Data Breach Statistics for 2021

What is a Data Breach?

- A data breach is any incident where confidential or sensitive information has been accessed without permission.

- Breaches are the result of a cyberattack where criminals gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within.

- The U.S. Department of Justice defines a breach as “the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access, to data, whether physical or electronic.”

_____

Common cyber attacks used in data breaches

- Ransomware:
    - Ransomware is software that gains access to and locks down access to vital data. Files and systems are locked down and a fee is demanded commonly in the form of cryptocurrency.
    - Common Target: Enterprise companies and businesses

- Malware:
    - Malware, commonly referred to as “malicious software,” is a term that describes any program or code that harmfully probes systems.
    - The malware is designed to harm your computer or software and commonly masquerades as a warning against harmful software
    - The “warning” attempts to convince users to download varying types of software, and while it does not damage the physical hardware of systems, it can steal, encrypt or hijack computer functions.
    - Malware can penetrate your computer when you are navigating hacked websites, downloading infected files or opening emails from a device that lacks anti-malware security.
    - Common Target: Individuals and businesses

- Phishing
    - Phishing involves sending fraudulent emails that appear to be from a reputable company, with the goal of deceiving recipients into either clicking on a malicious link or downloading an infected attachment, usually to steal financial or confidential information.
    - Common Target: Individuals and businesses

    - Denial of Service
        - Denial of Service is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
        - It is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.
        - Common Target: Sites or services hosted on high-profile web servers such as banks

_____

Recent Data Breaches + Statistics

On April 14, 2020, the credentials of over 500,000 Zoom accounts were found for sale on the dark web.

IdentityForce

With 3,950 confirmed data breaches in 2020, we’ve outlined some of the most recent and impactful security breaches of the year. This data indicates the recency and widespread impact data breaches are having on compromising sensitive information.

1. On January 22, 2020, a customer support database holding over 280 million Microsoft customer records was left unprotected on the web (IdentityForce).
2. On February 20, 2020, Over 10.6 million hotel guests who have stayed at the MGM Resorts have had their personal information posted on a hacking forum (IdentityForce).
3. On April 14, 2020, the credentials of over 500,000 Zoom teleconferencing accounts were found for sale on the dark web (IdentityForce).
4. On July 20, 2020, An unsecured server exposed the sensitive data belonging to 60,000 customers of the family history search software company, Ancestry.com (IdentityForce).
5. On August 20, 2020, Researchers at Comparitech uncovered an unsecured database with 235 million Instagram, TikTok, and YouTube user profiles exposed online belonging to the defunct social media data broker, Deep Social (IdentityForce).
6. On November 5, 2020, a database for Mashable.com containing 1,852,595 records of staff, users, and subscribers data was leaked by hackers (IdentityForce).
7. On December 10, 2020, an undisclosed number of users of the audio streaming service, Spotify, have had their passwords reset after a software vulnerability exposed account information (IdentityForce).

8. On February 18, 2021, the California Department of Motor Vehicles (DMV) alerted drivers they suffered a data breach after billing contractor, Automatic Funds Transfer Services, was hit by a ransomware attack (IdentityForce).

COVID-19 Specific Data Breaches

Scams increased by 400% over the month of March (2020), making COVID-19 the largest-ever security threat.
ReedSmith

2020 was a year like no other with COVID-19 severely impacting industries in every corner of the globe.

This opened the pathway for cybercriminals who were able to target vulnerable victims in the healthcare industry, as well as those who were unemployed or remote workers.

Here are a few of the most impactful data breach statistics related to the pandemic.

1. Remote work during COVID-19 increased data breach costs in the United States by $137,000 (IBM).
2. 54% of organizations required remote work in response to COVID-19 (IBM).
3. 76% of participants said remote work would increase the time to identify and contain a data breach (IBM).
4. Estimates show there have been as many as 192,000 coronavirus-related cyberattacks per week in May 2020 alone, a 30% increase compared to April (Unisys).
5. In 2020, 98% of point of sale data breaches in the accommodation and food services industry were financially motivated (Verizon).
6. Confirmed data breaches in the healthcare industry increased by 58% this year (Verizon).
7. Web application breaches account for 43% of all breaches and have doubled since 2019 (Verizon).
8. 33,000 unemployment applicants were exposed to a data security breach from the Pandemic Unemployment Assistance program in May (NBC).
9. A data breach of the federal disaster loan applications impacted 8,000 small business owners exposing their applications (U.S. PIRG).
10. Scams increased by 400% over the month of March, making COVID-19 the largest-ever security threat (ReedSmith).

Breaches by the Numbers

By stealing only 10 credit cards per website, cyber criminals earn up to $2.2 million through formjacking attacks.

Symantec

There are many factors to consider when preparing for and managing a data breach, like the amount of time it takes to respond to a data breach and the reputational impact it has on your company.

