ForgeRock Consumer Identity Breach Report

As the Cost of Breaches Continues to Rise, Personally Identifiable Information Remains Primary Target

2020

Executive Summary

U.S. breaches cost over $1.8 trillion; more than 7.8 billion consumer records exposed over last two years

In 2019, Gartner estimated worldwide spending on information security-related products and services would be $124 billion[1] – increasing 8% from 2018. And the the number of consumers and organizations impacted by breaches and malicious attacks continues to grow. For the second year of this report, personally identifiable information (PII) was the most targeted data type in 2019, accounting for 98% of data – further highlighting the appeal of personal data to malicious actors.

Since the 2019 "ForgeRock Consumer Breach Report" was released with data from 2018, the average cost of a breach in the U.S. increased 112% to $8.19 million in 2019[2], up from $3.86 million. Also increasing in 2019 was the number of consumer records impacted – over five billion consumer records, up 78.57% from the 2.8 billion impacted in 2018.

As organizations recover from effects of the COVID-19 pandemic, the impact of these breaches extends beyond the bottom line. Consumers are leveraging their digital identity more than ever for tasks and online activities to maintain their daily lives, for everything from remote access to work applications to ordering groceries or takeout delivery. Protecting digital identities is no longer an afterthought for organizations; it is an immediate mandate to maintain trust with consumers and avoid costly breaches.

This report shares detailed insights and data on the breaches impacting consumers in 2019 and Q1 2020, as well as providing year-over-year comparisons to breaches affecting consumers in 2018 in the U.S. It also includes findings from other key regions including Australia, Germany, and the United Kingdom.

Some key U.S. findings in this year's report include:

- PII continues to be the number one data target for malicious actors, 98%.
- For the second year in a row, unauthorized access is the number one attack method by cybercriminals, 40%.
- Social Security numbers and date of birth records were the most targeted data, 37%.

In this report, the findings and trajectory for future data breaches expose the need for organizations to adopt a comprehensive identity and access management (IAM) solution, not only to avoid the associated costs of a breach, but also to protect consumer data and relationships.

[1] Gartner, Forecast: "Information Security and Risk Management, Worldwide, 2017-2023, 4Q19 Update"

[2] Cost estimated using total identified breaches with Ponemon Institute findings for the cost of a U.S. security breach, as reported in the "Cost of a Data Breach Report 2019"

Key U.S. Findings

5.05 B

Over 5.05 billion records were impacted in 2019, up 78.57% from 2018, which had 2.8 billion records impacted

$250 B

In 2019, the technology sector had the costliest impact of over $250 billion for more than 1.3 billion breached records

37%

Social Security numbers and date of birth details accounted for 37% of breached data, down from 54% in 2018

+83%

Total cost of breaches in 2019 was over $1.2 trillion, up 83.48% from $654 billion in 2018

43%

The healthcare industry was the most targeted, accounting for 43% of breaches

+8.9%

2020 is on track to exceed 2019 (Q1 2019: 1,609,459,158) in number of records breached with an 8.9% YoY increase

98%

PII accounted for 98% of all data breached in 2019

40%

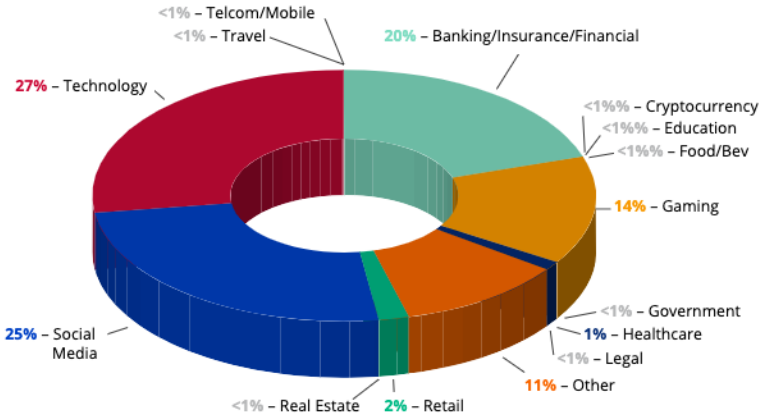
Unauthorized access was again the most common type of breach, 40%, up from 34% of all attacks in 2018

