RiskBased SECURITY + FLASHPOINT

2021 Year End Report

Data Breach QuickView

In This Issue

FEATURING VIEWPOINTS FROM

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 US She currently holds a CIPP/US designation.

Ashley Allocca
Cybersecurity Intelligence Analyst,
Flashpoint

Ashley Allocca is a cybersecurity intelligence analyst at Flashpoint. Her research focuses on cyber threats in the retail, financial, and healthcare sectors, as well as other emerging threats in illicit communities across the deep and dark web, and open web. She has presented at CNP's Holiday Preparation webinar, AARP's Cyber Security Awareness webinar, and participates in H-ISAC threat briefings, among others. She has also contributed to several cybersecurity-focused publications. Ashely holds an M.S. in Cybersecurity from Fordham University, which has been designated by NSA and Homeland Security as a center for excellence in cybersecurity.

2021 YEAR END DATA BREACH QUICKVIEW REPORT

Welcome

It is fitting that the publication of this report aligns nicely with Groundhog Day. In many ways, 2021 echoed several of the same themes we witnessed in 2020: sparsely stocked shelves returned as the coronavirus continued to wreak havoc with supply chains, return to work & school plans were upended yet again, and another year of brazen breaches made headlines.

The key trends examined in our Mid Year Data Breach QuickView Report stayed with us throughout the last half of 2021. Despite several notable law enforcement successes, ransomware attacks continue to cause financial and reputational pain to organizations around the world. Also in the first half of 2021, regulators and security researchers alike raised the alarm on the lengthening timeline for disclosing incidents. Unfortunately, by year end, the gap between discovery and disclosure showed no sign of shrinking. Lastly, in our Mid Year report we highlighted the creativity of attackers with our overview of autofill-assisted fraud. While a similar chain of attacks did not take place in the second half of the year, there was no shortage of breaches that caught our attention thanks to the ingenuity of the attackers.

Throughout this report we will explore these themes and more. The report will examine breach activity from several perspectives, ranging from what types of data was targeted, who was compromised, and the impact of these events. In keeping with our customary practices, this report covers publicly disclosed data compromise events. The statistics and findings are derived from breaches first reported between January 1, 2021 and December 31, 2021.

Key Highlights

- There were 4,145 publicly disclosed breaches in 2021, approximately 5% fewer than 2020. However, additional incidents continue to surface. It is typical for the number of breaches disclosed for a given year to subsequently increase by 5% to 10% as the data matures. Assuming this pattern continues, 2022 is expected to at least match the 2021 breach count, and potentially exceed it by as much as 5%.
- The number of records exposed during the reporting period exceeded 22 billion. While this is 14.5 billion fewer records exposed than in 2021 (the year that set an all time high of 37.2 billion records exposed) it is the second highest year for the amount of confidential data compromised since 2005.
- The number of breaches reported in the United States increased 10%, growing to 2,932 in 2021 compared to 2,645 in 2020.
- Names and Social Security numbers (or their non-US equivalents) were the two most compromised data types. Payment card information, which has become less attractive to malicious actors, was compromised in only 3% of reported breaches.
- Overall the healthcare sector experienced the most incidents, accounting for 14% of reported breaches. However, when economic sectors are broken out into their component risk groups, financial services and software providers were the top two most breached business groups, with healthcare practitioners' offices coming in third.
- Manufacturing, not typically considered a popular sector to target, was the sixth most compromised sector, accounting for 9% of reported breaches.

Looking Back at Six Years of Breach History

VIEWPOINT by **Inga Goddijn**

This is the sixth Year End Data Breach QuickView Report I've had the honor of shepherding to publication. Over the years, those involved in developing this information have grown from a small group of analysts to a talented and creative team of researchers, data scientists, designers and editors. Long-time readers of the QuickView Reports will have noticed the many changes we've introduced over the years, including increasingly closer looks at the key trends influencing breach statistics as well as additional commentary on the more interesting incidents that surfaced during the year. To that end, we're checking in on the state of ransomware attacks - because what discussion of breach activity would be complete without it - and the vexing issue of delayed disclosures. We'll also share the winners from our Cyber Risk Analytics researcher poll, in which our team was asked "which 2021 breaches stand out to you and why?"

WILL RANSOMWARE EVER GO AWAY?

If I had been asked six years ago whether ransomware was a serious threat, I'm fairly certain I would have said no without much hesitation. Back in 2016 there were a handful of data breaches that included a ransomware component, but those amounted to fewer than 1% of the breaches reported that year. Fast forward to 2019, and ransomware-related incidents had become prominent enough (present in 11.5% of reported breaches) to be called out as a significant shift in the threat landscape. By the close of 2020, 17% of reported breaches involved ransomware, and in 2021, the percentage climbed to 21%.

In the 2021 MidYear Report, we noted there were reasons to be hopeful that the tide was turning on ransomware operations. Thanks to a series of very public and very high profile attacks, significant resources flowed to combating the threat, which in turn led to several law enforcement successes. DarkSides' public infrastructure was knocked off-line, and REvil/Sodinokibi was shut down for good. Unfortunately, the lull in activity didn't last for long. In total, there were 874 breach events that included a ransomware component in 2021. 453 of those came to light in the first half of the year, 421 in the second half. As one operation shuts down, new groups emerge to take their place and keep the attacks flowing.

BETTER LATE THAN NEVER BUT NEVER LATE IS BETTER

In our 2018 Year End Report, we took a closer look at the average number of days between when a breach was discovered to when the breach was reported. We picked up on the topic because, after 3 years of closing the gap between discovery and disclosure, the number of days it took for organizations to go from knowing about the incident to reporting it was beginning to increase. That seemed unusual, especially with new regulatory emphasis being placed on timely reporting.

Since that time, the issue has only become more pronounced. In 2021, 15 breaches took more than 365 days - a full year - to go from discovery to the release of a formal breach notification letter. Another 169 events took six months or more. Broadening the scope to look at time of discovery to date of first disclosure (meaning an email, blog post, tweet, or some other form of communication about the event), 75 events took more than a year to go from

discovery to first disclosure and another 207 breaches took six months or more to disclose. It would be easy to blame delays on the pandemic, but this trend started well before COVID became a household name. Complex incident investigations, weak enforcement, and a deliberate blindness to notification obligations appear to be at the root of the delays.

NOTEABLE & NEWSWORTHY BREACHES

The Cyber Risk Analytics research team analyzes thousands of breach events every year. With such a high volume of data, it takes a truly unique set of circumstances for an individual event to stand out from the crowd. We touched on the more notable breaches reported during the first six months of 2021 in our Mid Year Data Breach Report. For this Year End edition, we're turning our attention to the breaches that caught our eye in the second half of the year.

The October ransomware attack targeting Sinclair Broadcast Group was one such noteworthy event. At first glance the incident appears to be a fairly typical event. A relatively new variant of WastedLocker ransomware dubbed Macaw was launched in Sinclair's systems on October 16th. Unfortunately for Sinclair, the attackers hit a sweet spot in Sinclair's operations leaving many local affiliates scrambling to fill air time. TV stations across the country were left unable to broadcast local news, access syndicated programming, or air local advertising. Even as programming came back on-line, local newscasters were left without access to the supporting tools used to create content. That led to journalists reading from paper copy, sports scores taped up on a wall, and one weatherman resorting to holding an umbrella and using a whiteboard-drawn map for the weather update. Other than the Colonial Pipeline incident, no other event this past year was so starkly put on public display.

