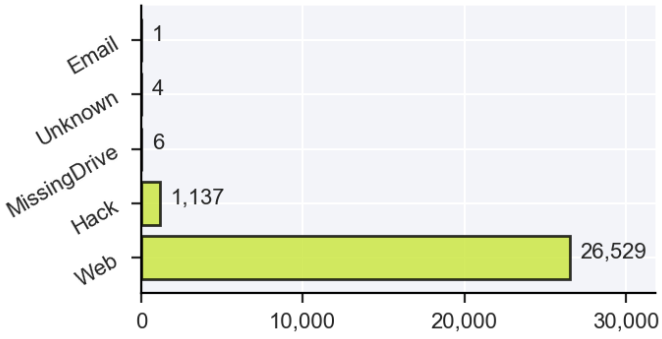


Figure 4: Number of records lost by breach type (in millions), reported by Q2 2020

As ransomware attacks evolve to become confirmed data breaches, it is worthwhile to look deeper at the difference between breach type “Hack” and breach type “Virus”. In our classification system, the action that most closely resulted in the data compromise is captured as the primary breach type. The various components leading up to, or contributing to, the data breach are captured in other fields. For example, an attack that begins with phishing for access credentials and ultimately allows malicious actors to gain access to email systems would typically be classified as “Hacking” with phishing and use of stolen credentials captured as contributing factors.

In the first six months of the year, there were 239 breaches that included ransomware as an element of the attack. If malicious actors gained access to the systems and leveraged this access to exfiltrate data, the event is captured as a “Hack” as opposed to “Virus”. Likewise, the “Web” category includes 23 events that were attributed to a publishing error, another 23 events that were attributed to a programming error, and 73 events that were attributed to misconfiguration.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Not surprisingly, with “Hacking” as the top breach type, attacks originating from outside the victim organization also comprise the top vector behind the number of reported incidents. Of the incidents originating from insiders, only 12% were from malicious insiders.