25%

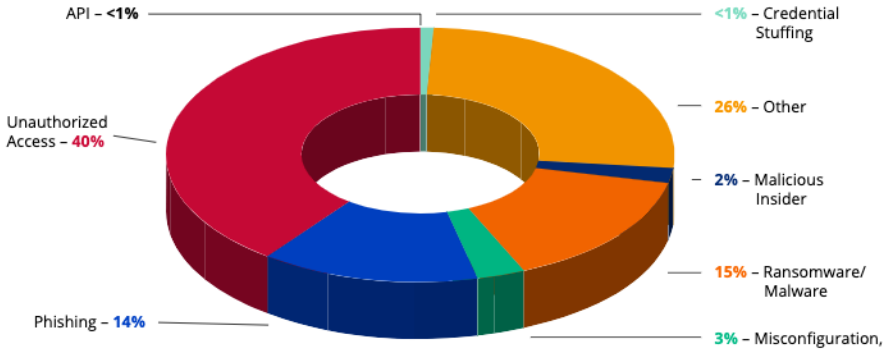
Medical details were the most targeted data type in Q1 2020, accounting for 25%

Attack and Data Types 2019

Total Records by Industry



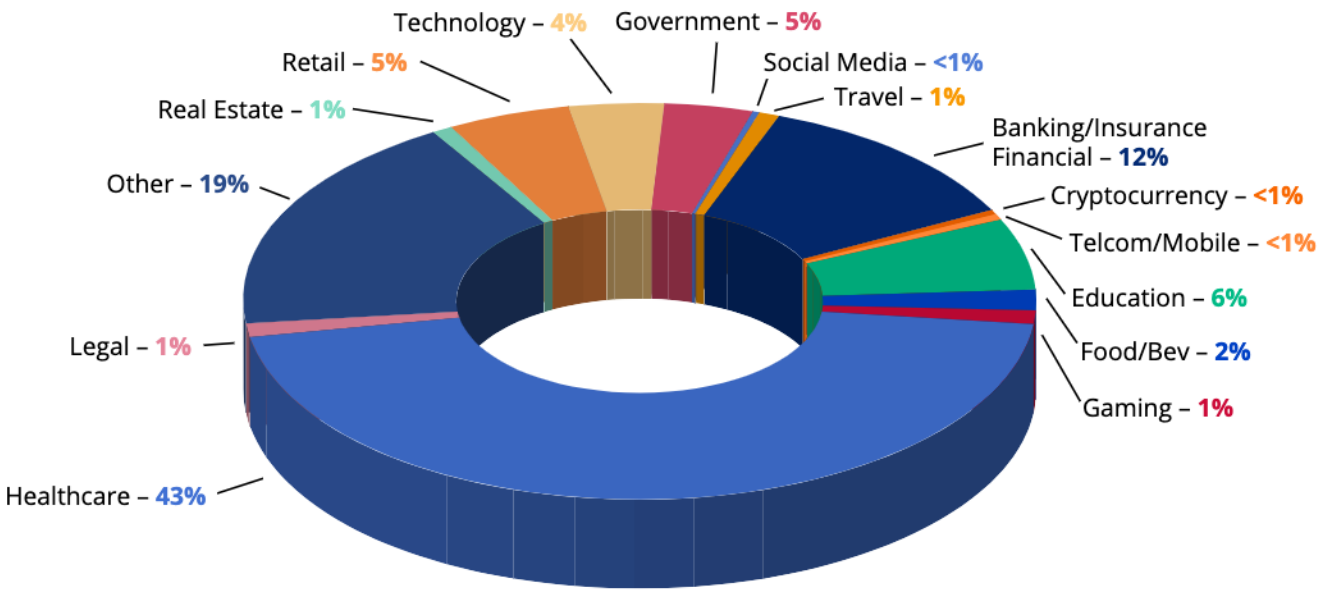
Totals by Vulnerability



- In 2019, unauthorized access was the most common type of breach, 40%, up from 34% in 2018.
  - This increase in unauthorized access attacks showcases the need for organizations to employ a sophisticated identity solution to prevent nefarious agents from accessing consumer data.
- Ransomware/malware was the second highest breach type in 2019 at 15%, down 2% from 2018.
- In 2019, phishing attacks overtook misconfigurations as the third most used attack type at 14% of all breaches.
- The number of SSN and DoB data breached in 2019 made up 37% of data breached, down from 54% in 2018, a 14.5% decrease.
  - However, the number of attacks targeting this data was up 37% from 2018.
  - This consumer data will continue to be a priority target for cybercriminals, as they look to leverage this data to open accounts, exploit it for ransom or use it to access other sensitive data, such as bank account information or health records.
