RiskBased SECURITY

2019 Year End Report

Data Breach QuickView

Welcome

Hello and thank you for picking up a copy of the 2019 Year End Data Breach QuickView Report. What a wild year it has been! Readers of the Q1 report will recall that the year started off with a whopping 1,903 reported breaches. That set a record for the most data compromise events disclosed during the first three months of a year. While the pace of disclosures did level off going into the summer months, activity picked up again in the fall, leading to over 7,000 breaches reported for the year. That count, along with the 15 billion records exposed, makes 2019 yet another "worst year on record" for breach activity.

This report covers publicly disclosed data breaches first reported between January 1, 2019 and December 31, 2019. Our analysis of the year in breaches is presented through a variety of charts and commentary, each highlighting a different view into trends that shaped the year. We hope you find this report to be a valuable resource for understanding breach activity and putting a years' worth of headlines into context.

Happy reading!

In This Issue

FEATURING VIEWPOINTS FROM

Inga Goddijn
Executive Vice President,
Risk Based Security

WELCOME

Key Highlights

- In 2019, there were **7,098** breaches reported, exposing over **15.1 billion** records.
- The number of records exposed is ⬆ **284%** compared to 2018, ⬆ **91%** compared to 2017.
- Although the number of breaches in 2019 is only 1% higher compared to 2018, it is anticipated the gap will continue to grow throughout Q1 2020 as more 2019 incidents come to light.
- **Web** (inadvertent exposure of data online) compromised 13.5 billion records while hacking exposed 1.5 billion records. All other data types combined exposed approximately 120 million records.
- Breaches at technology providers pushed the **Information** sector to the top spot for number of breaches, followed by the **Healthcare** sector.
    - 88% of **Information** sector data breaches can be attributed to Software Publishers, Data Processing & Hosting services, and Internet Publishing.
- Risk Based Security's Cyber Risk Analytics team analyzed 25 million unhashed passwords from email accounts affected in the Zynga breach.
    - A breakdown of password security shows that less than 1% of passwords followed basic security requirements.
        - 77% of passwords contain at least half of recommended requirements.
    - Of the passwords analyzed, Gmail users tended to have slightly more secure passwords compared to other email domains.
    - Of the passwords analyzed, AOL users tended to have the least secure passwords compared to other email domains.

Breaking Down Healthcare's "Wall of Shame"

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.

The healthcare sector landed in second place for the number of breaches in 2019. This trend started earlier in the year leading to a number of media outlets highlighting security issues across the healthcare industry and the copious number of records compromised at a wide variety of service providers.

One such article detailing healthcare data breaches caught our eye. According to their source the total number of breached healthcare records stands at 38 million, which would be 11.64% of the US population. That's an alarming statistic that is hard to ignore, especially when we consider the treasure trove of sensitive information that healthcare providers have on their patients. Providers can hold everything from basic contact details and insurance information to family histories, diagnosis, medications taken… and perhaps even a blueprint of your DNA. As we've argued before, you can replace your credit card, but you can't get a new body.

This 11.64% statistic is designed to catch your attention over your morning coffee. It's alarming and yet plausible. It's also worth exploring further, because it may not be entirely representative of what is happening. We are not claiming that the referenced article is wrong. Instead, what we are saying is that the figure may be even larger (or smaller) than reported.

THE BUILDING BLOCKS OF THE "WALL OF SHAME"

Better risk management requires better data. That's a core value, here at Risk Based Security. In this case, that means understanding where breach data is coming from. The cited 38 million records exposed comes from one source, the U.S. Department of Health and Human Services Office for Civil Rights breach portal, commonly referred to as "The Wall of Shame." This wall is composed of breaches of unsecured protected health information, but with the following stipulations:

- The breach must affect 500 or more individuals; and
- The incident occurred at a 'covered health entity.'

500 OR MORE INDIVIDUALS

If the incident did not affect 500 or more individuals, it is not published to the list. This means the list alone is not fully representative of the breaches occurring across the healthcare industry. There are many smaller data breaches that occurred throughout the year which are not included in the report, meaning the actual number of incidents is much higher.

COVERED HEALTH ENTITIES

A breach has to apply to a 'covered health entity' to make the list. That means the breach would have to occur at a health insurance plan, a healthcare provider, or healthcare clearinghouse.

At first glance that might seem logical, however medical service providers are not the only organizations that can have healthcare related data. Consider how much medical information can be collected – whether intentionally or not – in personnel files and communications between employees. Doctor's notes, diagnosis details and injury reports can easily make their way into a company's email system and files. Should those systems or files be breached, and the information is lost to malicious attackers, the breach most likely won't make it to "The Wall". So the total of 38 million healthcare records exposed would not necessarily include all breaches of healthcare data.

WHAT DO WE MEAN BY "HEALTHCARE" RECORDS?

Putting aside the under-reporting, we also need to ask ourselves what is meant by "healthcare records" in the first place. For most readers, when you see 38 million "healthcare" records lost, you associate that with **actual** medical data – such as condition and medical history. But with how the "Wall of Shame" is designed, that association is not entirely accurate. In reality, those 38 million records lost may well contain something other than sensitive diagnosis or treatment information.

Health and Human Services has made it clear that protected health information – which must be breached for an incident to be posted on the "Wall of Shame" – is more than a physical or mental health condition. It includes demographic information as well as "many common identifiers" such as name, address, date of birth and Social Security number.

Because "The Wall" is not clear as to the specific data types exposed in the breach, the compromised information will include a mix of data. Yes, if malicious attackers know 11.64% of all American's medical diagnosis and medical history, something must be done **now** to rectify this. But if attackers have compromised the names and addresses of 11.64% Americans within Healthcare systems, it's less of a call-to-arms.

THE REASON IT IS DIFFICULT

Making these distinctions is difficult and it is not our goal to discredit the Wall of Shame as a source of information or the article that referenced it. More information, and more transparency, is a positive. However, there is always more to the story when considering information from only one source. There are grey areas when it comes to breaches, complicated by the fact that what ends up posted on a public list can vary widely depending on who is doing the reporting and the reason the information is being published. Without understanding the regulation driving the disclosure or the selection criteria of the organization publishing the list, it is easy to make assumptions that lead to inaccurate conclusions.