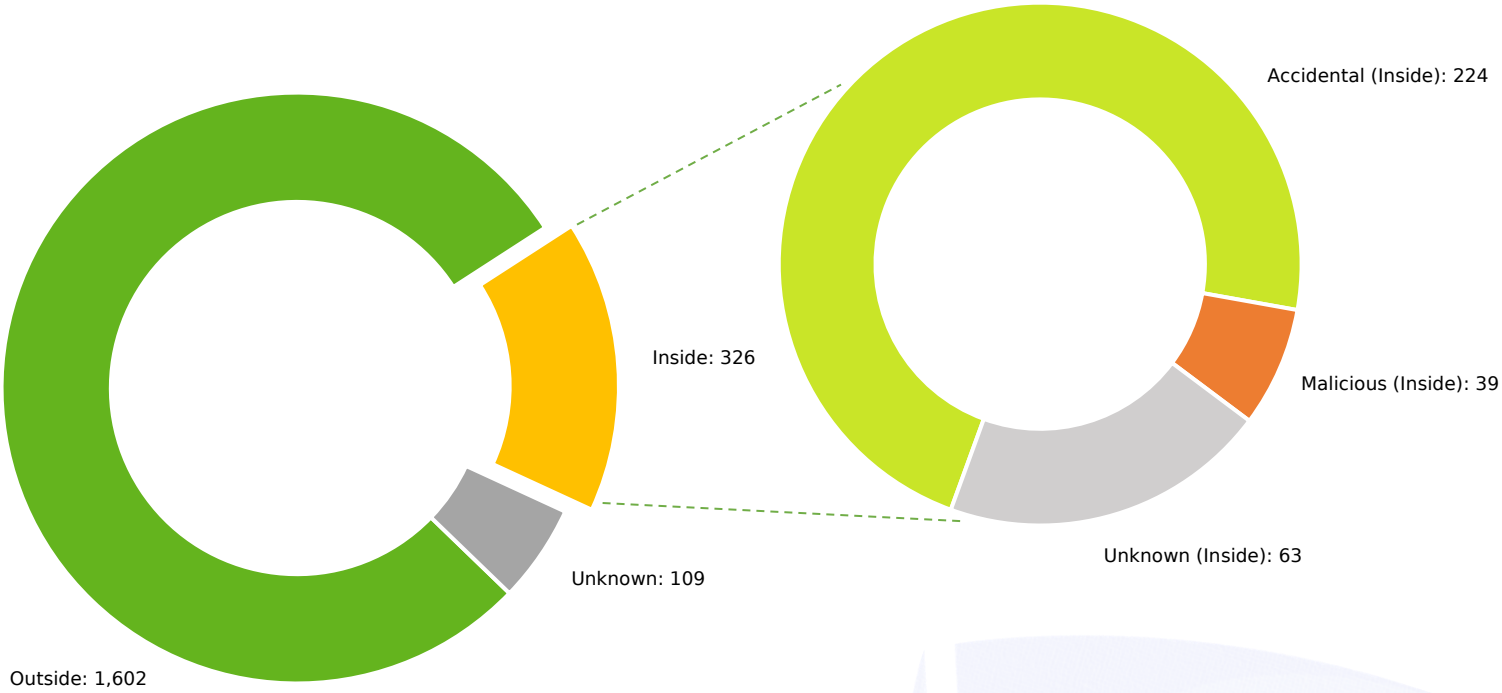


Figure 5: Number of breaches by attack vector, reported by Q2 2020

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Is it a breach if the steward organization loses control of access to sensitive information? We think so - as do many regulatory bodies. But that means not every breach results in data ending up in the hands of malicious actors. Incidents that are known to have resulted in unauthorized access to sensitive data are flagged as “Confirmed” exposure. Incidents where data was put at risk and unauthorized access cannot be ruled out are flagged as “Potential”. 66.5% of reported breaches included confirmed exposure of sensitive data while 31.1% of events put data at risk of exposure, such as an April event at a large university where documents containing names and Social Security numbers were inadvertently made publicly available in a digital library and archives.

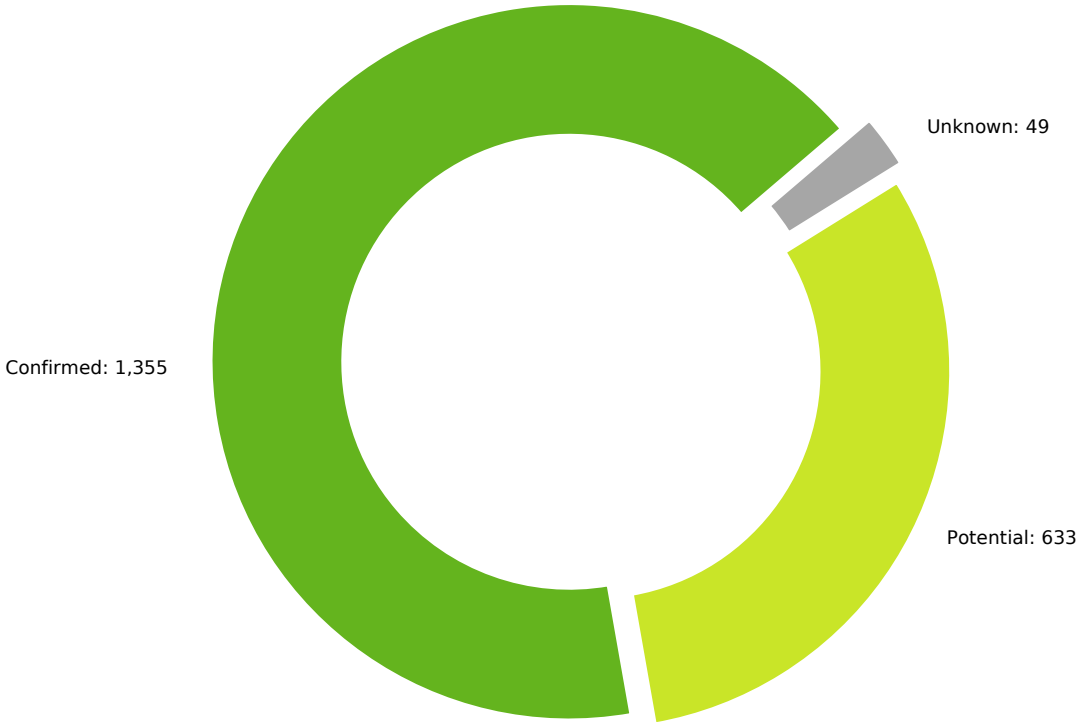


Figure 6: Number of breaches by known confidentiality impact, reported by Q2 2020

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Passwords in conjunction with email addresses or usernames remain some of the most targeted data types. New for this period is the steady rise in the number of breaches that include individuals' names. The reason(s) behind the shift are not entirely clear as no distinct pattern has yet emerged explaining the fluctuation**. It is possible that the slow down in breach disclosures is contributing to the trend**. As less breach information surfaces, the events that trigger a statutory obligation to notify impacted individuals may play a more prominent role in shaping the data types exposed, since names in conjunction with another piece of identifier information can result in a legal requirement to disclose the incident.