It is tempting to see the Sinclair incident as representative of more sophisticated targeting by attackers. Not only are malicious actors seeking targets where downtime can result in significant financial losses, they are seemingly also keen on targeting organizations where the disruption cannot be shielded from public view. Case in point is the December attack on payroll services provider Kronos. The malware disabled the Kronos Private Cloud, which hosted data for clients of UKG Workforce Central, UKG TeleStaff, Healthcare Extensions and Banking Scheduling Solutions. As of this report, at least twenty five Kronos customers, including major U.S. cities and healthcare systems, were left resorting to manual workarounds in order to pay employees. Breach fatigue may leave many feeling indifferent to the latest attacks. By threatening the payroll of thousands of workers across the country, attackers were all but guaranteed to generate publicity for their actions.

Lastly, no discussion of 2021 breaches would be complete without a shoutout to one of the more entertaining events of the year. In early summer, Russia-based pizzeria franchiser Dodo Pizza had data on 584 franchisees shared on Github. Included in the mix were the URLs to access live security camera streams, displaying real-time pizza making operations across their various locations. Not only did it remind us of the near-universal appeal of a really good slice, it was charming to see the considerable care going into creating a pie in far flung locations like Kyrgyzstan.

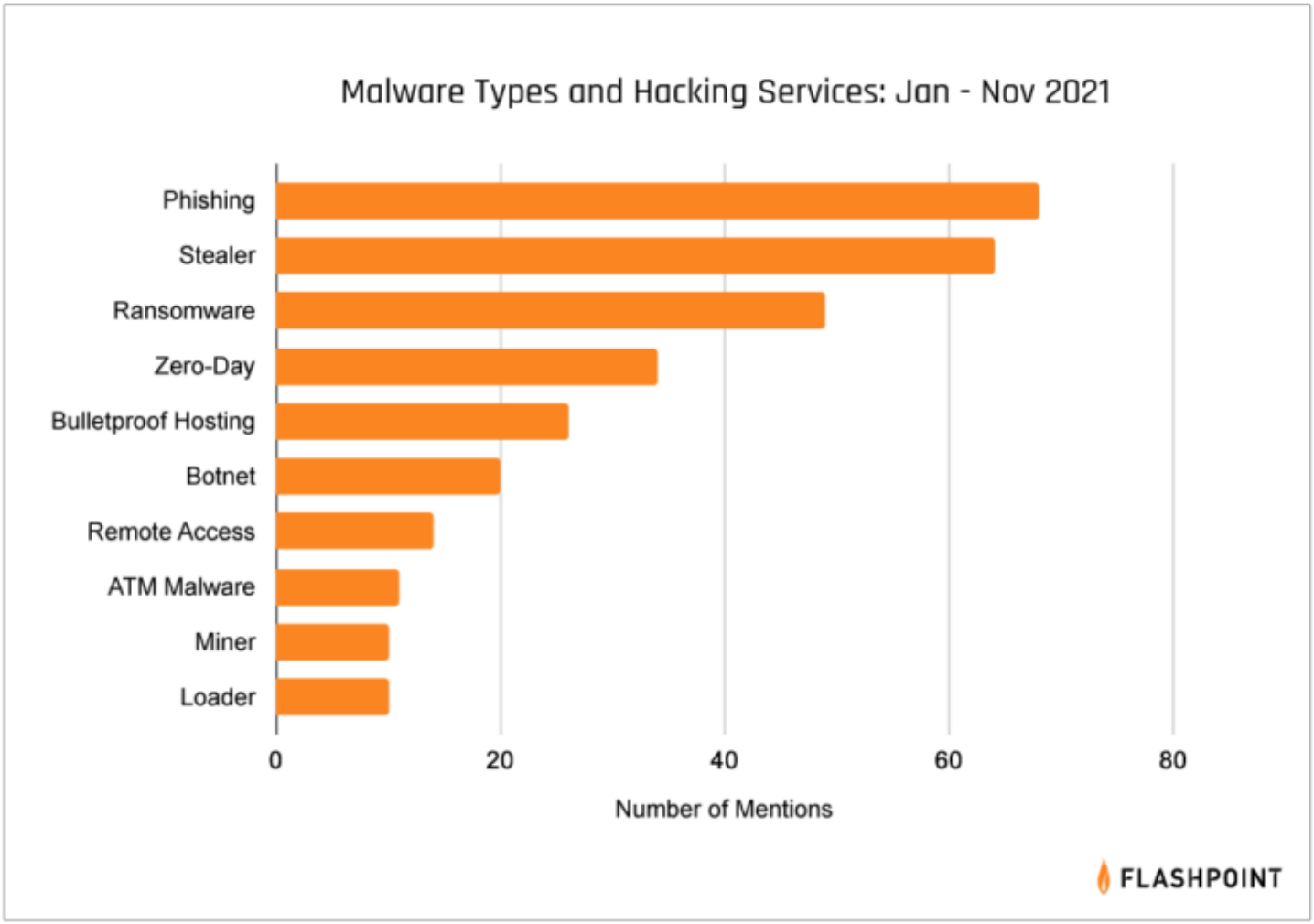
2021 Trends in Data Theft and Malware

VIEWPOINT by **Ashley Allocca**

On January 12th, Risk Based Security and Flashpoint announced that we are joining forces. Flashpoint is the leading provider of threat intelligence, with expansive data collections backed by an unrivaled team of security analysts. We're pleased to include Flashpoint's review of 2021, highlighting key observations of activity taking place on illicit and underground forums.

1. MOST DISCUSSED MALWARE TYPES AND HACKING SERVICES

The top 10 most discussed malware types and hacking services discussed over the last year were dominated by phishing, stealers, Zero-day attacks, and ransomware, which has notably been banned from a number of top-tier illicit forums.



2. MOST POPULAR FORUMS

The most popular forums where threat actors advertised and solicited breached reporting were Raid Forums and Exploit, by far.

3. MOST TARGETED SECTORS

The sectors most commonly linked to data advertised in forums in 2021 were:

- **Government** (commonplace data types were Social Security Numbers (SSNs), driver's licenses, passports, and other government-issued identity documents);
- **Financial** (fullz, bank logs, and databases, online retailers that store financial data)
- **Healthcare** (mostly U.S.-based, personally identifiable information (PII), protected health information (PHI), financial data, and login credentials)
- **Education** (compromised credentials, e.g.)
- **Retail** (holiday fraud, e.g.)

4. MOST POPULAR ACCESS TYPES ADVERTISED

The most popular access types advertised for sale on forums was admin- or user-level access for Remote Desktop Protocol (RDP) / virtual private network (VPN) and content management systems (CMS). This type of access could lead to the compromise of customer personal information and, in some cases, financial information.

5. RISE OF SQL INJECTION ADS

Advertisement of SQL injections (SQL) trended upward, gaining steam in popularity as a method for sellers to guarantee data integrity to their customers.

6. PRICING IS BEING WITHHELD

Recently, threat actors have been omitting pricing information more than usual although it's unclear exactly what motivations may be spurring this emerging trend. It is possible that withholding the desired sale price leads only seriously interested buyers to contact the seller. This trend further increases the difficulty of assessing data pricing within illicit forums. Since negotiations are being held in private chats and listing and sale prices are increasingly being withheld, it remains difficult to know the exact value of these data types.

7. NEGOTIATIONS VIA CHAT

Negotiations (including communications around vouching and proof-of-concept) have appeared to shift to encrypted chat services from the forum themselves.

8. GEOGRAPHIC DISCLOSURES

Threat actors, most of whom are out for financial gain, are increasingly disclosing geographical information about the data and access they advertise. According to our collections, the "unknown" category - which denotes data for sale *without* location-specific information - is down almost 42%.