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
www.cyberriskanalytics.com

Data EVERYWHERE

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.

2019 was a rough year for breach activity. The numbers really do speak for themselves with reported breaches reaching an all-time high and the number of records exposed up 284% compared to 2018. As ghastly as those numbers are, there is much more to the story of 2019 and it's not entirely bad news. One such bright spot is that the number of incidents where sensitive data was accessible, but not confirmed as taken, increased to 22.6% of breaches compared to 18% at the close of 2018. Another interesting nuance is that there were three breaches that compromised 1 billion records or more exposed transaction logs. So while the total number of unique records exposed was very high for these events - 7.6 billion to be exact - the number of individuals whose data was put at-risk is far less.

With that said, let's take a closer look at the trends that shaped the year, and shed a little more light on data behind the numbers.

WHAT'S IN YOUR ~~WALLET~~ EMAIL ACCOUNT?

The practice of targeting employee email accounts hit new heights in 2019. It was a scenario that played out in a similar manner across different industries and organizations of all sizes. Attackers used phishing emails or click bait to lure users into giving up access to their email account. Once in, malicious actors were free to explore the content and contacts of the account holder.

These events can be time-consuming, resource-intensive incidents to remediate. The breach at Children's Hope Alliance (CHA) illustrates just how challenging it can be to sort through the aftermath of this type of intrusion. Consider this timeline:

April 23, 2019 – Unauthorized access to CHA email accounts begins

May 15, 2019 – CHA became aware of suspicious activity on one account and launches an investigation

May 20, 2019 – All compromised accounts secured; work gets underway on determining what information was contained in emails

July 20, 2019 – CHA confirmed the compromised accounts held sensitive data

August 1, 2019 – CHA begins notifying business partners who may have provided the sensitive data to Children's Hope; a list of potentially affected individuals is created, but it requires substantial de-duplication and is missing addresses for notification

September 10, 2019 – Contact list is clean and ready for use

September 26, 2019 – CHA begins mailing notification letters to affected persons

That's 134 days from discovery to finally being able to alert those that may have had their data accessed by attackers. Or in other words, Children's Hope Alliance spent one third of the year in response to 27 days of unauthorized access to emails.

RANSOMWARE STRIKES BACK

Looking over the year it can be hard to believe that ransomware was once relegated to the back of the list of security concerns. Extortion malware has gone through a renaissance in recent years culminating in a fair amount of havoc in 2019. 11.5% of the breaches covered in this 2019 report included a ransomware component. Some organizations were lucky, emerging relatively unscathed from the experience. Others fared much worse.

As we observed in last quarter's report, cyber insurance can play an important role in softening the financial pain of a security event. This is especially true when it comes to extortion events. Rockville Centre Union Free School District showed how valuable a resource it can be after suffering a Ryuk infection in late July. After collaborating with their insurance carrier, the District and the insurance company concluded that obtaining the decryption keys would be the most effective path to recovery. The insurance carrier negotiated with the attackers and paid $78,000 of the final $88,000 extortion demand.

Where will ransomware go next? Events like the November incident at Allied Universal and the December incident at a CyrusOne data center suggest we should expect malicious actors to leverage the threat of leaking data in order to ratchet up the pressure to pay – *and actually follow through on that threat*. The group behind Maze ransomware used this tactic with Allied Universal. After Allied failed to come to terms with the actors, 700 MB worth of stolen data was released online.

Three weeks after the Allied Universal event, news broke that the group behind REvil/Sodinokibi ransomware was following form and threatening to release data exfiltrated from CyrusOne. We have not been able to confirm whether that data was in fact leaked, but by January of this year the group did follow through on the threat by leaking information allegedly belonging to Artech Information Systems.

TOMAYTO, TOMAHTO

As mentioned in the opening, 2019 saw three breaches that compromised 1 billion or more transaction log records. That statement highlights how important it is to understand the data behind reports such as this one. After all, without insight into what the data actually represents it can be easy to misconstrue what it's telling us. In our schema, a "record" is not synonymous with a "person". There are certainly many breaches where the record count is the same as the number of people affected. But as events like those at Orvibo and LightInTheBox show, there will be breaches that impact more records than people, just as there are breaches that impact more people than records. We explored the intricacies of understanding data in the previous section of this report, taking a much closer look at one popular source of information, the U.S. Department of Health and Human Services Office for Civil Rights breach portal.

Speaking of data, we've done something special for this report. Regular readers won't be surprised to see that once again, access credentials in the form of email addresses and passwords dominate the types of data most compromised. We've mined our rich dataset of plaintext passwords to bring a fresh look at what we can learn from analyzing this data.

We hope you enjoy the analysis as much as we enjoyed putting it together.

Data Breach Trends in 2019

Bigger is definitely not better when it comes to data breach events. Unfortunately, in many ways the same data loss patterns present at the close of 2018 are still with us at the end of 2019, only more so. More breaches reported, more data exposed, and more access credentials dumped online. Throughout this report, we explore various perspectives on the breaches that were publicly disclosed in 2019, including analysis of the types of data lost, how the data was exposed, where events are taking place, and what types of organizations were impacted.