- Name and address (18%) and personal health information (PHI) (17%) were the second and third most targeted data types, respectively.

Industry Breaches 2019

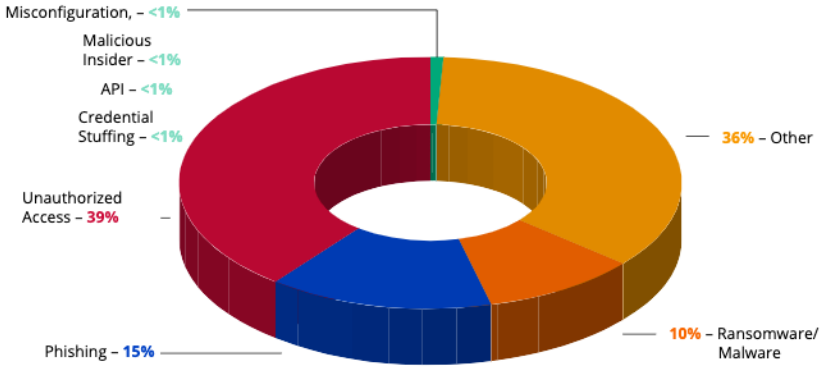
Total Breaches by Industry



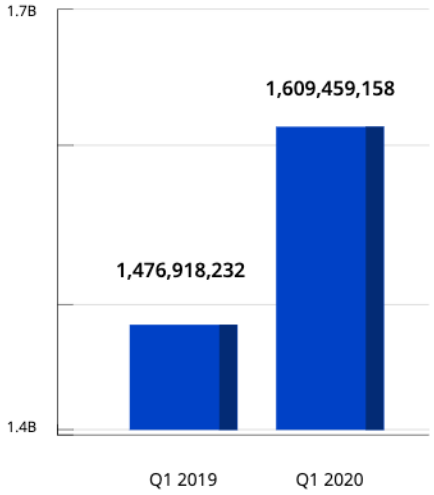
- In 2019, breaches cost the healthcare industry $17.76B, as each breached record cost $429, up 5.14% from $408 in 2018.
- Rounding out the top five industries impacted by number of breaches, after healthcare, are:
  - Banking/Insurance/Financial: 12%
  - Education: 7%
  - Government: 5%
  - Retail: 5%
- Healthcare was again the biggest target in 2019, comprising 43% of all breaches, followed by banking/insurance/financial at 12%.
- In 2019, while the healthcare industry had the highest number of breaches, the technology sector had the highest number of consumer records impacted at 1.37B. This goes to show that hackers are targeting fewer organizations in the technology sector but focusing on accessing more records with a single breach.