9. ZERO-DAY AND PHISHING ADS DOMINATE RAID

Raid Forums - traditionally popular amongst threat actors for buying and selling breach data - emerged as a major player in malware and hacking services as well in 2021. Zero-day and phishing attacks were by far the most advertised exploits.

10. RANSOMWARE IS TABOO

Ransomware has been widely banned on major forums as evidenced by referring to their ransomware offerings as “crypters” or “lockers” to avoid their post or account getting immediately banned.

The Data Breach QuickView report is powered by

Cyber Risk Analytics

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

1. Cyber Insurance
2. Security & Vulnerability Management
3. Vendor Risk Management
4. Procurement
5. Governance & Management

REQUEST A DEMO
riskbasedsecurity.com/contact

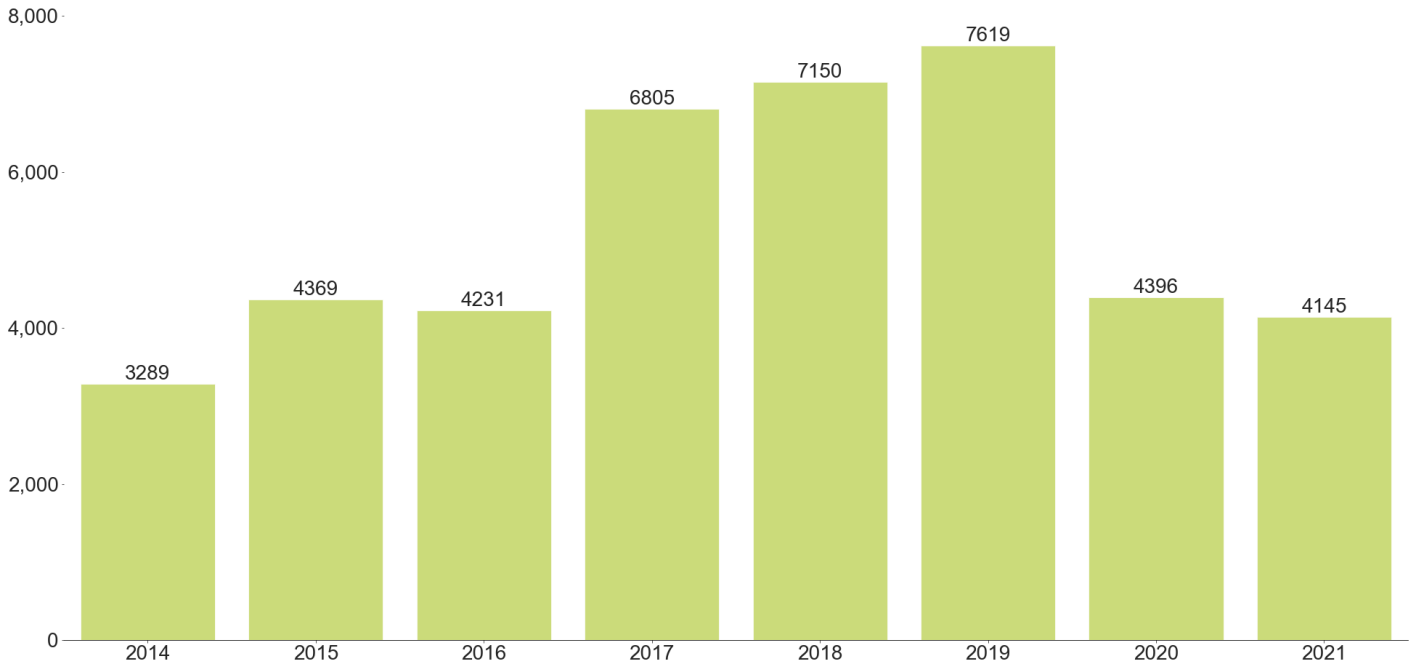
LEARN MORE

Data Breach Trends in 2021

A question we are often asked is whether the data breach landscape is 'getting better'. Looking back over 2021 and 2020, the numbers do not provide a simple answer. The time it takes to report a breach, coupled with the lingering effects of a drop-off in media coverage and more ransomware attacks that can be kept out of public view, has undoubtedly played a role in the decline in publicly reported breaches. At the same time, the number of sensitive records exposed continues to reach well into the billions. Read on for more insights into the who, what, when, and where of breach activity that shaped 2021.

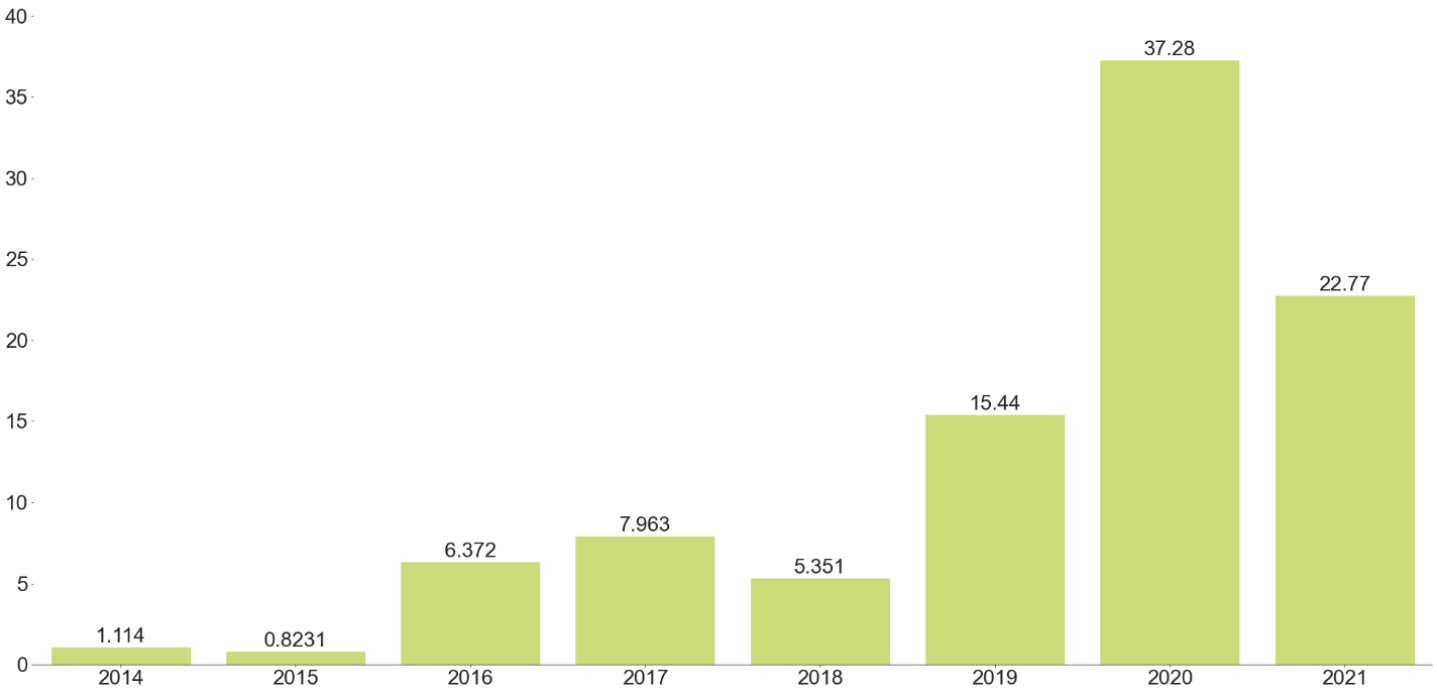
2021 At a Glance

Figure 1. Number of breaches reported by EOY, for the past eight years



At the time of this report, the number of publicly disclosed data breach events stood at 4,145 or approximately 6% below 2020. Does this mean there were fewer breaches in 2021? Based on our experience of how the data develops over time, the answer is a resounding no. Readers of the 2020 Year End Report may recall at the time that report was issued, the number of publicly disclosed breaches stood at 3,932. We estimated that number would grow by 5% to 10% over the course of 2021. The number actually increased by 11.8%. The same factors, noted in the above introduction, that impacted 2020 continue to be present today. Assuming another conservative estimate of 5% to 10%, we anticipate the number of breaches for 2021 will settle in a range between 4,352 to 4,560.