2019 At A Glance

Figure 1: Number of breaches reported each year

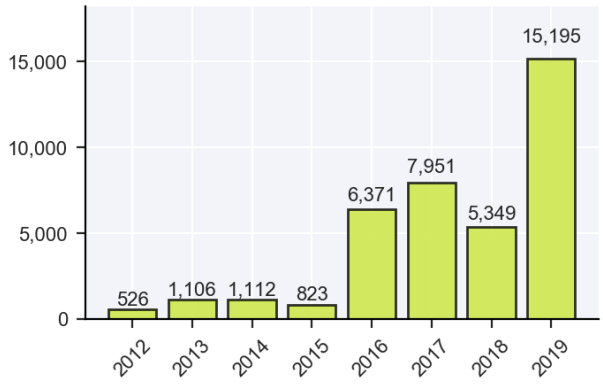

Figure 2: Number of records lost (in millions) each year

As predicted in the Q3 report, the number of breaches disclosed in 2019 once again hit an all-time high. It's worth noting that 2019 incident reports were still trickling in at the time this report was created. Some lag time is typical as information can be slow to develop. Looking back at the patterns from the prior three years, we anticipate another 250 - 300 incidents will be added to 2019. Meaning, the difference between the 2018 and 2019 breach counts will grow in the coming months.

Readers of the Q3 report will also notice the extraordinary jump in the number of records exposed during the last three months of the year. 7.2 billion - yes billion - records were compromised between October 1 and December 31st. Four events in particular accounted for 93.5% of those 7.2 billion records. All four of these breaches were caused by open, misconfigured databases made publicly accessible to anyone with an interest in finding them.

While these data leaks may appear more annoying than threatening, interest in finding these rich sources of information shows little sign of abating. Security researchers and malicious actors alike have made good use of the various tools for finding, analyzing, and downloading databases. Thanks to the combination of low risk of detection and low barrier of entry for this type of activity, we anticipate open, unsecured data will continue to be an issue well into the new decade.

The top breach types by number of incidents and number of records exposed illustrates just how challenging the practice of security is. For several years now, more records have been exposed due to misconfigured services than any other breach type. It's true we see our fair share of organizations - or their vendors - that clearly dropped the ball when it comes to basic hardening practices. But we also see this type of breach taking place at organizations with solid security programs. Rather than subpar practices, there is simply a mistake made, a loop not closed, or a box not checked on an update or change that inadvertently leaves data exposed for a short period of time.

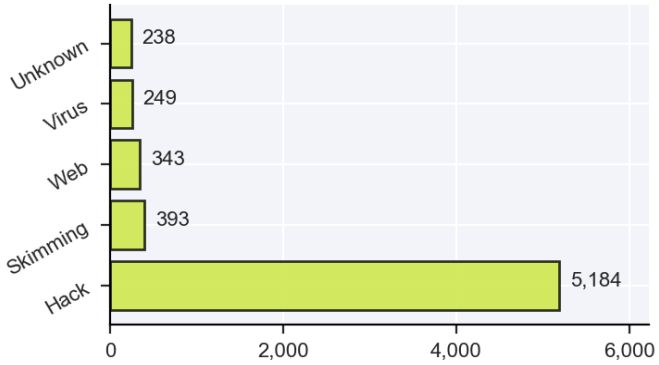

Figure 3: Number of breaches by breach type, reported in 2019

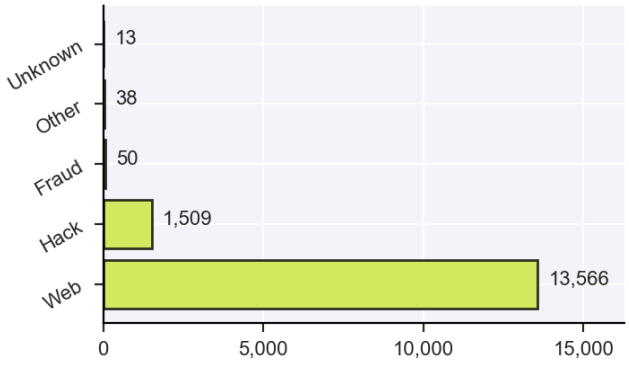

Figure 4: Number of records lost by breach type (in millions), reported in 2019

As the data shows, there are plenty of malicious actors ready to take advantage of any and every shortcoming or oversight. Hacking, defined as unauthorized intrusion into systems, has been the top breach type by number of incidents for every year of the past decade except for 2010.

Our research includes the tracking of the actor's position relative to the breached organization. In other words, was the breach due to an employee stealing sensitive information or perhaps accidentally sharing the data, or was the breach triggered by the actions of outsiders? With Hacking as the top breach type, it's not surprising that outsiders are by far the leading source of data loss incidents.