2020 Outlook: On Track to Overtake Number of Breached Records in 2019

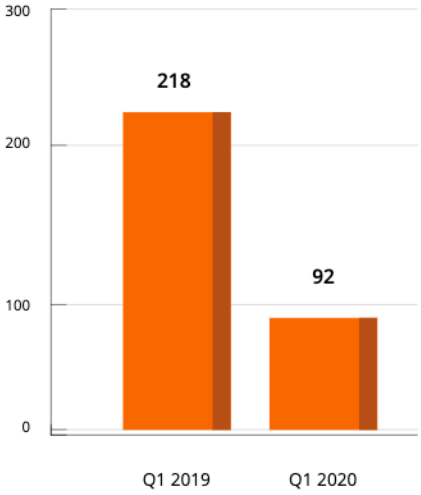
Totals by Vulnerability



Total Records Impacted



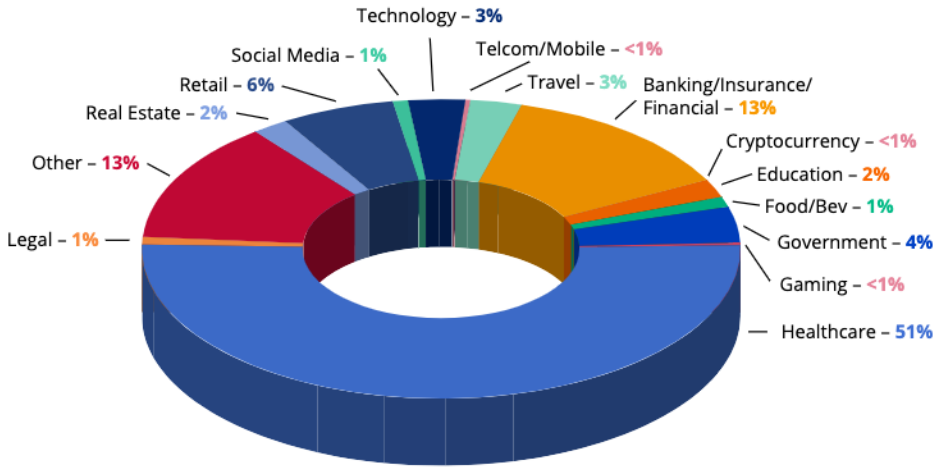
Total Breaches



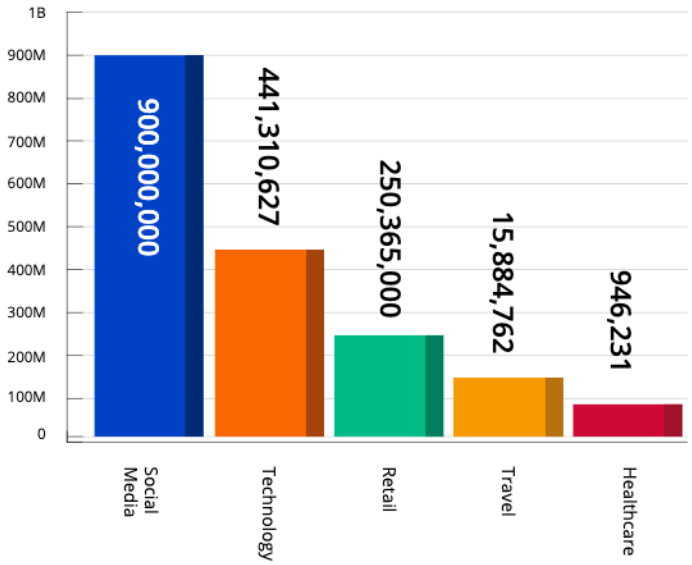
- Over 1.6 billion consumer records were impacted with these breaches – demonstrating 2020 is on track to top the more than five billion records impacted in 2019.
- In Q1, 2020 92 breaches occurred, and PII was again the most targeted type of data compromised at 96%.
- Compared to Q1 2019, the number of consumer records impacted is up 9% from 1.4 billion, even though total breaches are down 57.79%.
- Unauthorized access was the top method used to breach records in Q1 2020, accounting for 39% of the breaches.
- Phishing is the next most popular breach method at 15%. Phishing is likely to continue to be a top attack method in 2020, as malicious agents use this method to target consumers with false information on the COVID-19 pandemic.
- Cybercriminals targeted SSNs and DoBs the most in Q1 2020, making up 34% of data breached, with over 1.15 billion records breached that contained this data.
  - Medical records were the second most targeted in Q1 2020, accounting for 25%.