Figure 2: Number of records lost (in billions) reported by EOY, for the past eight years



Unlike the number of breaches reported, we anticipate little change to the colossal number of records exposed in 2021. At 22.7 billion records, 2021 is second only to 2020 in terms of the volume of data compromised. The three largest breaches of 2021 account for 82% of exposed records, with the largest breach of the year contributing 16 billion records (70%) to the total.

Figure 3: Number of breaches by breach type, reported by EOY 2021

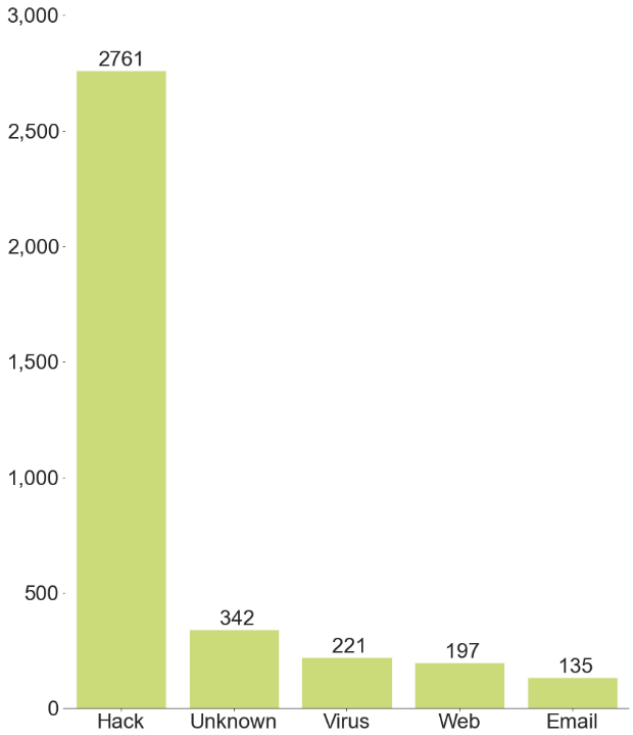
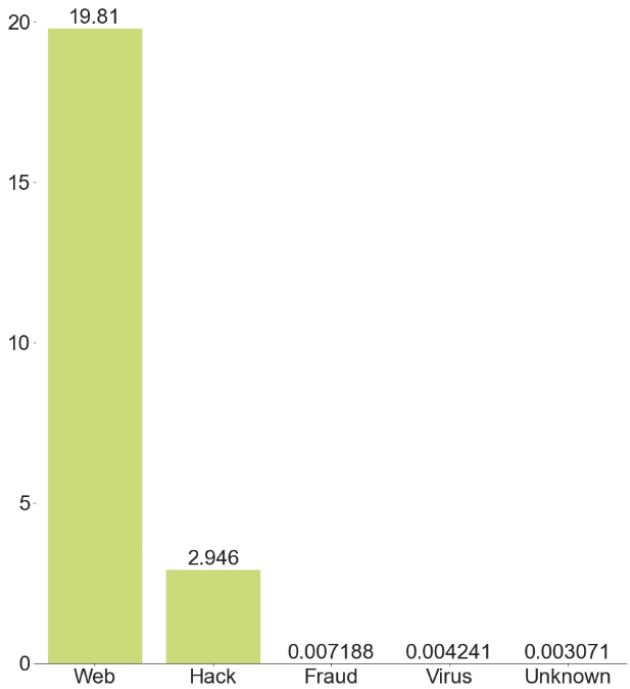


Figure 4: Number of records lost by breach type (in billions), reported by EOY 2021

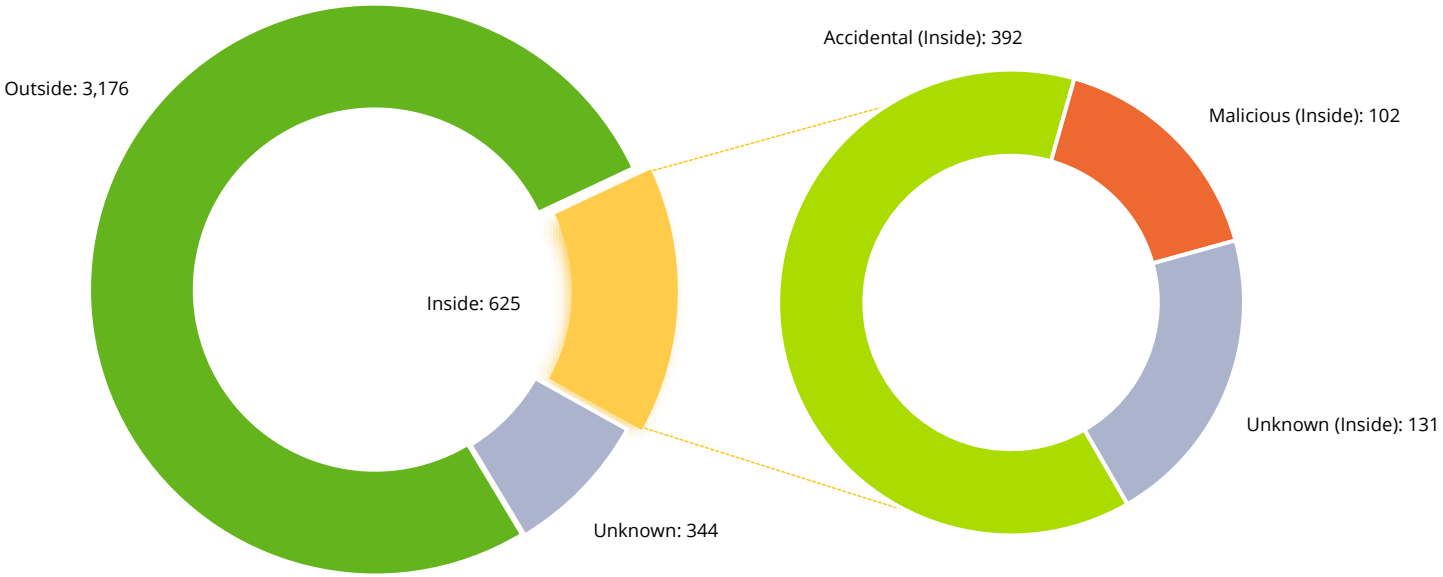


Since the 2017 Year End Report, "Hacking" (unauthorized access to systems or services) has been the top breach type, accounting for the most reported breaches, while "Web" (publishing, sharing or open access to data online) has been the top breach type responsible for exposing the most records. Where the trends become more interesting is looking down the charts to the subsequent breach types.