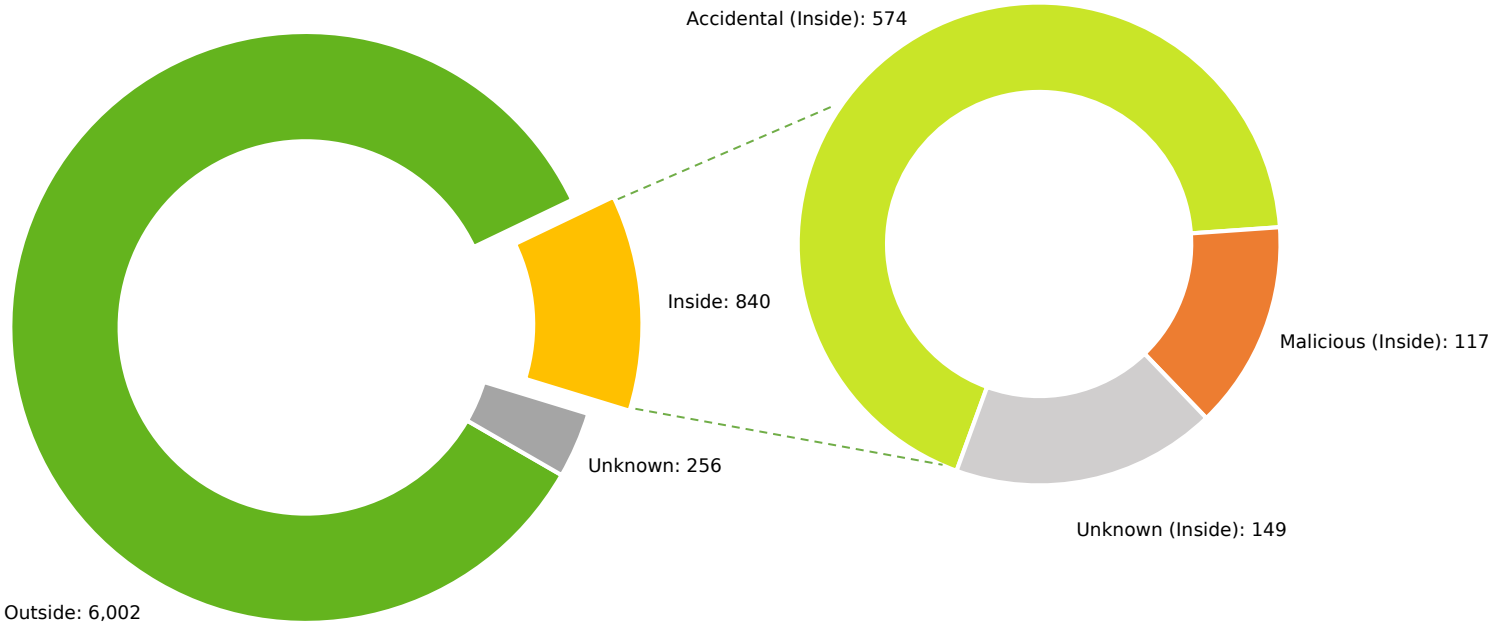

Figure 5: Number of breaches by attack vector, reported in 2019

If data is lost in the forest and no one is there to see it, was it really a breach? Certainly! But clearly not all breaches pose the same level of risk to those that have had their data exposed. This year, compromised organizations (or at least the attorneys and Public Relations professionals drafting their notifications) went to great lengths to emphasize whenever there was uncertainty around whether data was taken or merely accessible. While we applaud sharing as much information as possible about the event, there is a difference between a spreadsheet on a missing laptop and months of access to multiple employees' email accounts.

(Pass)Words with Friends

Since 2012, access credentials in the form of email addresses, usernames and passwords have been the top data types compromised. It is easy to understand why. Obviously they are a key ingredient for accessing users' accounts, but they are useful for much more. Leaked credentials taken from one source, such as the September breach at Zynga, are frequently used in brute force attacks and targeted phishing campaigns. Analysis of such leaks can also lead to valuable insights. In the next section, we take a deeper dive into this data and share our observations.

On September 12th, news broke that Zynga, the company behind Words with Friends, had been hacked. The attack exposed data on millions of players including names, phone numbers and login information. Much has been said and written about the need to strengthen passwords in recent years. With the Zynga data, we saw an opportunity to investigate the question, "Are passwords getting better?"

A straightforward analysis of the top 10 passwords present in the leak shows that there has been very little movement away from weak, easy to guess passwords. In fact, "password" came in at the top spot, followed by ubiquitous number sequences. The presence of "words" in the #6 spot is disheartening. Not only is it a weak choice, it's taken directly from the name of the service.

It is worth noting, our analysis is based on a pool of **unhashed** passwords, meaning these may be representative of passwords that are **particularly easy to unhash**. With that in mind, let's take a look at what we saw.

Top 10 Passwords in the Zynga Breach
10. changeme
9. 12345
8. qwerty
7. 12345678
6. words
5. 123123123
4. 123456
3. 1234567
2. 123456789
1. password

Table 1: Top 10 passwords in the Zynga breach

Password Strength

There is no shortage of advice on how to create a strong password. It's common knowledge sequences and keyboard patterns should be avoided - we're looking at you, "qwerty"! Google suggests account holders consider using song lyrics, a favorite quote, or series of words that are meaningful to the user. Others suggest using a random password generator or better yet, using a password manager to corral the entire process.

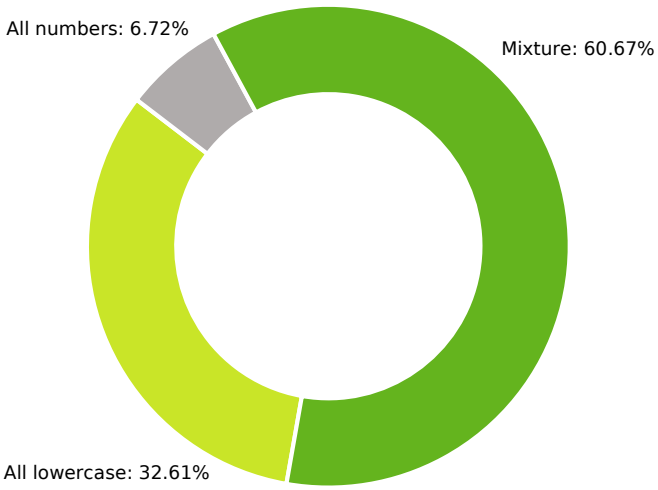

Figure 6: Proportion of passwords containing all numbers or all lowercase letters

Conventional wisdom suggests passwords should be at least 8 characters long - though the trend is moving toward 12 or 15 characters - containing both upper and lower-case letters and a mix of numbers and symbols, and not contain a substring of the users name, email address or the service being accessed.

Granted, a lighthearted pastime such as Words with Friends may not provoke much thought about password strength. That said, just how close were the Zynga passwords to meeting the mandates of conventional wisdom?

The answer, not very close at all. Of the passwords analyzed, about 33% were comprised of all lower-case letters and 7% were number strings. About 61% of passwords contained a mix of lower case letters and numbers, but only 1% included a symbol.

Less than 1% of passwords contained all six of the suggested qualities. Figure 8 shows how many passwords contain a combination of password mandates. 77% of passwords cap at having at least three qualities, dropping down to about 47% at four, and falls even further to 11% at five.