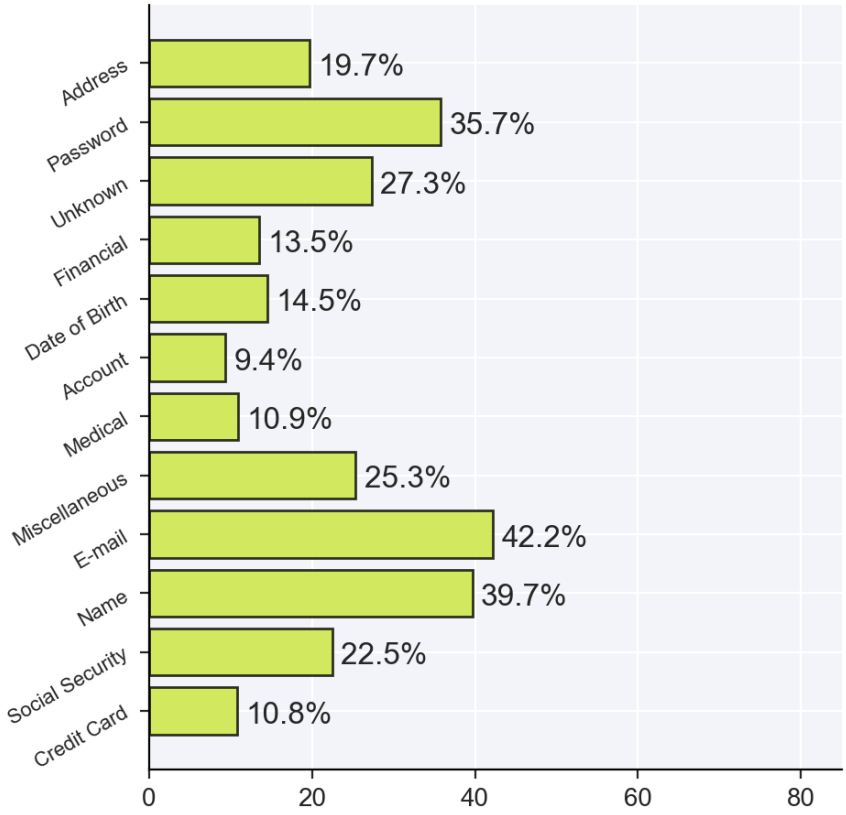


Figure 7: Data types exposed in breaches reported by Q2 2020

Data Type	2020	2019	2018
Email	42%	67%	44%
Names	40%	28%	38%
Passwords	36%	60%	39%
Unknown	27%	9%	13%
Misc.	25%	19%	19%
SSN	22%	15%	21%
Address	20%	13%	22%
DoB	14%	9%	13%
Financial	14%	7%	13%
Medical	11%	6%	9%
Credit Cards	11%	11%	16%
Accounts	9%	11%	8%

Table 1: Top data types lost in breaches reported by Q2 for the past three years

Beyond the increase in the percentage of incidents exposing individuals' names, perhaps the most prominent change is the increase in the percentage of breaches where the type of data exposed is unknown. This is due in part to an increase in the number of incidents where attackers were confirmed to have access to confidential company information, but where the nature of that information was not disclosed. This is often the case with the recent ransomware events that include holding exfiltrated data hostage in conjunction with encrypting systems. Data is confirmed to be in the hands of the attackers, but little is shared about the nature of the information taken.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

A mere five years ago, in the first half of 2015, only six breaches exposed 10 million or more records. Fast forward to 2020 and 33 incidents reported through June 30, 2020 have exposed 10 million or more records. This includes three incidents that exposed over one billion records, 12 incidents that exposed between 100 million and one billion records, and five incidents that exposed 50 million to 100 million records.