For the first time since the 2016 Year End Report, the breach type "Email" makes the top five, appearing in our chart of 'breaches by breach type' as a result. Much like "Web", these events are largely driven by user error. Attaching documents containing sensitive information, sending emails to the wrong recipients, and failure to appropriately utilize the BCC function all contributed to the rise of Email breaches (note: unauthorized access to email accounts is typically captured as a "Hacking" event). These may seem like minor incidents, but these are often subject to disclosure or notification laws. That means what may seem like an innocuous event can still result in additional costs to the organization.

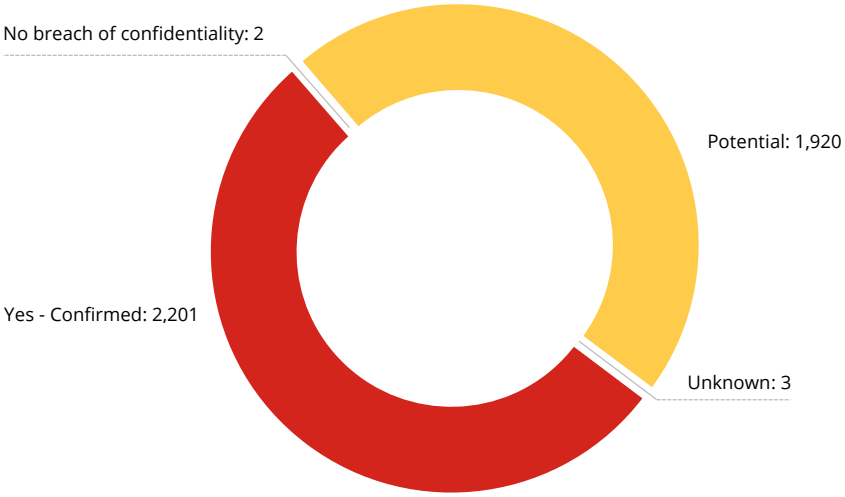
The usual suspects dominate the breach types responsible for exposing the most records. Of note, the breach type "Unknown" is making an appearance in the 'records exposed by breach type' chart. How can a breach type be Unknown? This is often a function of how the event is publicly surfaced. Certain sources reveal little more than the fact that a data compromise event has occurred. While these are typically smaller events, impacting fewer than 10,000 records, 2021 saw ten incidents with an "Unknown" breach type impacting more than 10,000 records, including four that impacted over 500,000 records each. These incidents combined to push "Unknown" into this year's statistics.

Figure 5: Number of breaches by attack vector, reported by EOY 2021



There is no doubt a malicious insider can do significant harm to an organization. Even ransomware operators have picked up on the opportunity, with news surfacing in late summer that unhappy employees of targeted organizations were being bribed to deploy ransomware. But insider errors can be equally damaging. In 2021, seven incidents attributable to insider mistakes accounted for the exposure of more than 19 billion records, including the leak at FBS Markets, the largest breach ever recorded.

Figure 6: Number of breaches by known confidentiality impact, reported by EOY 2021



If a database leaks online, but no one is there to pick up the data, is it a breach? In our view yes, but we also recognize there is a world of difference between attackers stealing troves of sensitive data and a loss of control over the same dataset. In approximately 53% of the reported data breaches, information was confirmed to be in the hands of unauthorized persons, while in 46% of breaches data was exposed but no conclusive evidence has surfaced confirming its theft or compromise.

Figure 7: Severity distribution of breaches in 2021 H1 and H2

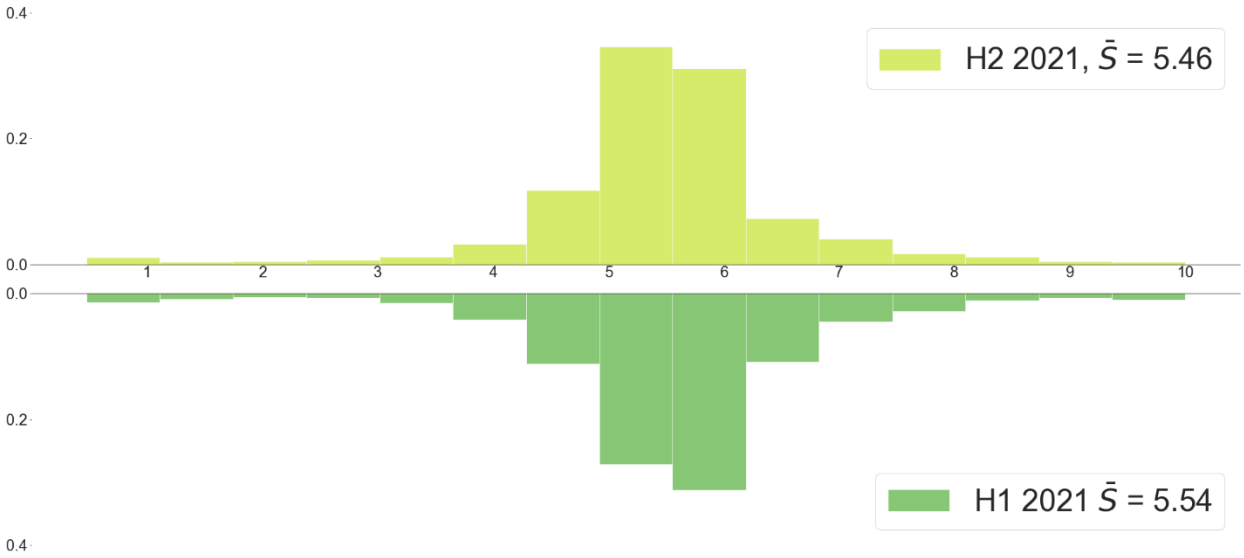
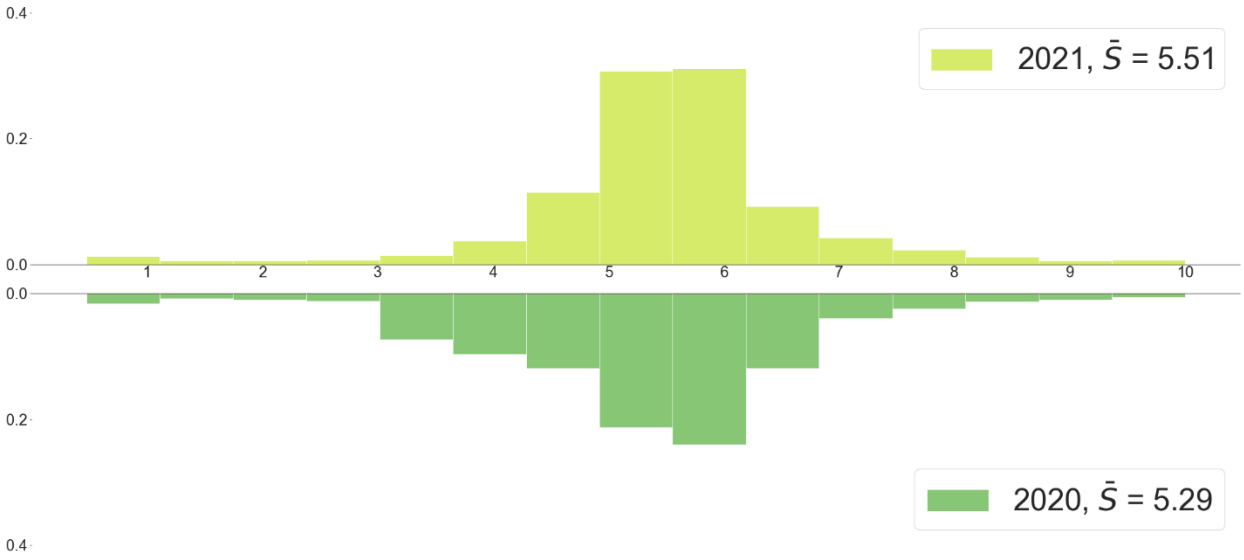


Figure 8: Severity distribution of breaches in 2020 and 2021



Severity score (a measure based on the number of records exposed in combination with the data types compromised, how the attack occurred and more) showed improvement in H2 compared to the first half of the year. With the increasingly long tail for disclosing breach details, it would not be surprising to see the average severity score for 2021 increase somewhat. That said, predicting which direction the severity score will go is difficult. What can be safely assumed is that regardless of direction, it will most likely stay in the range of 5.4 to 5.7.