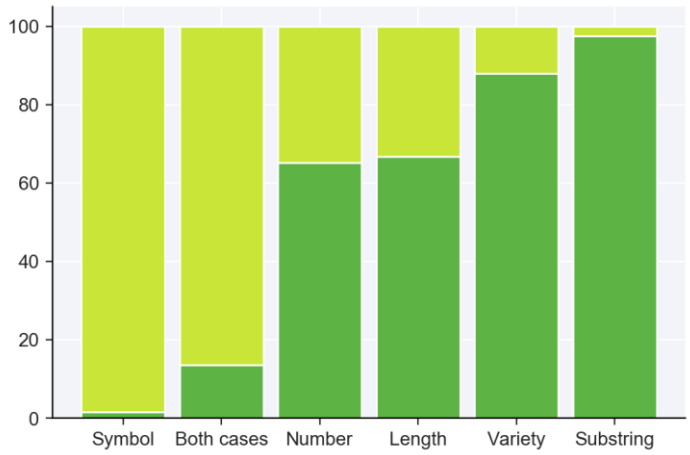

Figure 7: Proportion of passwords that meet each requirement

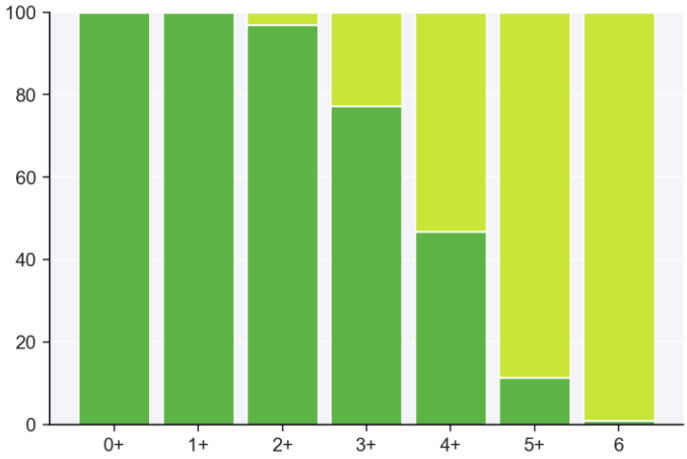

Figure 8: Proportion of passwords that meet a minimum number of requirements

Can the email domain tell us something about account holders' proclivity for more secure passwords? The answer is yes.

Assume that each one of the 6 conventional characteristics were equally important to the overall strength of the password. The average security of a given password would score 3.33 out of a total possible score of 6.

Domain	Average Security Score
@gmail.com	3.39
@yahoo.com	3.33
All domains	3.33
@hotmail.com	3.29
@aol.com	3.25

Table 2: Average score given to breached email domains

Domain	Average Security Score (RBS-Weighed)
@gmail.com	.5312
All domains	.5199
@yahoo.com	.5191
@hotmail.com	.5126
@aol.com	.5019

Table 3: RBS weighed score given to breached email domains

Applying the above scoring method to the passwords in the Zynga breach, we see that Gmail users tended toward slightly more secure passwords while AOL users tended to have the least secure passwords.

An argument can be made that valuing each characteristic equally fails to recognize that some strategies are more useful for strengthening passwords than others. After all, a string of 8 or more random letters is probably a safer bet than "Letm3in".

Weighting each of the characteristics produced similar results. We choose to add value for longer passwords and the inclusion of a number or symbol and devalue weak character uniqueness and substrings. Following this method Gmail users were creating stronger passwords while AOL users trailed behind, still.

As noted earlier, our analysis is based on a pool of **unhashed** passwords. The full Zynga leak included approximately 213 million rows of data. This included duplicates as well as some records that appeared to be test or "dummy" accounts. Our analysis focused on a subset of the full leak, consisting of 25 million records. The domains represented in the sample are illustrated in Figure 9.

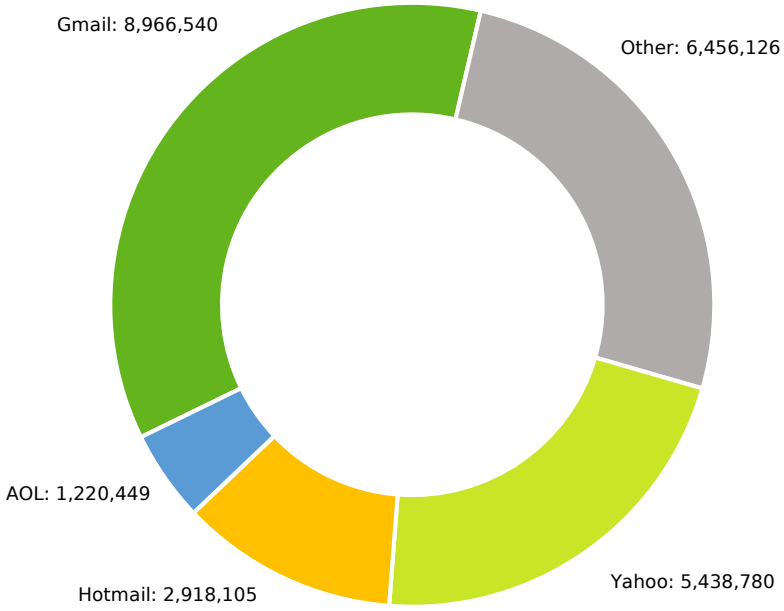

Figure 9: Breakdown of 25 million email accounts affected in the Zynga breach

Government and Military Email Domains Playing Words with Friends

25.8% of domains in the studied dataset were identified as something other than belonging to the four major consumer email service providers. We took a closer look into the "others", and wondered - how many were government email addresses? Many commercial organizations frown on the practice of using work email addresses for personal pursuits. Governmental entities have a reputation for being particularly finicky about using official assets for civilian use. Despite these constraints, we identified 8,360 email addresses belonging to .gov domains (separated by country in Table 4) and 3,935 to the U.S. military (.mil).