While these "mega" events are attention grabbing, these alone should not be taken as the sole indication breaches are becoming more severe. Instead, looking at the number of events by range of records exposed provides more meaningful insight into how many sensitive records are compromised by an "average" breach. By this measure, breaches do appear to be trending toward a greater number of records exposed. As mentioned earlier in the report, two data points stand out supporting this: the median number of records exposed and the percentage of breaches exposing between one and 9,999 records. Focusing on the breaches where the record count is confirmed, we observed:

- Median number of records exposed in the first six months of 2020: 219
- Median number of records exposed in the first six months of 2019: 125
- Percentage of breaches exposing less than 10,000 records in the first six months of 2020: 74%
- Percentage of breaches exposing less than 10,000 records in the first six months of 2019: 92%

What do we conclude from our observation?

Records Lost	Incidents
Unknown	391
1 to 9	17
10 to 99	200
100 to 999	334
1,000 to 9,999	114
10,000 to 99,999	56
100,000 to 999,999	47
1,000,000 to 9,999,999	21
10,000,000 or above	16

Table 2: Number of incidents with records lost in these ranges reported by Q2 2020

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

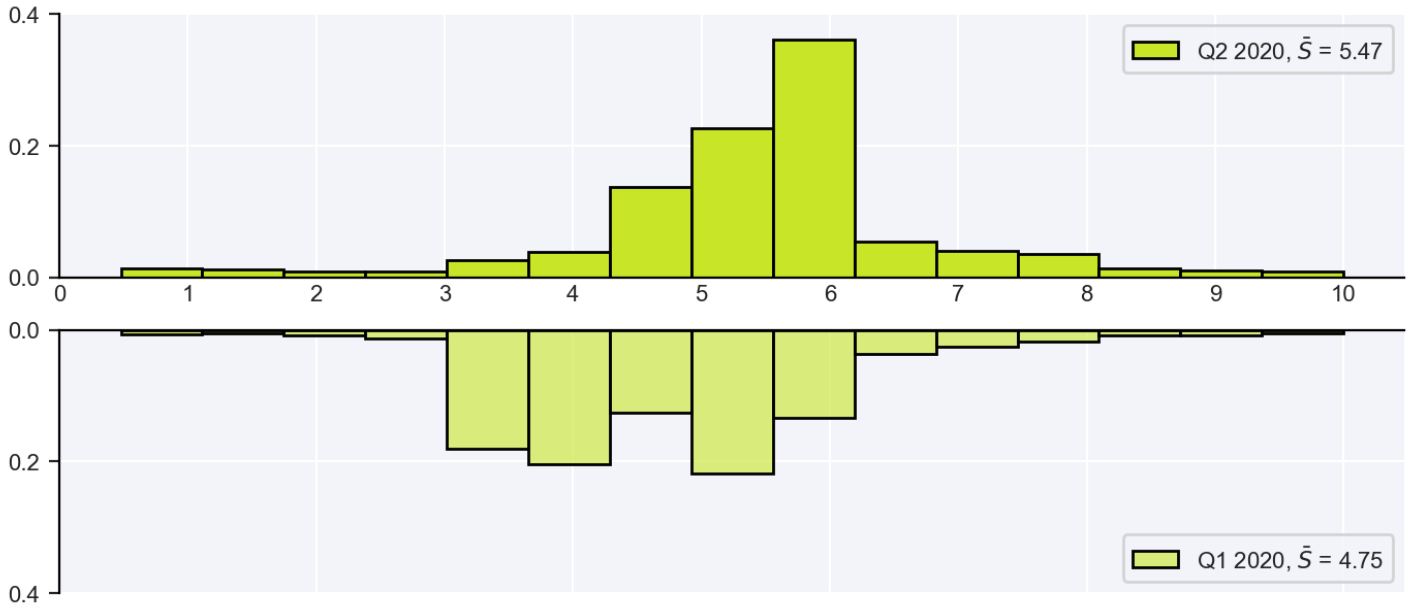


Figure 8: Severity distribution of breaches in 2020 Q1 and Q2

Another option for measuring severity is the individual breach severity score. Breach severity scores are based on a number of factors including how many records are exposed in the event, the type of data compromised, how the breach occurred, and other follow-on actions. This, too, is indicating breach severity is on the rise. The average severity score increased from 4.75 for breaches reported in Q1 to 5.47 for breaches reported in Q2.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Who Was Breached in 2020?

In a near perfect mirror image to the first three months of the year, the Information Sector edged out Health Care services to claim the top spot as the sector reporting the most breaches. For comparison, in the first three months of the year Health Care services was the leader with 106 reported breaches with the Information sector in second place with 104 reported breaches. The difference between these two sectors is how the breach experience is divided among the sub-groupings that make up these sectors. In Health Care, breach activity is fairly evenly distributed between hospitals, practitioners, and other facility or support service providers. In the Information sector, approximately 85% of the breaches originate from software publishers (which includes Software-as-a-Service) and other web-based services.