Records Compromised	Number of Incidents
Unknown	2186
1 to 9	108
10 to 99	61
100 to 999	364
1,000 to 9,999	602
10,000 to 99,999	452
100,000 to 999,999	234
1,000,000 to 9,999,999	95
10,000,000 or above	43

Table 1: Number of incidents with records lost in these ranges reported by EOY 2021

Year	Number of Incidents
2021	43
2020	66
2019	68
2018	48
2017	39
2016	40

Table 2: Number of incidents that exposed 10 million or more records for the past 6 years

One of the effects of the popularity of ransomware attacks is less detail around the number of records exposed. The goal of these attacks is less about targeting certain types of data, like customer account information, and more akin to "smash and grab" operations, with attackers pilfering whatever seems to be of value to the compromised organization. This has contributed to nearly 53% of breaches with an unknown - or more precisely, unconfirmed - number of records compromised.

That said, there is positive news contained in these numbers. For incidents where the number of records *is* known, more than half (58%) exposed fewer than 10,000 records. Another positive statistic: the median number of records lost stands at 5,269, well below the 10K mark. Lastly, the number of breaches exposing 10 million or more records is well below its 2019 peak of 68 incidents.

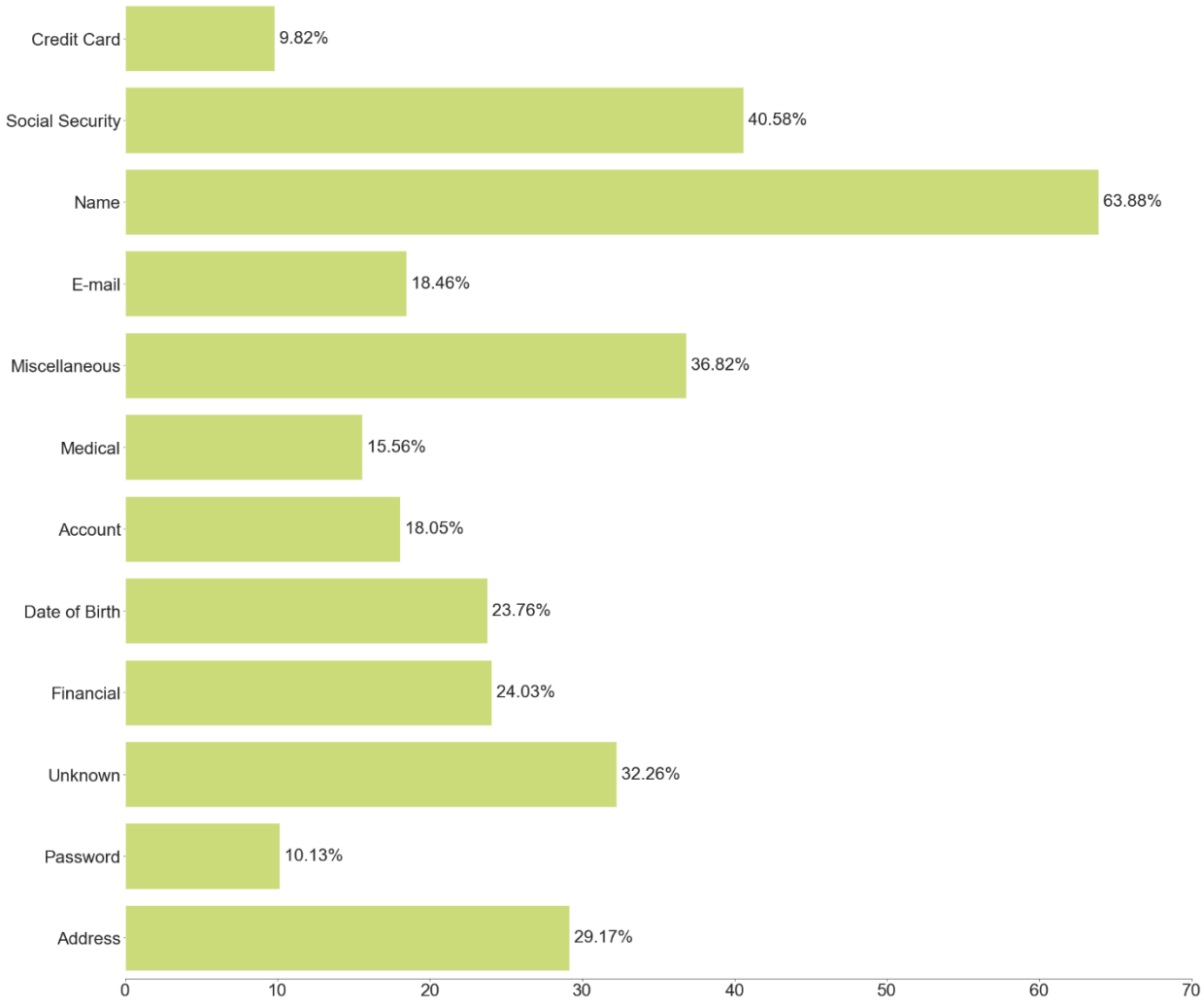
Year	Average Number of Days
2014	91
2015	70
2016	61
2017	49
2018	50
2019	72
2020	72
2021	89

Table 3: Average time interval between discovery and reporting

In the 2018 Year End Report, we took a closer look at the disclosure timeline. With GDPR regulations taking effect that year, significant attention was being given to the 72 hour deadline for informing data protection offices of the breach. The prevailing question at the time was whether this attention would impact how long it would take to go from initial discovery to the date of first public disclosure (though it should be noted, specific reports made to European regulators are generally not public information). Sadly, the progress that had been made in closing the gap between discovery and disclosure has only lengthened since that time. By 2021, the average number of days to disclose a breach had climbed to 89, just 2 days shorter than the high water mark set in 2014.

What Was Breached in 2021?

Figure 9: Data types exposed in breaches reported by EOY 2021



Just as ransomware operations are impacting the number of records exposed, the types of data contained in those records are also influenced by these attacks. With 874, or 21%, of the publicly reported breaches including a ransomware component, we see a broad range of data types compromised as well as Unknown/Unconfirmed data type appearing in 32% of breaches.