Countries	Number of Emails
Australia	4,028
United States	3,721
United Kingdom	285
Other	266
Brazil	32
New Zealand	28

Table 4: Emails belonging to governmental entities

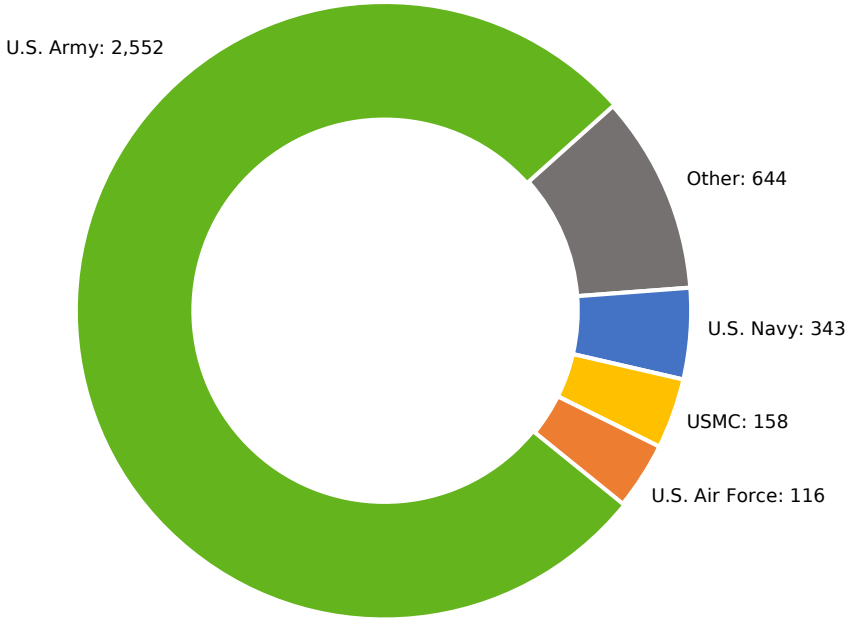

Figure 10: Breakdown of U.S. military emails affected by the Zynga breach

Information Sector Takes Top Spot for Number of Breaches

The U.S. Census Bureau, which is responsible for the North American Industry Classification System, or NAICS for short, defines the information sector as establishments engaged in:

a) producing and distributing information and cultural products

b) providing the means to transmit or distribute such information or cultural products; and

c) processing data.

In short, this sector applies to organizations as diverse as traditional newspaper publishers to satellite telecommunications.

Three subgroups within the Information sector - Software Publishers, Data Processing & Hosting, and Internet Publishing - accounted for 88% of the breaches in the Information sector.