Industry Breaches 2020

Total Breaches by Industry



Top 5 Total Records by Industry



- Healthcare was the most breached industry in Q1 2020, at 51% of all breaches, and banking was the second most impacted industry, accounting for 13% of breaches. As more consumers are tested and treated for COVID-19, healthcare organizations will continue to be a target for malicious actors and must prioritize not only their patients' well-being, but their data protection as well.
- However, in Q1 2020, the most records were exposed from social media breaches, accounting for 56% of breached records.
  - Retail had over 400 million records breached – the second highest number of records impacted at 27%.
  - The technology industry accounted for 16% of records breached for the quarter.

International Perspectives

United Kingdom Data Security in Focus

With the second anniversary of the GDPR – Europe's flagship regulatory data standard – having just passed, now is the perfect time to reflect on its first full calendar year of operation in 2019. All across the U.K., businesses have been creating and embedding the responsible data protection practices which were first mandated on May 25, 2018. These efforts are now being accelerated due to the COVID-19 pandemic and the explosion in the amount of data being handled as work and life increasingly moves online.

GDPR has led to vast changes in attitudes on data security – with increasing awareness of the importance of protecting personal data at an organisational level and with individual consumers. For the first time ever, the general public is actively exercising their rights in cases of malpractice.

Coupled with the introduction of mandatory breach reporting, it is not surprising that the number of breaches reported to the U.K. regulator, the Information Commissioner's Office (ICO), increased – there were 14,000 between 25 May 2018 to 1 May 2019, an increase of nearly 324.24% from 3,300 over a similar period between 2017/18. Encouragingly, in 82% of these cases no further action – for example, further audits, mandated improvement action plans, or civil financial penalties - was required. This suggests breaches are being proactively and systematically reported.

This is supported by the fact that, according to the U.K.'s Department for Digital, Culture, Media & Sport (DCMS), 80% of businesses say cybersecurity is a high priority for senior management and board directors. Simply put, it appears that organisations are taking their data protection obligations seriously.

To ensure organisations continue to remain well informed and motivated, this report addendum reviewed the data available from U.K. regulatory bodies to highlight trends in consumer data breaches through 2019. Armed with this information and a robust identity and access management system which facilitates and manages secure access to the connected world, organisations will be able to gain assurance that their data is appropriately secured.

In 2019, healthcare was the most at-risk sector in both the U.K. and U.S., comprising 51.5% and 45% of total breaches, respectively. However, in contrast to the U.S. findings, in the U.K., according to the DCMS and ICO, phishing was the most common method of attack.

It's easy to see why the U.K. healthcare sector represents such an attractive target to malicious actors. The National Health Service (NHS) alone has access to 55 million high-quality primary care and 23 million specialist care records, with an estimated value of £9.6bn annually, per Ernst & Young. These data sets are a comprehensive and rich trove for cybercriminals, containing information on everything from patient names, addresses, treatments, and medical conditions to insurance records. Compared to personal health information can be extremely lucrative for malicious actors, selling for six times more. And, unlike PII, a lot of this information cannot be changed once the breach is detected.

Healthcare presents unique challenges due to the extent of sensitive data being shared in the complex and multi-partner clinical process. Medical facilities are often public, meaning devices are susceptible to physical tampering. And third-party risk arises from the long chain of medical partners, including labs, specialists, and doctors' surgeries. Each represents a vector for malicious attack.

However, more common than a technical entry point is the risk of humans being exploited (or exploiting from the inside), like targeted phishing attacks on professionals in the healthcare sector to gain access to legitimate credentials or to plant malware. Last year, the NHS said that its systems blocked nearly 12,000 phishing attacks a day.

