FORGEROCK

U.S. Consumer Data Breach Report 2019

Personally Identifiable Information Targeted in Breaches that Impact Billions of Records

Executive Summary

2.8 billion consumer data records were exposed at an estimated cost of more than $654 billion*

Despite enterprises' worldwide investments in information security products and services estimated at more than $114 billion in 2018 – an increase of 12.4% from 2017 – compromises of consumer data abound. Consumer personally identifiable information (PII) data remains the holy grail of cybercriminals, and given that enterprises across a wide range of industries – including healthcare, government, and financial services – store and manage billions of consumer data records, these organizations are consistently under siege from cyberattacks.

In 2018 alone, 2.8 billion consumer data records were exposed at an estimated cost of more than $654 billion*. The long-term effects of data breaches, such as loss to reputation, reduced customer loyalty and other soft costs are hard to estimate, but should not be ignored. By orders of magnitude, PII was the most targeted type of consumer data in 2018, and unauthorized access to that data was the most frequent cause of breaches.

This report provides in-depth insights into consumer data breaches executed in the U.S. in 2018 and Q1 2019. The findings highlight three trends: PII is overwhelmingly the most attractive type of consumer data to cybercriminals; cybercriminals' most effective attack method is unauthorized access; and healthcare is the most targeted industry.

The report's results illustrate the gaps in enterprises' identity and access management (IAM) practices, underscoring why robust IAM is a critical requirement for securing consumer data and access across the modern enterprise.

*Estimated using total number of breaches identified alongside Ponemon Institute findings for costs of U.S. security breaches as reported in "2018 Cost of a Data Breach Study: Global Overview."

Key Findings

2.8 B

In 2018, more than 2.8 billion consumer data records were exposed in 342 breaches – at an estimated total cost of more than $654 billion

97%

Personally identifiable information was the leading type of data breach in 2018, comprising 97% of all breaches

54%

Date of birth and/or Social Security Numbers were the most frequently compromised type of PII in 2018, with 54% of breaches exposing this data

34%

Unauthorized access was the primary type of attack in 2018, totaling 34% of all attacks

48%

Healthcare was the most affected industry, with the sector falling victim to 48% of all breaches

$6.2 B

In Q1 2019, financial services breaches cost the industry $6.2 billion, up from just $8 million in Q1 2018

$114 B

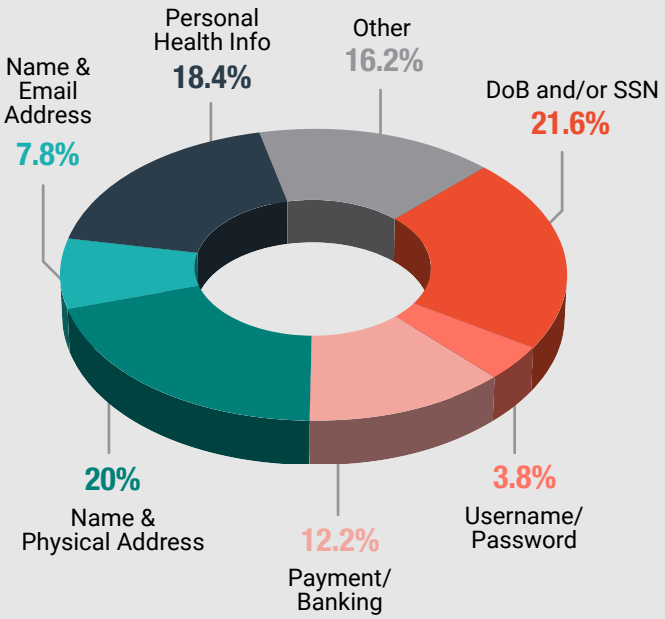
$114B invested by enterprises in information security products and services in 2018; a 12.4% increase from 2017