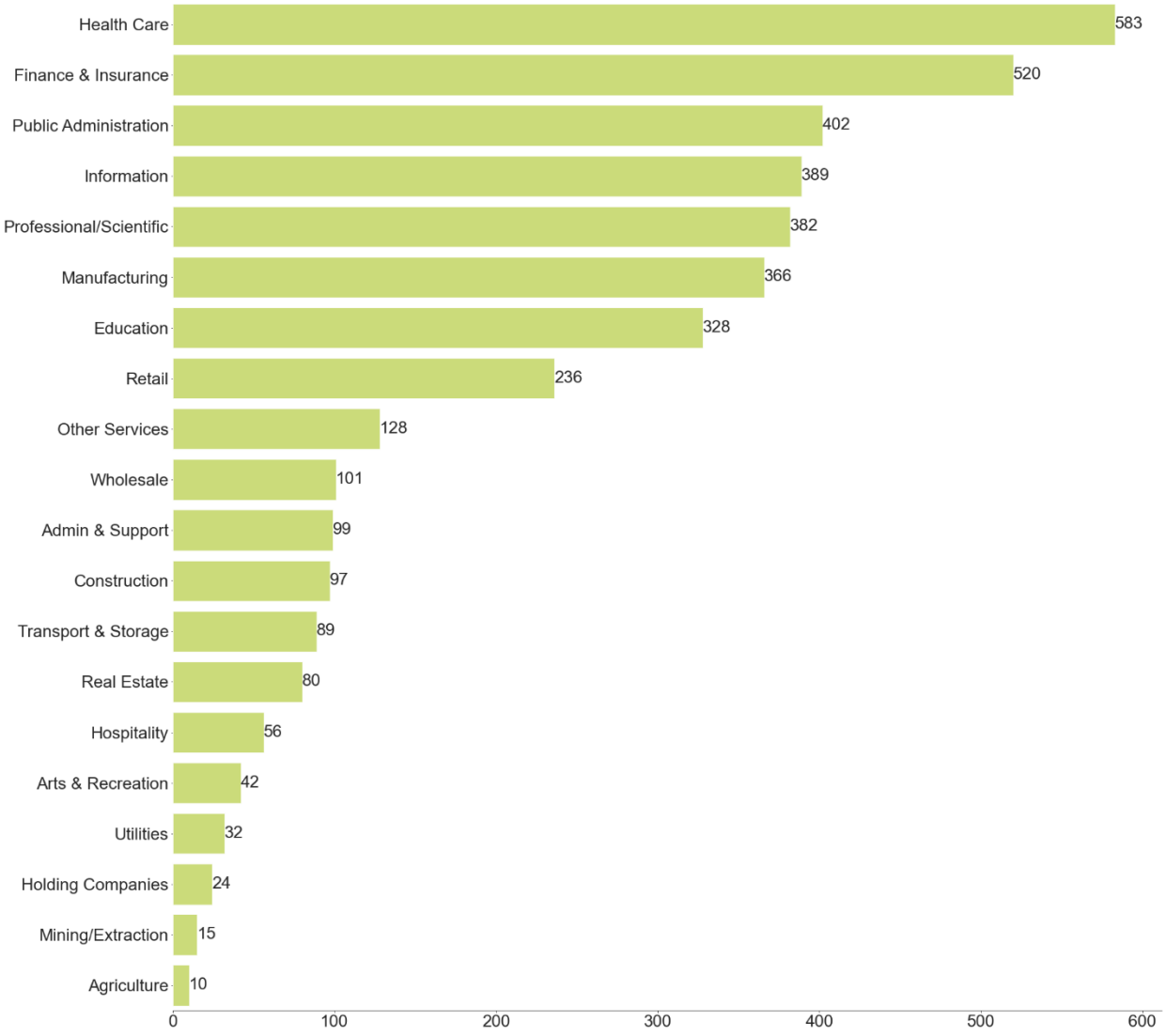
A notable trend over the past three years is the steady increase in the number of incidents that expose Social Security numbers or their non-U.S. equivalent. Digging deeper into this number, we see that during 2021 the breach types exposing this data do not vary significantly from the overall top 5 breach types. We were however surprised to find that the Manufacturing sector accounted for 11% of the breaches exposing Social Security numbers. While Finance/Insurance, Healthcare, and Professional Services topped the charts as the first, second and third economics sectors respectively that exposed Socials, Manufacturers beat out Education and Governmental entities.

Data	2021	2020	2019
Names	64%	51%	30%
SSN	41%	31%	15%
Misc.	37%	31%	23%
Unknown	32%	28%	12%
Address	29%	25%	14%
Financial	24%	18%	8%
DoB	24%	18%	10%
Email	18%	32%	62%
Accounts	18%	12%	9%
Medical	16%	14%	7%
Passwords	10%	25%	56%
Credit Cards	10%	12%	12%

Table 4: Top data types lost in breaches reported by EOY for the past three years

Who Was Breached in 2021?

Figure 10: Number of breaches by economic sector, reported by EOY 2021

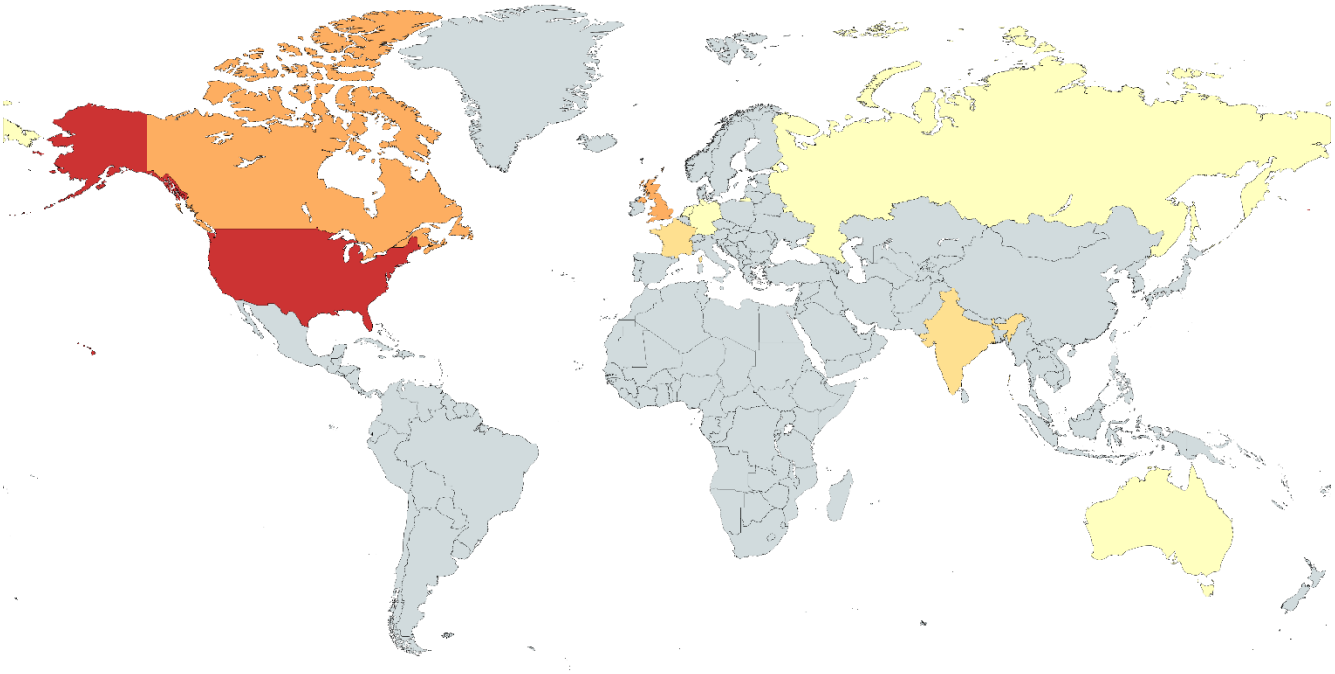


Not surprisingly, the Healthcare sector experienced the most breaches in 2021 followed closely by the Finance and Insurance sector. While landing at the top of the chart for most compromised economic sectors is not an enviable position, it is important to put the breach count into context. While Healthcare topped the list, the industry accounted for only 14% of reported breaches. Likewise, Finance and Insurance accounted for 12.5% and Government, taking third place, accounted for only 10% of breaches.