Nearly 46% of U.K. businesses experienced a data breach in the last 12 months - and as our wider report demonstrates, the frequency and sophistication is only increasing year over year. The debate about the value of data breach defenses is over.

All U.K. organisations must, at a minimum, implement baseline measures. This can include anything from hiring security and compliance teams to frequent software patching to eliminate vulnerabilities, or adopting a zero-trust approach to all activity, and ensuring every user is verified and they are who they say they are - the ever-present threat of phishing makes this all the more important. Additionally, organisations must consider modern, intelligent authentication methods that move beyond simple username and password and provide fine-grained authorisation to protect and secure confidential data.

In the midst of the COVID-19 pandemic, healthcare organisations are especially high value targets for malicious actors, so the need to beef up defences is even greater.

The Information Commissioner's Office (ICO) also has a role to play in data breach prevention. While the organisation has used education and enforcement to reduce data breaches over the last year, there is still a lack of granular data available to the public and industry to help them research and understand this problem. As of May 2020, the ICO has not released the breakdown of nationwide data security incidents in Q4 2019, leaving the year of 2019 incomplete. The issue is even more stark when compared to other jurisdictions, like Australia, where comprehensive data sets are available. The access to this data must be made freely and widely available in a timely manner.

Germany Data Security in Focus

In 2019, more than 10,000 data breaches were reported in 2019 in Germany alone. According to surveys, there have been 37,636 breaches in Germany in the period since GDPR was introduced.

While Germany has had strict regulations on data protection since the 1970s, reporting a data breach in accordance with the criteria of Art. 33 GDPR is now a legal obligation. As a result of the reports, fines amounting to €114 million have been imposed by the European Data Protection Commissioners since May 2018. The fines in Germany alone amounted to a total of €24.5 million, or $26.5 million USD.

The reported data breaches in Germany can be divided into internal and external threats. Examples of internal threats are unprotected folders and human errors, such as misdirected letters, open e-mail distribution lists, improper disposal of files, and lost external storage devices, as well as programming errors. A quarter of all data breaches are due to technical system errors; 19% are due to human error.[7]

Virtually every German industry is affected. In addition to breaches in the healthcare system where patient data was sent to the wrong recipient by mistake or published online, large aviation or fashion companies have also had to deal with data leaks since the GDPR came into effect. Due to a technical malfunction in one of Lufthansa's frequent flyer programs, the customer data of other program participants was visible for a short time to 4,100 logged-in users. At an H&M customer centre, managers systematically collected personal data on the living situation of employees in unprotected data folders. The authorities subsequently evaluated around 60 gigabytes of data.

In November 2019, the Berlin data protection authorities imposed a fine of €14.5 million on a real estate company. The company had archived sensitive personal data such as self-disclosures, salary statements, excerpts from employment contracts, and tax, Social Security and health insurance data for years without deleting the data. Germany's small and medium-sized businesses (SMBs) seem to be particularly affected by the changes in the GDPR: one in 25 SMBs in Germany had reported a data breach by May 2019.

External threats are responsible for 56% of all data breaches in Germany[7]. These include, for example, malware sent by email or specifically targeted cyberattacks leveraging ransomware. All of these are included in the data breach statistics and remain one of the biggest and most expensive threats. The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) recorded almost 320,000 breaches per day in 2019. Not only is the number of incidents remarkable, but the amount of personal data that is leaked and published online is as well. Identity theft, in which personal data is used by third parties, leads to losses averaging €194 per data set. Popular forms of identity theft include phishing, the use of malware, or the use of unprotected, public cloud storage. Inadequately patched systems or zero-day exploits are also used to read out data.

In addition to office communication, production and manufacturing industries are also increasingly targeted by attacks. Digitalization and networking through Internet of Things (IoT) and Industry 4.0 increase the possibilities of attack in these industries. The threat level from botnets remains unchanged: up to 110,000 bot infections of German systems per day were registered by the BSI in 2019. More than half of all attacks are carried out via compromised or improperly hired cloud servers. This means that almost every cloud service provider has been misused at least once to carry out distributed denial-of-service (DDoS) attacks.