For readers agile with addition, something might look amiss in this graph. A quick tally of the breach counts by classification comes up well below the 2,037 incidents reported at the outset of the report. So what is the story behind the missing 564 breaches? Unfortunately the responsible organization is not always identified. In some instances, the breached organization may be unidentifiable or is simply not disclosed, as can be the case when an impacted client declines to name the vendor that suffered the breach. Those "**Unknown Organizations**" are removed from this chart as well as the following distribution of impacted business groupings.

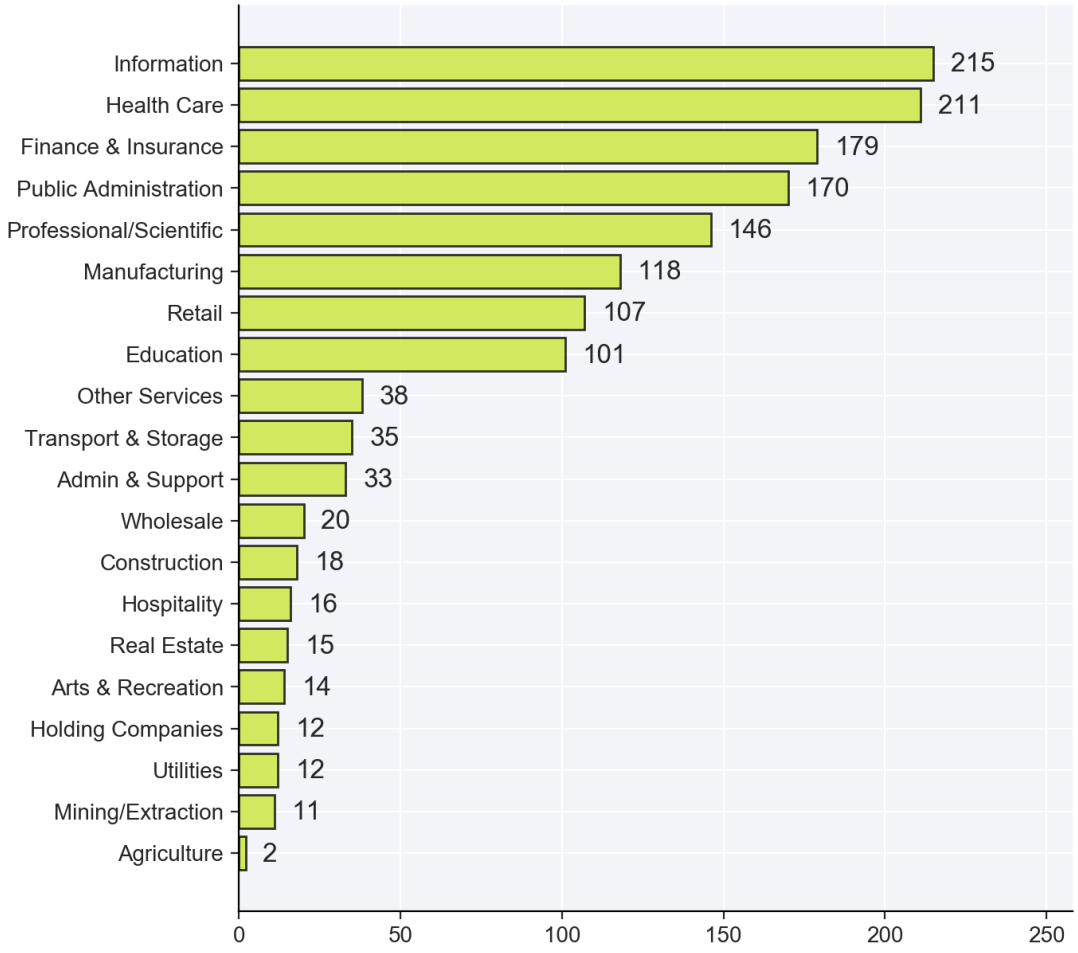


Figure 9: Number of reported Q2 2020 breaches experienced according to economic sectors

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Each Economic Sector is further divided into various sub-groups. A closer look at the Business Groups comprising each sector reveals some interesting differences. In Health Care and Public Administration (i.e. governmental entities) breaches are fairly evenly distributed across the Business Groups that make up these sectors, implying the entire sector faces similar risk factors. Contrast that with the Retail sector, which sees more breaches in Economic Sector 44 in the NAICS system than Sector 45, even with car dealerships and other motorized vehicle dealers removed from the former. It is unclear why there would be such a sizable difference between the Retail sectors. It is possible that there are simply more businesses falling under Sector 44, which includes electronics, home goods, grocery & liquor stores, pharmacies, and clothing stores.