FORGEROCK

2018 Breaches at a Glance: U.S.

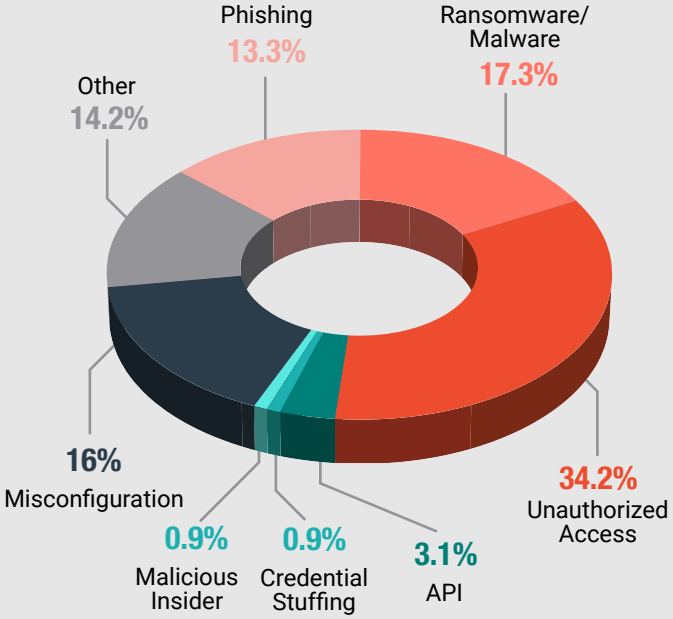
Breach Types

Types of Data Exposed in Every Breach



Attack Types

Number of Attacks by Type



- Personally identifiable information (PII) was by far the most common type of breach in 2018, representing 97% of all breaches.
- Date of birth (DOB) and/or Social Security Numbers (SSN) were the most frequently compromised type of PII in 2018, with 54% of breaches exposing this data.
- Further, the leaking of critical data points like DOB and/or SSN can lead to malicious actors taking over other critical accounts, such as bank accounts and credit lines.
- Name and physical address (49%) and personal health information (46%) were the second and third most commonly compromised type of PII.

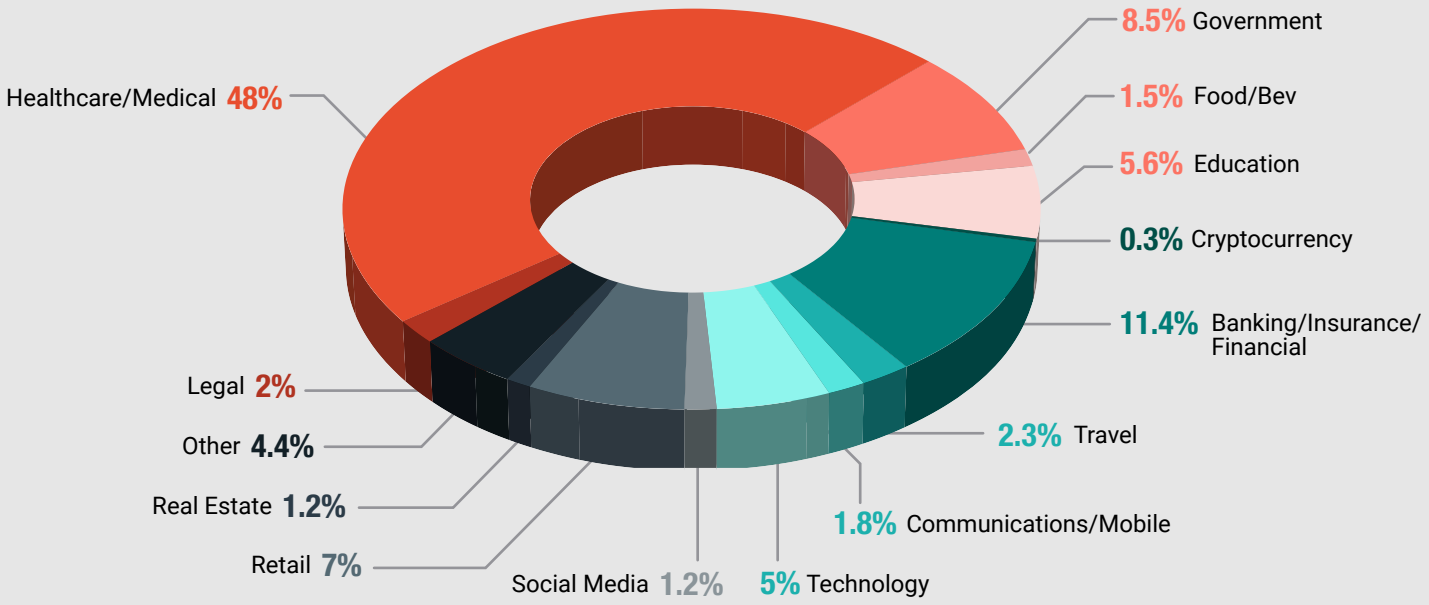
- Unauthorized access was the most popular type of attack in 2018 by a significant margin, comprising 34% of all attacks.
- The frequency of unauthorized access attacks underscores the critical role identity and access management plays in securing the enterprise.
- Ransomware/malware was the second most frequent attack in 2018; an expected outcome given the popularity of ransomware attacks in the healthcare industry.