Data protection is especially important in times of crisis. New registration requirements and systems are currently being introduced quickly in many places, for example, in the healthcare system, causing many citizens to feel uninformed about how the state or their employers collect and use data during a crisis. Pseudonymisation and anonymisation procedures are exceedingly important, especially for medical and pandemic data.

Although fewer data breaches are currently being reported, those responsible expect malware to become more widespread soon. Many remote workers connect to the Internet outside of a professional IT infrastructure, increasing the risk of errors or data misuse – not only for their own data but for data they're processing for consumers. In addition, phishing campaigns are generally geared to current social events and trending topics, so COVID-19 offers an ideal opportunity to attack.

In Germany, more than three million companies, plus state institutions and other bodies, are subject to the obligation to report data breaches under Art. 33 GDPR. This suggests that, despite the increased transparency and sense of duty – especially compared with other EU countries – the number of data breaches should realistically be much higher. Additionally, it can be assumed that data protection requirements will become even more comprehensive and complex in the future, as ongoing digitalization projects open up new potential areas of attack in many sectors. Nevertheless, the reported data leaks in Germany demonstrate that digital personal responsibility of everyone – private user or company – is an essential component for data collection and security now and in the future.

[3] https://www.dlapiper.com/en/germany/insights/publications/2020/01/gdpr-data-breach-survey-2020/
[4] https://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.251507.de
[5] https://www.bdsg-externer-datenschutzbeauftragter.de/datenschutz/datenpannen/
[6] https://www.dlapiper.com/en/germany/insights/publications/2020/01/gdpr-data-breach-survey-2020/
[7] Ponemon Institute, IBM „Cost of a Data Breach" study, 2019
[8] https://www.gdv.de/de/medien/aktuell/ein-jahr-eu-datenschutz--jeder-25--mittelstaendler-musste-bereits-datenpanne-melden-47882
[9] Ponemon Institute, IBM „Cost of a Data Breach" study, 2019
[10] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4
[11] Ponemon Institute, IBM „Cost of a Data Breach" study, 2019

Australia Data Security in Focus

There was a 22% increase in the number of data breaches reported to the Office of the Australian Information Commissioner (OAIC) from 2018 to 2019, jumping from 812 to 997. Increases in data breaches between 2018 to 2019 were consistent across contact information, identity Information, health information, financial details, and tax file numbers.

Data breaches involving health information saw the biggest increase between 2018 to 2019, with a 23.7% year-on-year increase. Data breaches involving contact information also saw a sharp increase between 2018 and 2019, with 17.3% increase year-on-year. Contact information like home addresses, phone numbers or email addresses remained the most frequently sought-after information involved in data breaches, followed by financial details.

Health service providers (the health sector) reported 222 data breaches during the reporting period. This sector has consistently reported the most data breaches compared to other industry sectors since the start of the notifiable data breaches (NDB) scheme. Similarly, the finance sector reported the second highest amount of data breaches during the report period, recording 146 in total.

With human error the second leading cause of data breaches in 2019, behind malicious or criminal attacks, it's clear that Australian businesses must invest in consolidated identity management strategies for both customers and employees to ensure they are secure on all levels of operation.

Australians also must be more wary of signing up to unnecessary services and supplying the same information, over and over again. The 817 data breaches in 2019 included contact information like an individual's home address, phone number or email address, and when this information is compromised in conjunction with identity information, like an individual's passport number, driver licence number or other government identifiers, it is much easier for cybercriminals to carry out elaborate identity thefts.

In light of the increasing number of data breaches between 2018 and 2019 alone, and human error standing out as the second-highest cause of data breaches in 2019, it's clear that industry, government, and regulators must come together to educate Australians on how to best manage their digital identities and develop consolidated platforms that minimise how often Australians have to submit the same information for different services.