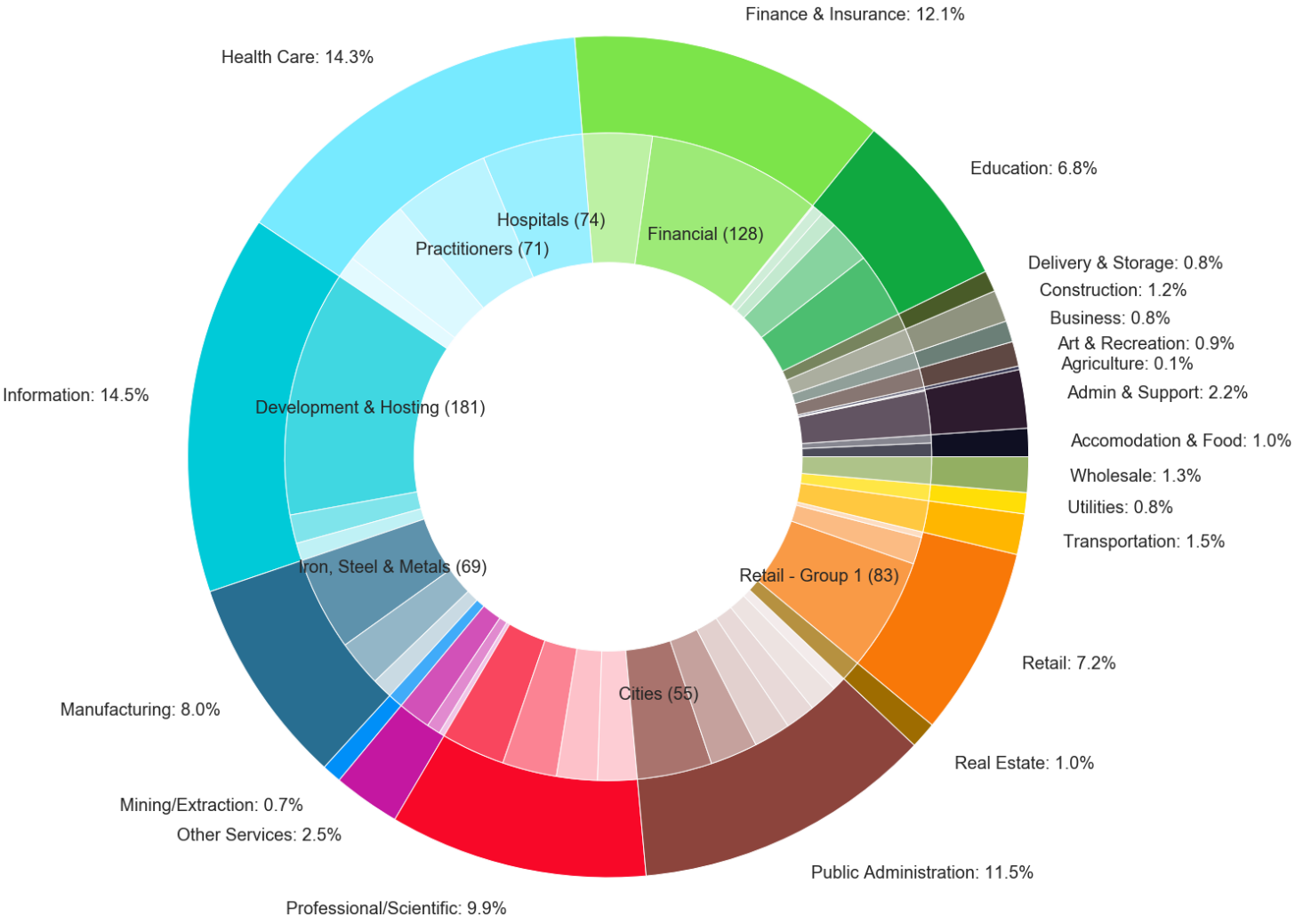


Figure 10: Distribution of breaches by business group and business subgroup, reported by Q2 2020

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Where Did Breaches Occur in 2020?