FORGEROCK

2018 Breach Targets at a Glance: U.S.

Breaches by Industry

Number of Breaches by Industry

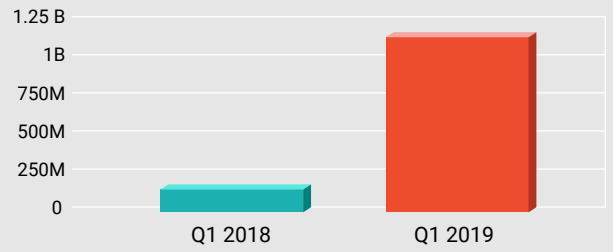


- The healthcare industry suffered more than four times the number of breaches as any other industry in 2018, equivalent to almost half (48%) of all breaches.
- Healthcare organizations store and manage massive amounts of PII, making them a highly attractive target for cybercriminals.
- The healthcare industry has traditionally lagged in modernizing IT due to its strict regulatory environment. Further, focus on usability improvements to drive adoption for non-technical audiences have at times outpaced security measures. With new mandates for electronic health records and increased awareness by consumers around data breaches, this trend is slowly shifting to re-focus on security.
- Banking/insurance and government were the second and third most victimized industries, collectively comprising 20% of all breaches.
- It is critical to note that the industries that reported lower breach numbers are by no means immune to breaches – data protection should be a concern for all businesses, regardless of industry sector. Criminals today have “easier” and more profitable targets in other industries, but as they modernize their identity management approaches, malicious actors will look to new sectors to cash in.

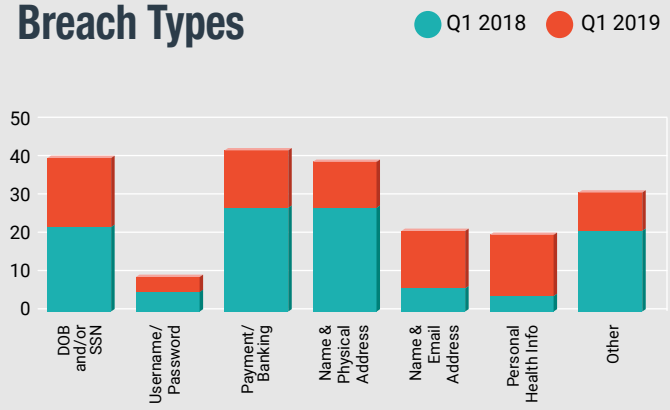
FORGEROCK

Q1 2018 vs. Q1 2019: U.S.