Australian References

2019 OAIC Notifiable Data Breaches Reports:

- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-quarterly-statistics-report-1-january-31-march-2019/
- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019/
- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/

2018 OAIC Notifiable Data Breaches Reports:

- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-january-to-31-march-2018/
- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2018/
- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-july-to-30-september-2018/
- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-october-to-31-december-2018/
- https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

ForgeRock

Conclusion

In 2019, many organizations faced their first full year of General Data Protection Regulation (GDPR) enforcement or impending California Consumer Privacy Act (CCPA) enforcement, or both. Additional mandates and market pressures related to security, such as Open Banking in the financial services sector, continue apace. Yet even as organizations invest billions into security solutions and services, cybercriminals continue to advance their tactics and means of accessing precious consumer data – with no sign of slowing down.

The trend from 2018 into Q1 of 2020 shows that these cybercriminals remain focused on targeting consumer PII. Even the most seemingly harmless piece of data can be combined with other sources of information to result in serious compromise. Service providers should help consumers avoid providing unnecessary copies of data by adhering to the privacy principle of data minimization. Additionally, they can provide users with greater transparency and control in how information is collected and used through a comprehensive consent and permissions management approach.

Data breaches are increasingly caused by unauthorized access, which is a symptom of poor access management. In the U.S., fully 40% of breaches were caused by unauthorized access in 2019, and Q1 2020 shows the same trend. This can be a problem caused by either malicious actors from outside or inadvertent access by inappropriate actors inside an organization. In both Germany and Australia, human error – an internal threat – was noted as a challenge. Employing a comprehensive identity and access management solution is the best approach for preventing access in cases of both internal and external threats.

At the same time, there are signs that phishing is on the rise as an attack method. In 2019, phishing rose to become the third most frequent attack type in the U.S., and in Q1 2020 it rose again to the second most frequent. Phishing is likely to continue to be a popular attack method in 2020, as malicious agents use it to target consumers with false information on the COVID-19 pandemic. Using adaptive, context-aware authentication methods can help to combat this threat without negatively impacting the consumer experience.

Across the globe, it's clear that healthcare information continues to be a lucrative hunting ground for cybercriminals. In 2019, the U.K.'s National Health Service (NHS) fended off nearly 12,000 phishing attacks a day. In Australia, the sector has reported the most data breaches compared to others every year since 2017. In the U.S., healthcare has remained the top breach target since the previous year's report, with breaches costing the industry nearly $18B and personal health information commanding a 6x premium. Already in Q1 2020, the sector is outpacing all others and its own previous track record, at over half (51%) of breaches. The ongoing pandemic and the resulting explosion of telehealth practices, as well as new health-related apps for people to download and try, are accelerating security risks. Taking a Zero Trust approach to security, which emphasizes controlling access in a dynamic and adaptive fashion within a closely circumscribed perimeter around the protected resource, is a best practice.

Knowing the value of consumer data, both to the owner and cybercriminals, these statistics show that organizations must elevate their digital identity management strategies to protect consumer data, as well as their brand reputation.

What specifically should organizations be looking for?

The right digital identity solution should enable the orchestration of user identity journeys, like registration and authentication, in a convenient way that unifies the controls for security and user experience. It should enable access to be controlled close to each application, as befits Zero Trust, with context from authentication feeding into authorization. And it should enable the enterprise to protect personal data in a transparent fashion and extend control of data consent and permissions in a way that is unified for each user, increasing their confidence in the service provider.

Identity governance is a key part of preventing unauthorized access. The right approach leverages cloud and AI/ML to create intelligent governance solutions. It utilizes the vast amounts of data that a company already possesses as an input to learning and predicting good access. It allows organizations to employ a portfolio of machine learning models. It also allows the flexibility to ingest large amounts of data from the various data sources that are available. Most of all, the right solution actually reduces effort and unlocks value from current IAM investments.