The large number of data leaks from uncertain locations that came to light in early 2019 impacted the distribution of breach events in the first six months of that year. Comparing 2020 to 2018, however, reveals interesting differences. The percentage of breaches taking place in the United States was comparable, but differences emerged between Unknown Location and breaches taking place outside of the United States. This year, the percentage of breaches between Unknown Location and outside of the United States is fairly evenly split while in 2018, **Unknown Location** was a more significant portion of reported breaches.

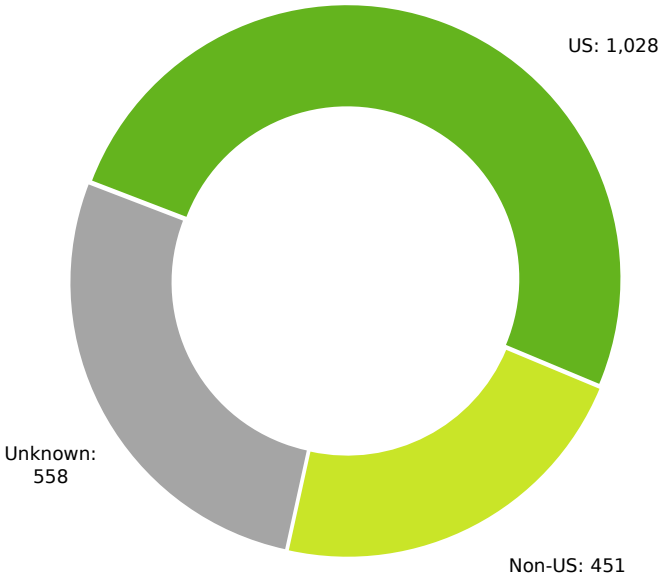


Figure 11: Number of breaches by global location, reported by Q2 2020

First Six Months	United States	Non-US	Unknown Location
2020	50.5%	22.2%	27.4%
2019	28.7%	9%	62.2%
2018	48.7%	11%	40.3%

Table 3: Percentage distribution of breach types by country, reported by Q2 2020

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Do different locations experience different breach types? It's a question that we've been asking ourselves for some time. So for this report we are digging into breach type by location. Our expectation was to see roughly the same breach types occurring across all countries. Looking at the 10 countries with the most publicly disclosed breaches reveals an interesting split. Not surprisingly, unauthorized access to systems or services ("Hacking") is the top breach type regardless of location. However the five countries with the most reported breaches also showed most diversity among breach types, with nearly every breach type in our schema represented. The five countries that make up the second half of the group saw much less diversity, with only three breach types represented: online exposure ("Web"), malware ("Virus"), and Hacking.