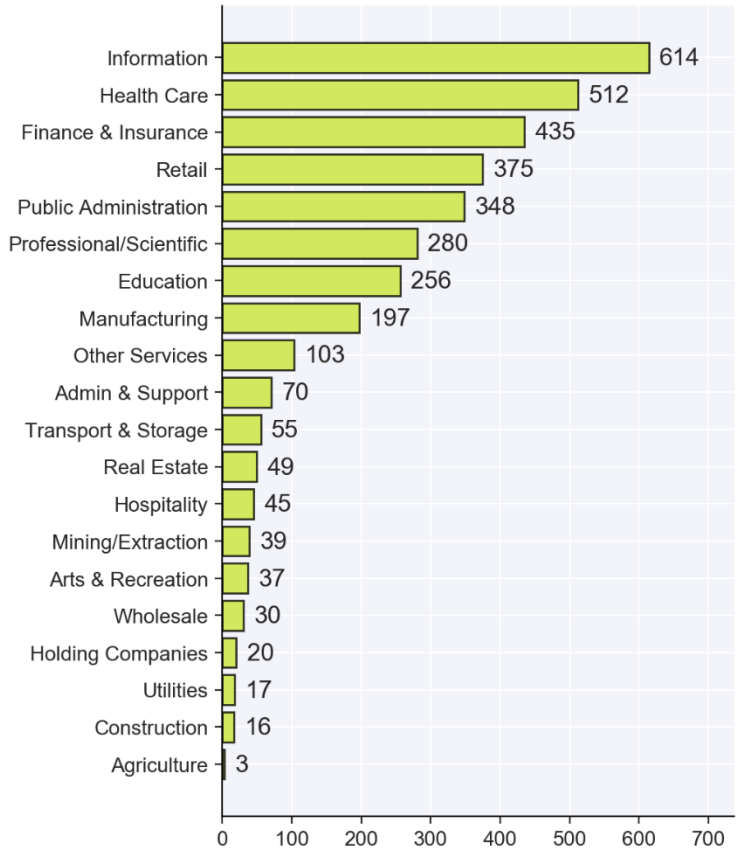

Figure 11: Number of breaches per economic sector, reported in 2019

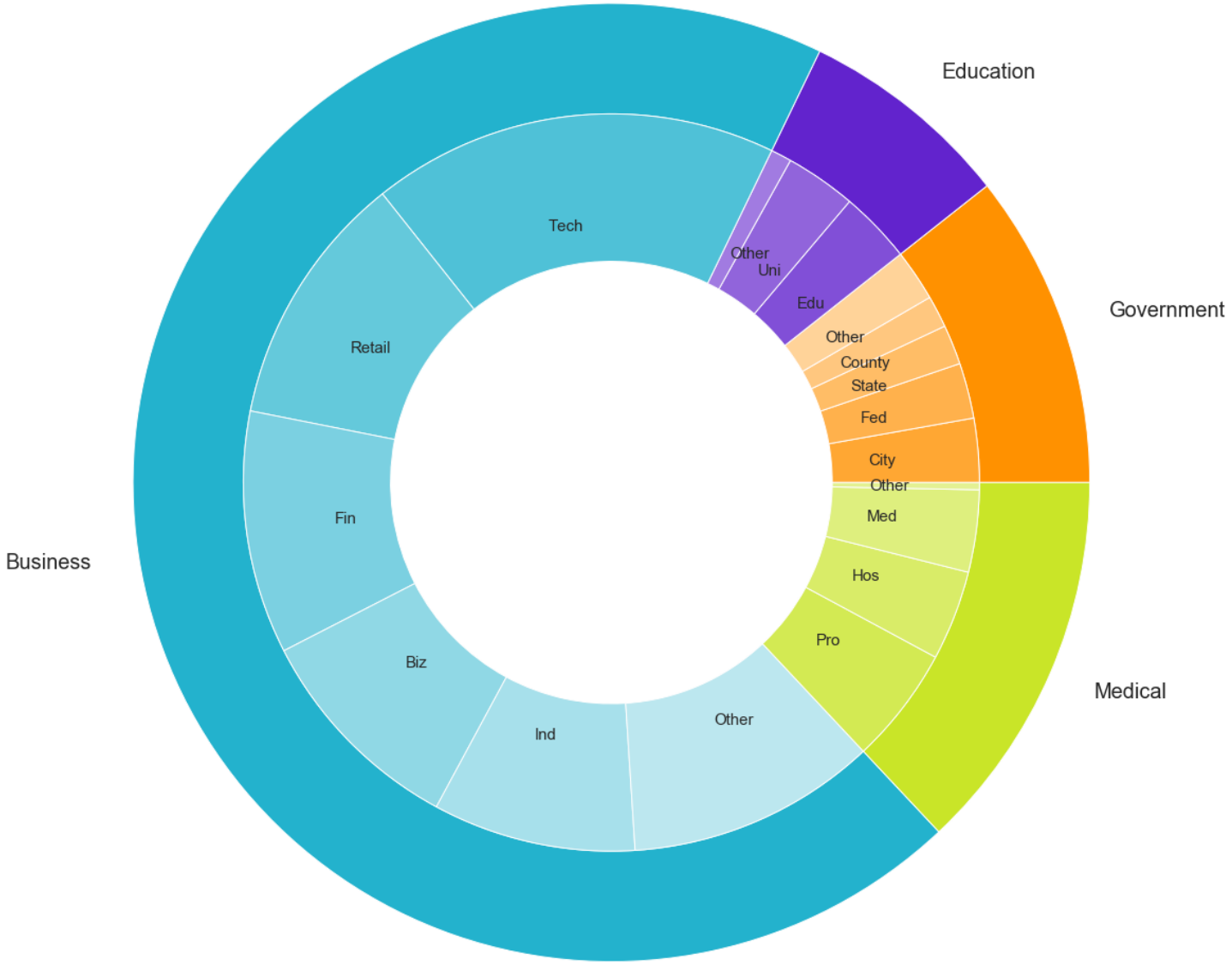

Figure 12: Distribution of breaches by business group and business subgroup, reported in 2019

Stepping back for a different view, General Business accounted for 69% of reported breaches, Medical 13%, Governmental 10.5%, and Education 7.2%.

Where Did Breaches Occur in 2019?

The majority of publicly disclosed breaches are in the United States. It's worth noting that strong notification laws across the US drive the number of reported events. Why is the breach location unknown for so many events? There are a number of reasons including the responsible party going unidentified or the breached entity operating across multiple jurisdictions.

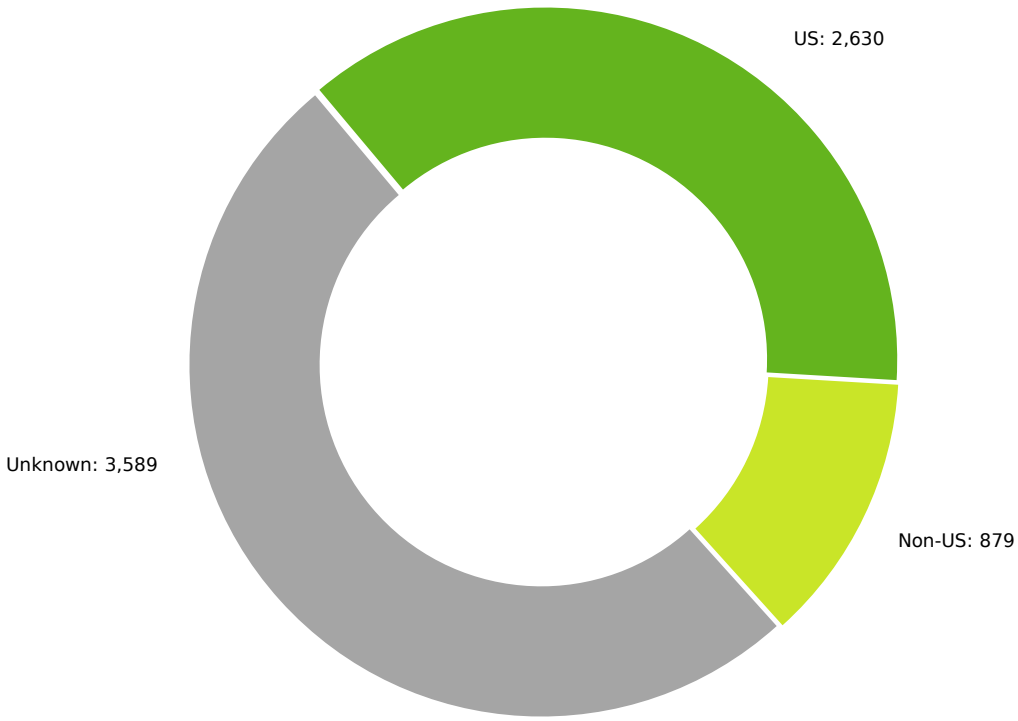

Figure 13: Number of breaches by global location, reported in 2019

Third Party Breaches

In our schema a single data loss event is considered one breach, regardless of how many entities may have been impacted. Events that expose data belonging to business partners or clients are referred to as third party breaches. This means a 'steward' organization tasked with responsibility for securing data lost control of the sensitive information, impacting upstream entities. 2019 saw one of the largest third party events on record. Attackers targeted Pearson Clinical Assessments, capturing students' names, dates of birth and email addresses from approximately 13,000 schools and universities.