A closer examination of the Healthcare sector reveals that practitioners' offices contributed 40% to the sectors' total, with hospitals accounting for 28%, other facilities coming in at 19% and social services rounding out the sector contributing 13% of the breaches.

Where Did Breaches Occur in 2021?

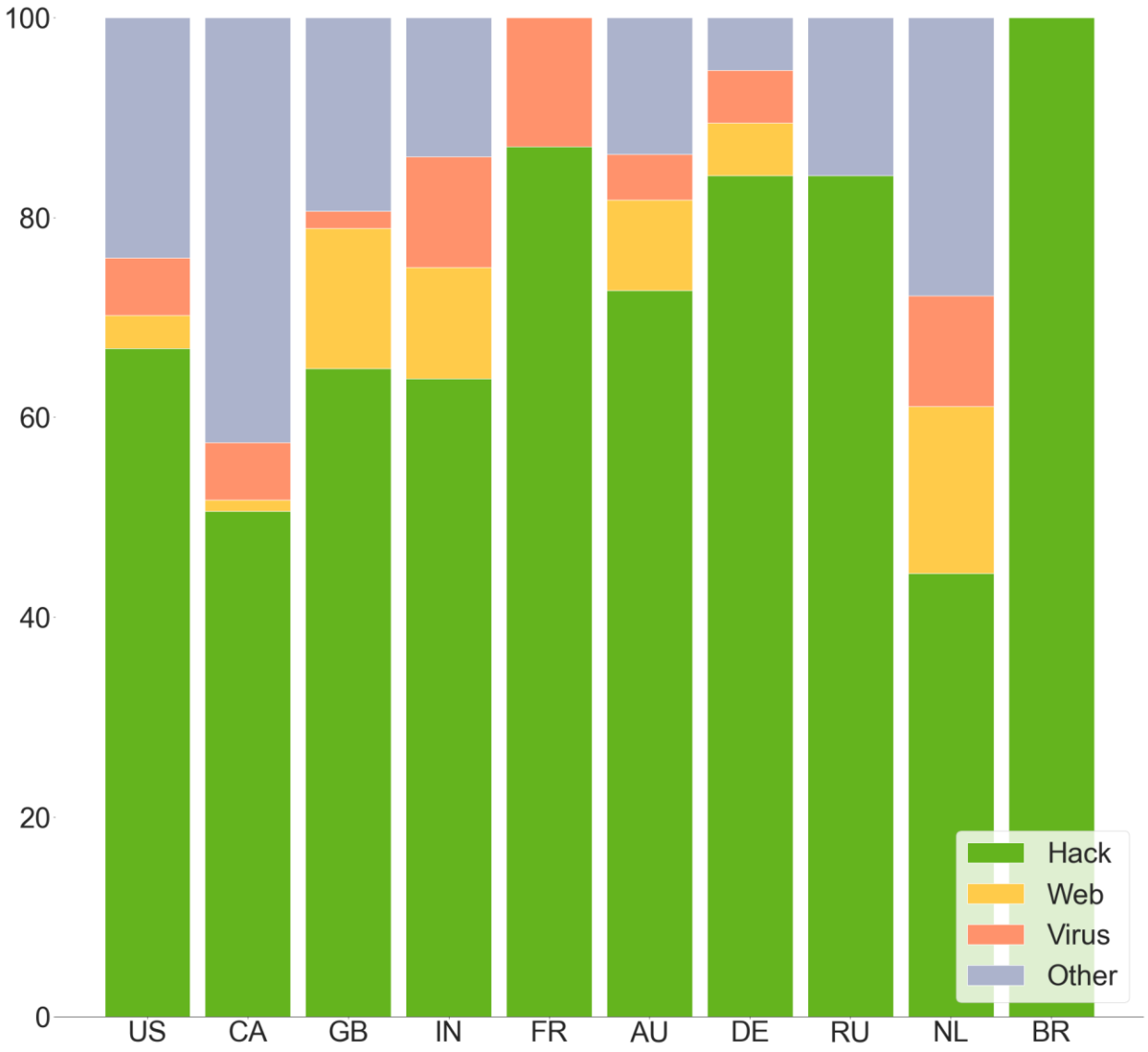
Figure 11: Distribution of breaches reported by EOY 2021



In keeping with prior years, the United States was home to the most breaches, accounting for 2,953 or 71% of incidents. This is due in part to the notification laws that require breach disclosures, as well as being the home to a significant number of high-value targets. While the overall number of breaches reported for 2021 is on par with 2020, the number of breaches reported in the United States increased 11.6% in 2021 compared to 2020.

USA	2,953
Canada	181
United Kingdom	125
France	79
India	71
Germany	53
Russia	42
Australia	39
Netherlands	33
All Other	569

Figure 12: Percentage of breaches by country, reported by EOY 2021



Are some countries home to more "hackable" organizations than others? It is a challenging question to answer, but breach type by country does reveal interesting results. The United States, while reporting the most breaches, experienced a wide variety of breach types, similar to the Netherlands and Canada. Other locations, like Brazil and France, mostly reported hacking or malware attacks.

In Closing

If 2020 was a rollercoaster ride, 2021 was more of the same, but perhaps with a little less surprise at the twists and turns that defined the year. As hopeful as we were that law enforcement's successes against ransomware operators would put a damper on activity, new groups formed, updated malware strains arrived on the scene, and operations continued after a short blip in late summer.

Accidental insider errors took a toll as well, contributing significantly to the number of records exposed during the year. What's more, these errors exposed highly sensitive information like Social Security numbers and their non-U.S. equivalent. Much talk has been given to how the pivot to work from home would create a field day for malicious actors. Perhaps so, but the stress of the past two years is surely playing a role too in the amount of data exposed.

What will be in store for 2022? It's difficult to say but one thing we can be sure of is that as long as malicious actors have a pathway to attack monetization, there will be no shortage of breaches to cover.

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.

The Risk Based Security Platform

Transform your information security program with truly risk-based, asset-centric intelligence.

REVEAL

the risks that apply to your organization.

PRIORITIZE

what impacts your assets, products and supply chain.

REMEDIATE

what matters most, coordinating across teams.

With actionable intelligence, evaluate and monitor vendors in real-time based on five-star risk ratings and comprehensive historical breach data.

LEARN MORE ABOUT “THE PLATFORM”

About Risk Based Security

Risk Based Security® (RBS) is a leading provider of Cybersecurity risk management solutions. The award-winning Risk Based Security Platform automatically correlates enterprise IT assets with comprehensive, independently-researched vendor, product and vulnerability intelligence from VulnDB® and Cyber Risk Analytics®. The result is better risk management outcomes, as well as time and cost savings. In addition, YourCISO® provides organizations with on-demand access to high quality security and information risk management resources in one easy to use web portal. Headquartered in Richmond, VA, RBS has been a trusted partner to many of the world's best known brands for more than a decade.

For more information, visit www.riskbasedsecurity.com, call +1 855-RBS-RISK, or follow us on Twitter at @RiskBased.

About Flashpoint

Trusted by governments and the Fortune 500, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners - including cyber threat intelligence (CTI), vulnerability management, DevSecOps and vendor risk management teams - rely on Flashpoint's intelligence platform to proactively identify and mitigate risk and stay ahead of the evolving threat landscape. To learn more about Flashpoint, visit https://www.flashpoint-intel.com/ or follow us on Twitter at @FlashpointIntel.

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
riskbasedsecurity.com/contact

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.