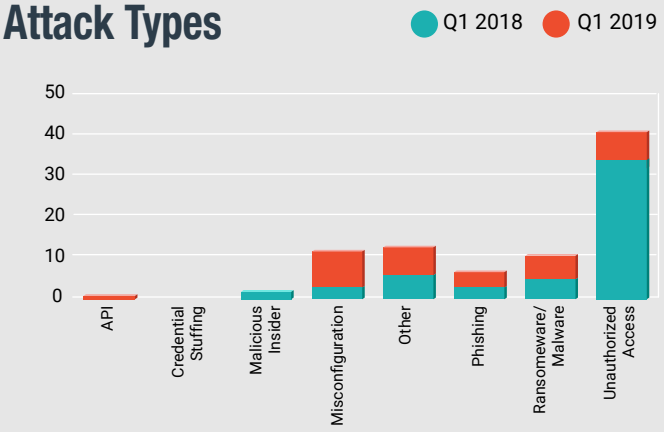
Records Accessed



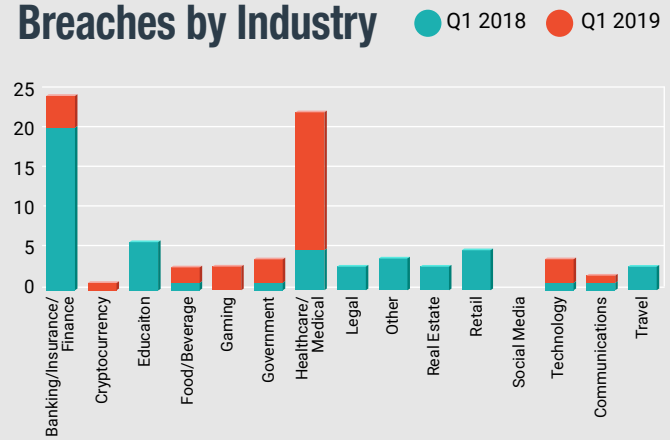
Breach Types



Attack Types



Breaches by Industry



- While there were fewer breaches in the financial sector reported in Q1 2019 (4 down from 20 in Q1 2018), the number of records impacted by these breaches grew significantly, by 78,900%. This resulted in an increase of leaked payment and banking-related personally identifiable information (PII).
- Following the trend seen across 2018, date of birth and/or Social Security Number and name and physical address were among the top most frequently-compromised data types.
- In Q1 2019, the higher number of healthcare-related breaches resulted in a high incidence of personal health information exposure, an increase of 400% over Q1 2018.
- While unauthorized access was the most frequent attack type in Q1 2018, misconfigurations were the leading cause of breaches in Q1 2019.

FORGEROCK

Conclusion

No industry is safe from cyberattacks, and the healthcare sector is particularly vulnerable to these hugely damaging breaches.

Cybercriminals today are highly sophisticated, executing a diverse range of security attacks at a greater volume and scale than ever before. While enterprises continue to invest heavily in information security products and services to defend against these threats, they are struggling to neutralize cybercriminals' unending appetite for consumer data.

Although cybercriminals target a wide range of consumer data and use a variety of methods to steal it, they are overwhelmingly seeking PII and are primarily using unauthorized access to obtain it. It is critical to emphasize that no industry is safe from cyberattacks, and the healthcare sector is particularly vulnerable to these hugely damaging breaches.

Given these findings and the highly confidential nature of consumer data, it is essential that enterprises critically evaluate their IAM strategies, practices, and solutions to ensure they are adequately protecting their massive volumes of consumer data. At a minimum, enterprises need to consider modern, intelligent authentication methods that move beyond simple username and password and provide fine-grained authorization to protect and secure resources. This needs to be a top priority for enterprises of all types and industry sectors, as the evidence is clear that cybercriminals show no sign of slowing down.

METHODOLOGY

ForgeRock compiled information on electronic consumer data breaches that were reported between January 1, 2018 and March 31, 2019 that have a known number of people or data records impacted.

Recommendations

For Businesses

- Opportunities directly correlate with user risk. For instance, a location service requires a user's location while the service is being used, but everything beyond that point might count as a risk to be mitigated. Be clear with why certain pieces of personal data are being collected and how they will be used.
- Education: Conceive of personal data as a joint asset and make this a mindset shift within your business. Not every unit within an organization will have the incentive structures to be mindful of data subject rights and is focused on the same goals.
- Consent: "lean in to consent". It is one of six lawful bases for processing personal data defined by the GDPR. Consumer consent gives an organization various freedoms and responsibilities and is the basis for building trusted, transparent digital relationships.

For Consumers

- Recognize that each of your login accounts represents a whole new opportunity for hackers to cause mischief when it comes to your personal data. You have a strategy for keeping your home and valuables safe, so why not your data?
- If your digital life threatens to be overrun with passwords, consider using a quality password manager (look for "encryption on the device"), using a strong passphrase to unlock it, and letting it generate and remember strong account passwords for you.
- Many businesses are making it possible for you to turn on account features such as "two-factor authentication" and notifications of suspicious account activity to help you become a partner in keeping your own valuable digital assets safe. Easy-to-use strong authentication methods are a good sign that a business has a good understanding of what it takes to become trustworthy.
- Finally, when assessing whether apps are safe for yourself or your children to use, it's valuable – if frustrating – to read the privacy policy but even more valuable to ask yourself just how the company makes it money. "Free" sites and apps still require payment in attention (ad viewing) or data (your personal data or user-generated content, such as status updates), or more likely both – and they might have in-app purchase features, too. You need to decide what you're up for, with eyes wide open.