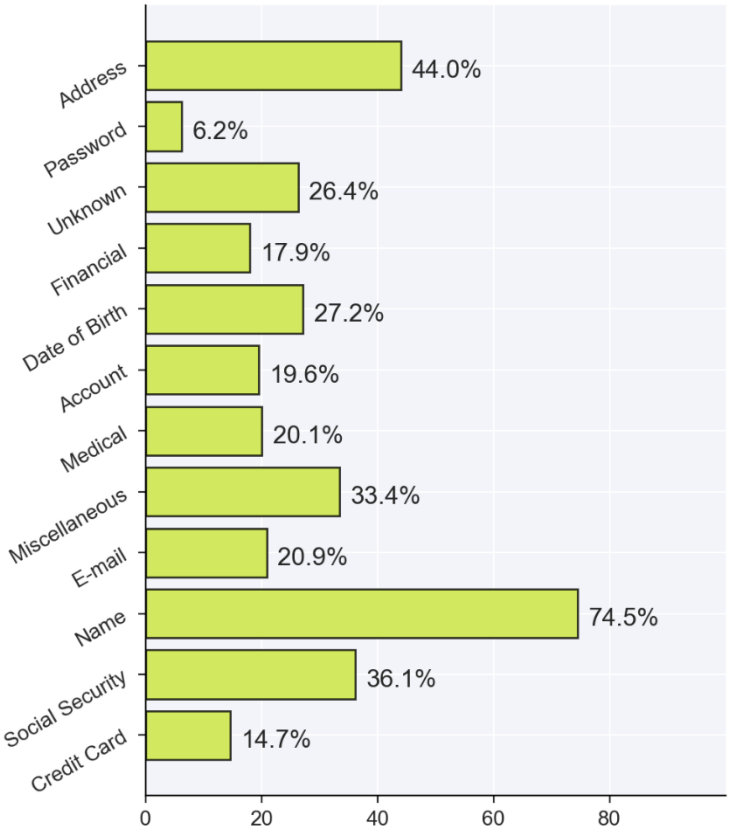

Figure 14: Types of data lost by third party breaches, reported in 2019

In keeping with the overall trend for 2019, the number of records exposed in third party breaches skyrocketed. The average number of records exposed in these breaches was just short of 13 million records per breach and the 4.7 billion records exposed was approximately 273% above 2018.

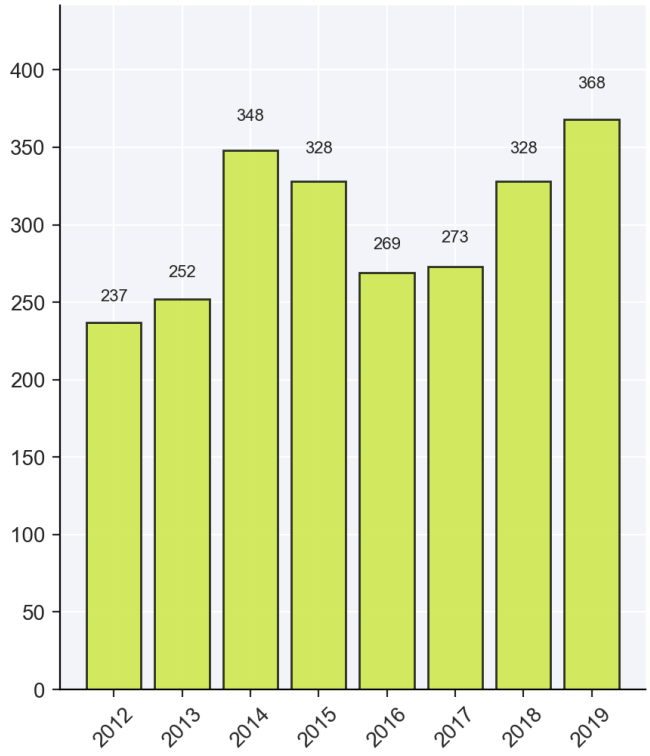

Figure 15: Number of third party breaches, reported in 2019

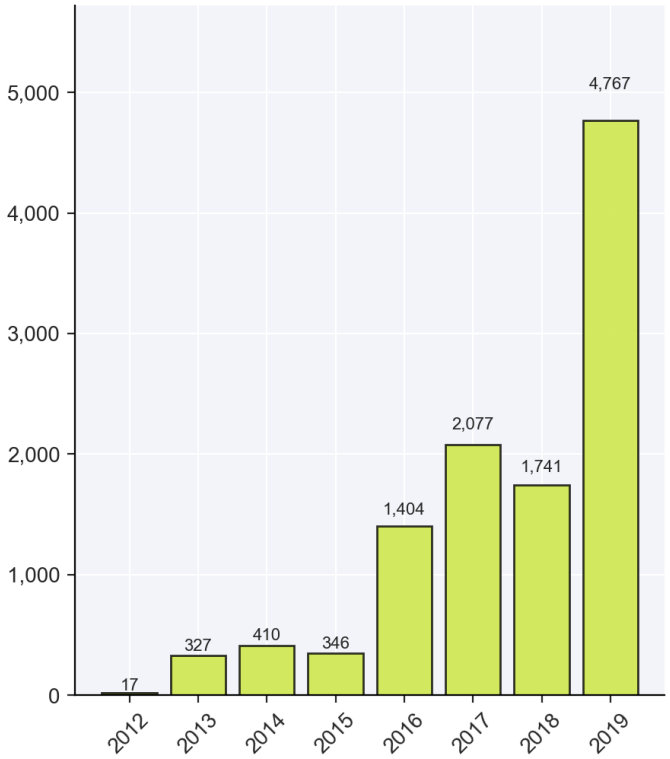

Figure 16: Number of records lost (in millions) from third party breaches, reported in 2019

In Closing

Looking back at the start of the decade, there were 986 reported breaches exposing 102,646,498 records in 2010. It only took two years to more than double the number of breaches - 2012 jumped up to 3,335 reported breaches - and by 2016 the number of records exposed was consistently over the 5 billion mark. Looking ahead, we see little indication of improvement. In fact, it's quite the opposite. Low complexity phishing attacks show no sign of slowing, malware is as virulent as ever, and the black market for stolen data continues to thrive. Tune in for the Q1 Data Breach Report in early April to see how these trends play out into the new decade.

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.

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.