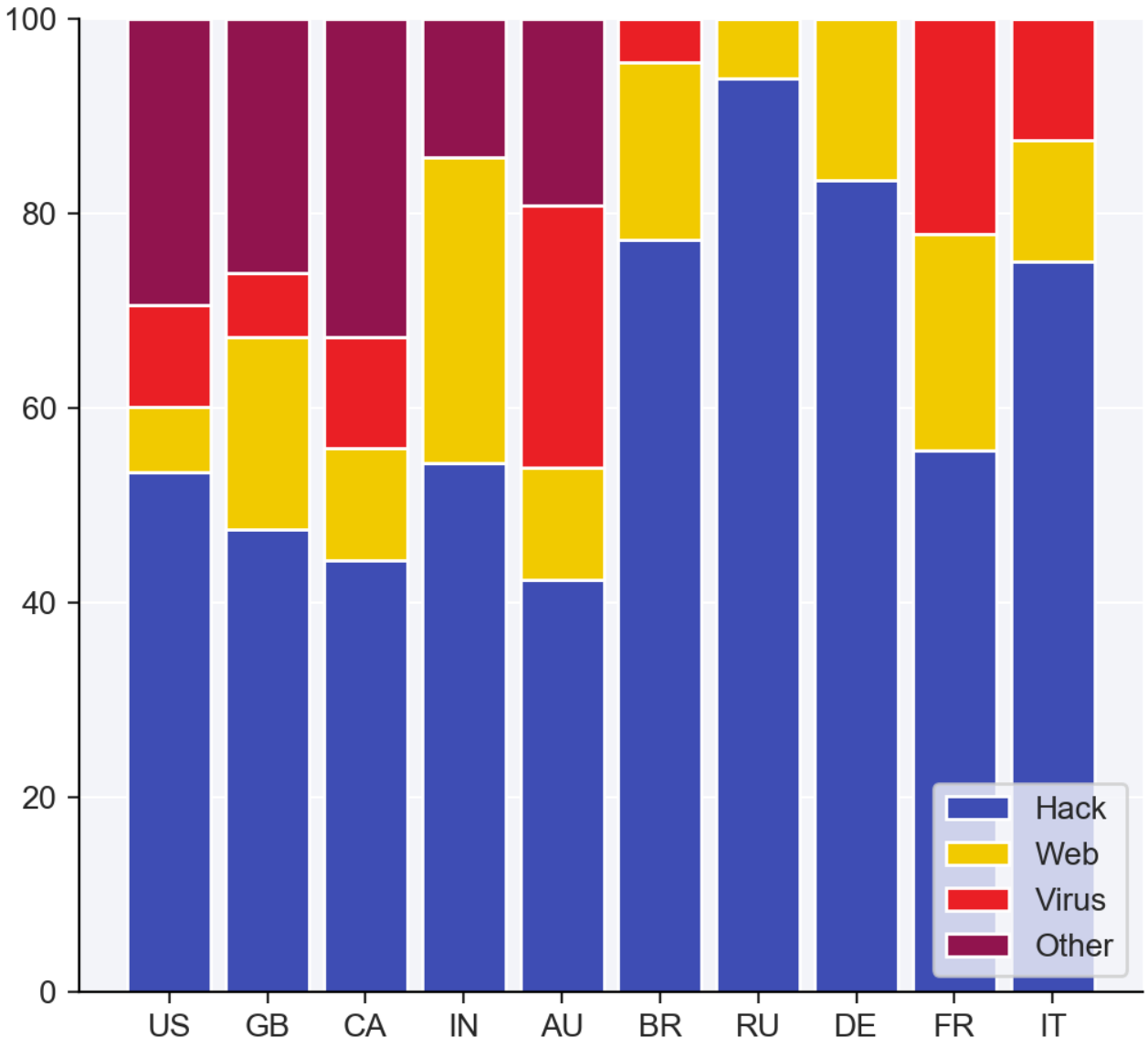


Figure 12: Percentage of breaches by country, reported by Q2 2020

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

In Closing

At the close of the Q1 report, we noted that the narrow three month time period reviewed allowed quirks in the data to bubble to the surface. We predicted that as time went on and the year developed, the effects of short-term fluctuations would moderate and larger themes would prevail. However, the unpredictability of 2020 continues to influence the year. At the start of this report we posed an important question: Why is the breach count low compared to prior years? It was clear early on in the pandemic that breach disclosures were slowing, but it is our belief that slow reporting should not be taken as an indication of less breaches taking place.

What is driving the growth in the number of records exposed? While we expected breach type "Web" to contribute substantially to the number of records exposed, we did not anticipate seeing multiple breaches exposing more than one billion records. We also anticipated that Hacking would continue to account for the highest number of reported breaches, but we are still surprised by the proliferation of incidents combining data theft with encryption in order to maximize extortion threats.

Most importantly, are these permanent changes in the data breach landscape? Our instinct is no, but it may be too early to fully answer that question. It will simply take a little longer to return to "normal." Be sure to tune in for the Q3 Data Breach QuickView Report in October to find out what else 2020 has in store for shaping this most unusual year.

Methodology and 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.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

About Risk Based Security

Risk Based Security (RBS) provides detailed information and analysis on Vulnerability Intelligence, Vendor Risk Ratings, and Data Breaches. Our products, Cyber Risk Analytics (CRA), VulnDB and YourCISO, 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.

For more information, visit www.riskbasedsecurity.com or call +1 855-RBS-RISK.

About Cyber Risk Analytics

Cyber Risk Analytics (CRA) provides actionable threat intelligence about organizations that have experienced a data breach or leaked credentials.

Along with our PreBreach Risk Ratings, this provides a deep dive into the metrics driving cyber exposures, as well as understanding the digital hygiene of an organization and predicting the likelihood of a future data breach.

The integration of PreBreach ratings into security and underwriting processes, vendor management programs, and risk management tools allows organizations to avoid costly risk assessments, while enabling businesses to act quickly and appropriately to proactively protect its most critical information assets.

REQUEST A DEMO
sales@riskbasedsecurity.com

LEARN MORE
www.cyberriskanalytics.com

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.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved