Data Breach QuickView Report
2019 Q3 trends
Issued November, 2019
Welcome

Hello and welcome to the Data Breach QuickView Report. Regular readers of our reports will notice things are looking different with this edition. Indeed, we've done a bit of remodeling, rearranging the proverbial furniture and adding some splashes of color, but rest assured the same great breach intelligence still forms the foundation of this report.

This quarter we're pleased to introduce a new Viewpoints section to complement our customary analysis of data compromise events. With the endless stream of breach announcements, it's easy to lose sight of the larger trends and interesting events that shaped the quarter. The new section offers an opportunity to take a step back and reflect on incidents that cut through the noise and embody the bigger picture.

The Q3 2019 Data Breach QuickView Report covers the data breaches reported between January 1 and September 30, 2019. The analysis is displayed in a sampling of charts highlighting breach trends by the numbers. We hope you find this helpful and insightful reading.

Enjoy!

Key Findings

- There were 5,183 breaches reported in the first nine months of 2019 exposing 7.9 billion records.
- Compared to Q3 2018, the total number of breaches was up 33.3% and the total number of records exposed more than doubled, up 112%.
- Hacking remains the top breach type for number of incidents while Web has exposed the most records this year.
- By NAICS economic sector, medical services, retailers and public entities experienced the most breaches, but when all business related sectors are combined, general business remains the most breached organization type.
- In Q3 alone, six breaches exposed 100M or more records, accounting for 3.1 billion records exposed between July 1st and September 30th.
- Accounts vs People vs Records - Orvibo, the largest breach disclosed so far this year, is reported to have exposed approximately 2 billion records. It is worth noting the open dataset included approximately 2 billion entries that were associated with a much lower number of user accounts. The actual number of user accounts exposed in the breach is unknown but is likely to be around one million, as that is the number of customers claimed by Orvibo.

Inga Goddijn
Executive Vice President,
Risk Based Security
In This Issue

FEATURING VIEWPOINTS FROM

Inga Goddijn
Executive Vice President,
Risk Based Security

Jake Kouns
Co-Founder, CISO,
Risk Based Security

WELCOME

In This Issue .................................................................................................................................................. 3

Viewpoints ....................................................................................................................................................... 4

Some Truths Remain Unchanged ................................................................................................................. 4
Integrating Cyber Insurance Into a Risk Management Program ................................................................. 6

Data Breach Trends Through Q3 2019 ........................................................................................................... 10

Q3 2019 At A Glance .................................................................................................................................. 10
Who Has Been Breached Through Q3 2019 .............................................................................................. 14
In Closing ...................................................................................................................................................... 17
Methodology and Terms .............................................................................................................................. 18
Data Standards and the Use of “Unknown” ................................................................................................. 18

About Risk Based Security .......................................................................................................................... 19

About Cyber Risk Analytics ........................................................................................................................ 19

No Warranty ................................................................................................................................................ 19
Some Truths Remain Unchanged

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.

We produced our first Q3 Security Intelligence Report back in October of 2011. Looking through that report I'm reminded of the saying, “the more things change, the more they stay the same.” Back then, it wasn't clear we would see more than 1,000 reported breaches and the total number of records exposed had barely crossed the 200 million mark. However, 2011 ended with over 1,300 reported breaches and 420 million records compromised. While it appears that the breach landscape has changed radically since that time, some truths remain unchanged. Unauthorized access into systems (“hacking” in our report) remains the top breach type by number of incidents, the majority of breaches still originate from outside of the organization (although insider events remain exceptionally damaging), and malicious actors continuously seek out opportunities to make a fast buck.

HELPING OUT THE HACKERS

Hacking has been the primary force driving increasing breach counts for the past eight years. Indeed, we have to look back all the way to 2010 to find a different breach type taking the top spot (it was fraud) and even then, hacking was a close second. Have our defenses performed so poorly when it comes to keeping up with the bad guys? There are plenty of points to be made on both sides of that argument. However, as we look over the experience of 2019 what stands out is that we are often our own worst enemy. Whether it's a phishing campaign that ultimately provides malicious actors with a toehold into systems or misconfigured databases and services that leave millions of sensitive records freely available on the internet, it seems to be human nature coupled with weak controls that contributed heavily to the number and severity of breaches we've seen this year.

WHEN INSIDERS GO ROGUE

What would be the worst-case scenario should a trusted insider steal data? Losing highly sensitive governmental intelligence? Or maybe closely guarded trade secrets? One event in particular from this year demonstrates just how damaging insider events can be. In April, news broke that from October 2014 through 2017, a technology manager working at the Department of Homeland Security's Office of Inspector General provided a co-conspirator with the source code for OIG's Enforcement Database System along with copies of a database containing information from more than 150,000 internal investigations and personal information of approximately 250,000 DHS employees. Although malicious insiders accounted for only 7.3% of the breaches reported this year, this example illustrates it's a minority that should not be discounted.
GETTING SCHOOLED ON BREACHES

While governmental entities have come into the spotlight recently thanks to a wave of ransomware attacks and the curious event at the Bulgarian National Revenue Agency, the education sector has suffered its fair share of bumps this year as well. In July, the for-profit heavyweight K12 left 6.9 million records exposed on a leaky MongoDB instance and malicious actors took aim at another big name in the industry, Pearson Clinical Assessments, attacking their AIMSweb system and compromising student data from approximately 13,000 schools.

Perhaps the most interesting disclosure of the year comes from the Australian National University. In June, the university announced they had discovered “a sophisticated operator” had accessed their systems in late 2018. Students, staff and visitors’ personal information, going back potentially 19 years, was accessed by attackers. What makes this event stand out is not so much the nature of the data exposed or the amount of information put at risk. Rather, it was the university’s response and commitment to sharing their analysis of the incident with others that set this one apart. From the outset, the university’s leadership stated they would share updates on the investigation. Instead of providing typical follow-up statements that offer little additional insight into the event, the university shared an incident report in September that was a fascinating read with enough detail to not only understand the chain of events, but also to learn from their experience. It’s the type of response we hope to see more of in the coming months.
Integrating Cyber Insurance into a Risk Management Program

Jake Kouns, Co-founder, CISO, Risk Based Security

Jake is an expert in the security industry who has briefed the DHS and Pentagon and is frequently interviewed by Forbes, Information Week, PC World, CSO, and CIO Magazine. He has appeared on CNN and presented at many well-known security conferences, including RSA, Black Hat, DEF CON, CISO Executive Summit, FIRST, and HITB Cyberweek. Jake is also co-author of Information Technology Risk Management in Enterprise Environments, Wiley, 2010, and The Chief Information Security Officer, IT Governance, 2011.

Just as all software is vulnerable, so are all companies. In many cases, it’s not a question of whether or not you will be breached, it’s when a breach will happen and how well you can mitigate the costs associated with a breach. At this point it’s safe to assume that we all know that data breaches can be very costly events. Data breaches aren’t slowing down, and findings from our previous QuickView report showed that compared to midyear 2018, the number of reported breaches was up 54% and the number of exposed records was up 52%. We are still on track for yet another worst year ever when it comes to data breaches.

What are your options as an executive in charge of security for your organization? There are four primary ways of dealing with risk: you can avoid, mitigate, accept, or transfer it. Many organizations are adept in these options, with the exception of transferring risk to cyber insurance products.

Love it or hate it, cyber insurance can bring a lot to the table when it comes to dealing with the financial fallout of a security breach. And to be clear, despite “risk” being in our company name, Risk Based Security does not sell cyber insurance policies. Nor should anyone think of cyber insurance as a substitute for a solid information security management system backed by well maintained controls. Buying cyber insurance is NOT a free pass to skimp on security. However, based on our involvement with cyber insurance and tracking data breaches over the years we are in a very unique position to understand both the good and bad. I simply believe that at this point the majority of organizations are still not adequately taking advantage of the market or integrating cyber insurance policies into their risk management programs. Public perception of cyber insurance, in my opinion, has allowed misconceptions take hold in the security industry, preventing people from seeing cyber insurance’s true worth.

THE MISCONCEPTIONS

Like most insurance gripes, people within the industry are convinced that cyber policies don’t pay out claims, that policies have hidden exclusions within them, and that overall, a policy is not worth allocating budget (which explains why not many organizations have purchased cyber policies). But all of this explains the main source of the general misconception; organizations just don’t fully understand cyber insurance.

Despite the many types of cyber policies in the market, and the different names including ‘Cyber Liability’, ‘Privacy Injury Liability’, ‘Network Security Liability’, etc. there is little commonality between them. At the heart of it, cyber insurance is a commercial policy and isn’t quite the same thing as an auto or homeowners policy, but there are some similarities.

What you need to know is that these commercial policies will be covering two main concepts: first party and third party damages. In first party damage situations, a payout will fix the things we own when damaged. In a third party case, it pays others when our
actions (or inaction) causes harm. Why does this matter? It matters because you can buy a cyber policy that can cover both. In
the case of a security event involving a data breach or compromise, recovery costs would fall under first party damages while
protection from lawsuits arising would be covered under third party damages. It is vital that you understand how different
policies address these types of incidents in order to eliminate misconceptions about cyber insurance exclusions.

If you want to transfer risk effectively so that you can recover costs, you need a cyber policy that covers first party damages. If
you are transferring risk to lessen the burdens of legal action against you in case of a breach, then you need a policy that covers
third party damages. If you don't or can't distinguish between the two, then when it comes to an event, you may become one of
the people that claim that cyber policies “don't pay out”!

As helpful as some of these policies can be, there are some things that are just not usually covered.

- **Reputation damage** - Survey after survey, reports have shown that the biggest concern of senior leadership is the
damage a breach can do to the organization's reputation. It can have an impact on the bottom line for months, if not
years. Unfortunately, there is nothing an insurance policy (or any risk transfer method for that matter) can do to repair a
tarnished public image or loss of customer confidence. However, there may be services available such as a public
relations or crisis management consultant to assist.

- **Regular maintenance, upgrades, and fixes** - Like almost every standard insurance policy out there, insurance will not
cover 'wear and tear' or regular maintenance fees of keeping systems up-to-par. If you have an old legacy system,
insurance isn't going to replace it with the latest and greatest technology.

- **Economic value of data / data in the care, custody or control of others** - It's hard to assign a specific value to “Data”.
Typically, policies will not reimburse the value of lost data itself and in some situations, data or systems that have been
entrusted to a business partner or vendor.

Every insurance policy has its own set of exclusions and some of those exclusions are not common in the industry, so you need
to have a watchful eye. Yes, you do need to read the policy. Or...hire someone to do it for you. Despite the limitations, when you
add up the many ways a policy can contribute to softening the financial blow of a security event, cyber insurance becomes an
attractive method for off-setting risk. What's even better is that insurance companies are still struggling to figure out how to price
insurance policies. That, combined with the intense competition in the cyber insurance market, translates to good news for
buyers.

**INTEGRATING INSURANCE INTO RISK MANAGEMENT**

Chances are, your organization is already transferring risk to protect your most important assets. Most likely, a policy exists for
your property, liability coverage, employment practices liability, workers compensation, and/or professional liability (also known
as errors and omissions). Let's face it, achieving perfect security is unlikely and chances are it's just a matter of time before the
worst happens and an incident occurs. Even highly effective security programs are being compromised despite the vast
resources that are put into them.
As with everything, the law of diminishing returns applies when it comes to cyber security. Adding more layers of controls or buying additional security products doesn't necessarily result in ‘better’ security. The goal should be to first find the optimal level of security for your organization, then to integrate cyber insurance into your risk management program to offset the cost of a security event. To be very clear, obtaining cyber insurance is not a replacement for implementing a security program. It is critical that organizations continue to focus on investing properly into cyber security.

Competitive forces in the insurance marketplace continue to put downward pricing pressure on cyber coverage. This means you could effectively transfer some risk inexpensively, especially if you are a small to midsize business. In the current insurance market, yearly minimum premiums can be $1,000 or lower for $1M in coverage and this includes many Risk Management Services for free. Pricing can definitely change based on industry and controls, but current pricing levels make cyber insurance an attractive option for any company. It is even more attractive small businesses that are generally confused by the complexity of security or have an immature security program by also gaining a partner which helps provide a path to improvements.

Even larger organizations can benefit from the market and get a reasonably priced policy. As is the case for smaller businesses, pricing can change based on industry and controls. Even for at-risk industries (for data breaches) such as Healthcare, estimates have been $100,000 - $200,000 for $1M and $5M in coverage respectively. Limits are available up to $250M, and large towers can be built up to $750,000. This is a great option for larger organizations that don't typically use Risk Management Services, but can utilize pre-negotiated lower service rates from legal to cyber security providers.

ACTIONS

With the rise of cyber insurance, if your organization doesn't have a policy, it will most likely soon. Regardless of how information security professionals and responders feel about cyber insurance they need to know how it works. This allows them to help with the applications process and ensure proper coverage, while being aware of what the policy covers and the requirements that need to be met before and during an incident in order to ensure that coverage is not nullified. In the case of a breach, do you want to say “Whoops? Sorry.” Most likely you would want to be in a position to say “We have a partner and coverage. Let's file a claim.”

Take advantage of the market and shop around. I can't stress this enough, but not all cyber insurance policies are the same, nor are they priced the same. But before you do that, determine if you currently have a cyber liability insurance policy in place for your organization and find out what it actually covers. Make sure to understand the coverage that would be important for your organization, determine the amount of desired coverage, and find that quote and review it carefully. If it checks all of those boxes, then you can feel comfortable about the integrating cyber insurance into your risk management plan.
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 Breach Trends Through Q3 2019

In many ways breach activity in 2019 is living up to the expectations set by our Q1 findings. The number of publicly disclosed data compromise events is predicted to reach an all-time high while the total number of sensitive records exposed has already surpassed the high water mark set in 2017. Throughout this report, we present various perspectives on the breach events reported during the first nine months of the year, including analysis of the types of data lost, how the data is compromised, where events are taking place and who is impacted.

Q3 2019 At A Glance

Despite occasional dips, there has been a steady increase in the number of breaches reported over the past eight years. So the increase in 2019 is not surprising. However, the change does stand out from the general trend, with a 33.3% increase in the number of breaches disclosed compared to the same point in 2018. The last time there was a jump like this was in 2015, which saw a 36.8% increase in breaches reported compared to the same point in 2014.
Most organizations that experience a breach are sensitive to the amount of data they share about the event. One such detail is the number of records compromised. Organizations will report this information when required but generally will not include this in standard breach notifications or disclosures. Despite reluctance by organizations to publicize the record count data, the first nine months of 2019 has already surpassed the 2017 year end total and is on track to reach as high as 8.5 billion records exposed.

Regular readers of our QuickView Report will not be surprised to see that unauthorized access to systems ("Hack") is, by far, the top breach type when it comes to the number of breaches reported through September 30th. This comes as no surprise to those of you that track the number of new software vulnerabilities disclosed each and every day. RBS' VulnDB has added 61 new vulnerabilities each day during 2019. Stay tuned for our VulnDB QuickView report scheduled for release later this month.

While malicious actors have been responsible for most incidents, it is accidental exposure of data on the Internet that has put the most records at risk. This year over 6 billion records have been made freely accessible thanks to misconfigured databases, backups, end points, and services. The widespread availability of tools useful for identifying such leaks coupled with an interest in reporting - as well as taking advantage of - these exposures has fueled the growth in the number of records compromised since 2017.
Actors outside of the organization, rather than insiders, are responsible for 87% of the breaches reported through September 30th. Pinpointing the motivation of external actors can be challenging. Some events are obvious – when data is offered for sale or ransomed back to the owner there is clearly a financial motive at work. Other events are less overt. While there may be tantalizing circumstances that could indicate motive, it is considered to be “unknown” absent definitive data indicating otherwise.

A loss of control of sensitive or confidential data by an organization responsible for its protection is considered a breach by our definitions. This allows tracking for a wide variety of events as well as an opportunity to distinguish between confirmed data access by unauthorized third parties from events where data is at risk but not confirmed to have been accessed. Approximately 80% of breaches reported this year have confirmed data exposure.
Access credentials in the form of email addresses and passwords are consistently the most compromised data types. Why? For the simple reason it's much easier to break in with keys in hand than to find an opening in an otherwise locked building. Credentials can provide direct access to valuable data as well as an opportunity to gain a foothold into systems enabling reconnaissance and potential escalation.

Looking beyond access credentials, most of the other data types are, for the most part, equally represented. "Name", which is an individual's full name, coupled with at least one other piece of identifying information such as date of birth or banking details, is typically the basis for triggering breach disclosure obligations. So it is not surprising to see “Name” coming in as the third most common data element exposed.

The “Miscellaneous” category is an interesting grouping of data points, some of which would be considered sensitive data under various regulatory regimes and others that would not. The “miscellaneous” data type includes items such as driver's license numbers, passport numbers, student records and IP addresses.
**Who Has Been Breached Through Q3 2019**

No organization is immune to data breaches. Large corporations such as American Express, Dunkin’ Brands, and Vodafone as well as small community projects, rural schools, and solo professional practices have experienced breaches this year.

There are multiple dimensions to our organization classification system, put in place in order to facilitate different views into what type of organizations have experienced a breach.

One of the most popular systems we offer is classification according to the North American Industry Classification System, or NAICS. Figure 8 illustrates the distribution of the “steward” organizations by NAICS economic sector.

In our system, a steward organization is the entity that lost control of the sensitive information rather than other impacted third parties. The classifications of those impacted third parties are not included in this graph, an important distinction to keep in mind when reviewing the chart.

Of the organizations that could be definitively classified, medical service providers have topped the list as the most compromised economic sector. Retailers were a close second, due in large part to both physical and ‘online’ skimming operations driven by continued interested in payment card data. The Information sector which includes software creators, data processing, hosting, streaming services, and websites made up 77% of the breaches attributed to the sector.

![Figure 8: Number of breaches per economic sector, reported by 9/30/19](image-url)
Taking a step back to look at breached organizations from another perspective, the Business Sector still accounts for 66% of breaches, Medical 14%, Government 12% and Education 8%.

Figure 9: Distribution of breaches by business group and business subgroup, reported by 9/30/19
Determining the location where a breach occurred can be as challenging as teasing out the motivations of malicious actors. With some events it’s plainly obvious, with others, it’s anyone’s guess. One trend that we know to be true is that locations with more stringent reporting requirements will have correspondingly more breaches being disclosed. Recent reports from regulatory bodies in the EU, Australia, and most recently Canada support this observation.

Combining the economic sector data with a closer look at the United States reveals more diversity than a mere “red states” and “blue states” distinction (that would be Finance and Healthcare, not that other red and blue). Not surprisingly, the Information sector, and more specifically the technology services that fall into that classification, dominate the breaches at organizations located in California while skimming at gas stations and convenience stores drives the experience in Texas and Florida.
Just as not all breaches have a confirmed impact on confidentiality, not all breaches are equally impactful. The severity score is a function of the number and type of records lost in combination with other factors such as how the breach took place, if third parties were impacted and any resulting regulatory or legal action arising out of the event.

### In Closing

As we look back over the breach experience for 2019, we can see that the trends set up in the first quarter of the year have continued unabated through the end of Q3. The number of publicly disclosed events shows no sign of slowing, setting up 2019 to be another “worst year on record” in terms of breach count, while the number of sensitive, confidential records exposed has already exceeded all prior years tracked. We are often asked, “what should be done to stop this?” Perhaps the better question is “what can be done to minimize the impact?” If we accept the axiom “it’s not a matter of if, but when” an organization will be breached - which is largely supported by this research - then focusing on prevention alone is not the solution. A vibrant risk management strategy coupled with incident response planning (including cyber insurance) can go a long way towards minimizing the damage that can come from a security event.
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.

*Figure 11 of this report was generated using mapchart.net®