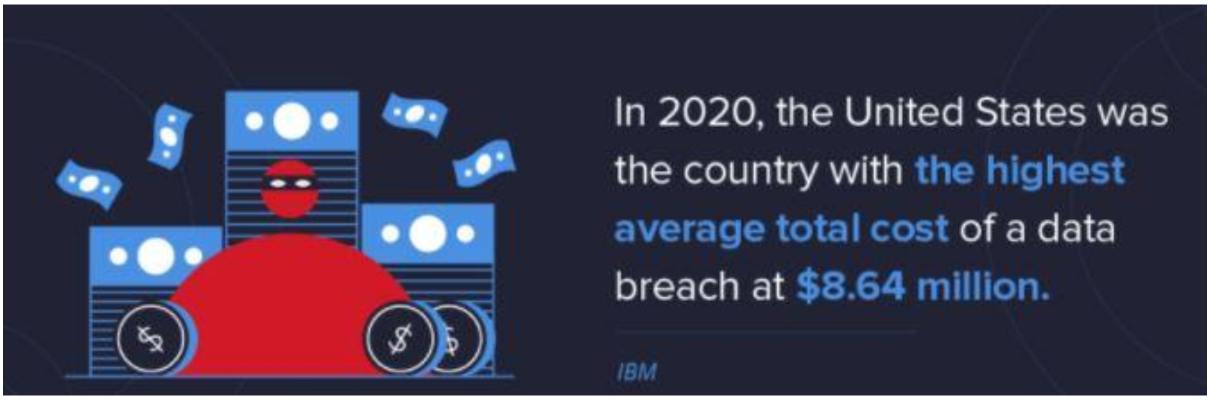
How Breaches Happen

1. An average of 4,800 websites a month are compromised with form-jacking code (Symantec).
2. 34% of data breaches in 2018 involved internal actors (Verizon).
3. 71% of breaches are financially motivated (Verizon).
4. Ransomware accounts for nearly 24% of incidents where malware is used (Verizon).
5. 95% of breached records came from the government, retail, and technology in 2016 (Tech Republic).
6. 36% of external data breach actors in 2019 were involved in organized crime (Verizon).

Average Response Time and Lifecycle

1. The average time to identify a breach in 2020 was 228 days (IBM).
2. The average time to contain a breach was 80 days (IBM).
3. Healthcare and financial industries spent the most time in the data breach lifecycle, 329 days and 233 days, respectively (IBM).
4. The data breach lifecycle of a malicious or criminal attack in 2020 took an average of 315 days (IBM).
5. 48% of malicious email attachments are Microsoft Office files (Symantec).
6. From 2016 to 2018, the most active attack groups targeted an average of 55 organizations (Symantec).

Cost of a Data Breach



In 2020, the United States was the country with the highest average total cost of a data breach at $8.64 million.

IBM

Direct expenses include forensic experts, hotline support and providing free credit monitoring subscriptions and potential settlements.

Indirect costs include in-house investigations and communication, as well as customer turnover or diminished client acquisition rates due to companies’ reputations after breaches. Some example are:

1. Healthcare is the most expensive industry for a data breach at $7.13 million (IBM).
2. The global average cost of a data breach is $3.86 million (IBM).
3. The average cost per lost or stolen record in a data breach is $150 (IBM).
4. A breach lifecycle under 200 days costs $1 million less than a lifecycle over 200 days (IBM)
5. 39% of costs incurred more than a year after the data breach (IBM).
6. In 2020, the country with the highest average total cost of a data breach was the United States at $8.64 million (IBM).
7. A mega breach of 1 million to 10 million records has an average total cost of $50 million, a growth of 22% from 2018 (IBM).
8. A mega breach of 50 million records has an average total cost of $392 million, a growth of almost 12% from 2018 (IBM).
9. Hospitals spend 64% more annually on advertising over the two years following a breach (American Journal of Managed Care).

Data Breach Risk

53% of companies found over 1,000 sensitive files accessible to every employee.

IBM

IBM’s Cost of a Data Breach Report found that the average total cost of a data breach is $3.86 million and moving in an upward trend.

See the data breach risk statistics below to help quantify the effects, motivations and causes of these damaging attacks.

1. A financial services employee has access to 11 million files (Varonis).
2. The average distributed denial-of-service (DDoS) attack grew to more than 26Gbps, increasing in size by 500% (Nexusguard).
3. In the first quarter of 2020, DDoS attacks rose more than 278% compared to Q1 2019 and more than 542% compared to the last quarter (Nexusguard).
4. 9,637 attacks were between 10Mbps and 30Mbps (Nexusguard).
5. Over 64% of financial service companies have 1,000+ sensitive files accessible to every employee (Varonis).
6. On average, 50% of user accounts are stale (Varonis).
7. 58% of companies found over 1,000 folders that had inconsistent permissions (Varonis).
8. Only 5% of a company’s folders are protected (Varonis).
9. 38% of all users sampled have a password that never expires (Varonis).
10. 28% of data breach victims are small businesses (Verizon).
11. Over 80% of breaches within Hacking involve Brute force or the Use of lost or stolen credentials. (Verizon).
12. A cyberattack occurs every 39 seconds (University of Maryland).
13. The larger the data breach, the less likely the organization will have another breach in the following two years (IBM).
14. 23% of data breaches are caused by human error (IBM).
15. 62% of breaches not involving an error, misuse, or physical action involved the use of stolen credentials, brute force, or phishing (Varonis).

Breach Projections

Cybercrime is estimated to cost the world $10.5 trillion annually by 2025.
Cybersecurity Ventures

In the rapidly evolving field of data security, it’s vital that business owners stay informed of all potential issues. Below are the projected cybersecurity incidents that may occur in the coming years.

1. It is estimated that a business will fall victim to a ransomware attack every 11 seconds by 2021 (Herjavec Group).
2. Cybercrime is estimated to cost the world $10.5 trillion annually by 2025 (Cybersecurity Ventures).
3. Attackers will zero in on biometric hacking and expose vulnerabilities in touch ID sensors, facial recognition and passcodes (Experian).
4. Skimming isn’t new but the next frontier is an enterprise-wide attack on a national network of a major financial institution, which can cause millions in losses (Experian).

5. A major wireless carrier will be attacked with a simultaneous effect on both iPhones and Android, stealing personal information from millions of consumers and possibly disabling all wireless communications in the United States (Experian).
6. A cloud vendor will suffer a breach, compromising the sensitive information of hundreds of Fortune 1000 companies (Experian).
7. The online gaming community will be an emerging hacker surface, with cybercriminals posing as gamers and gaining access to the computers and personal data of trusting players (Experian).

Data Breach Prevention

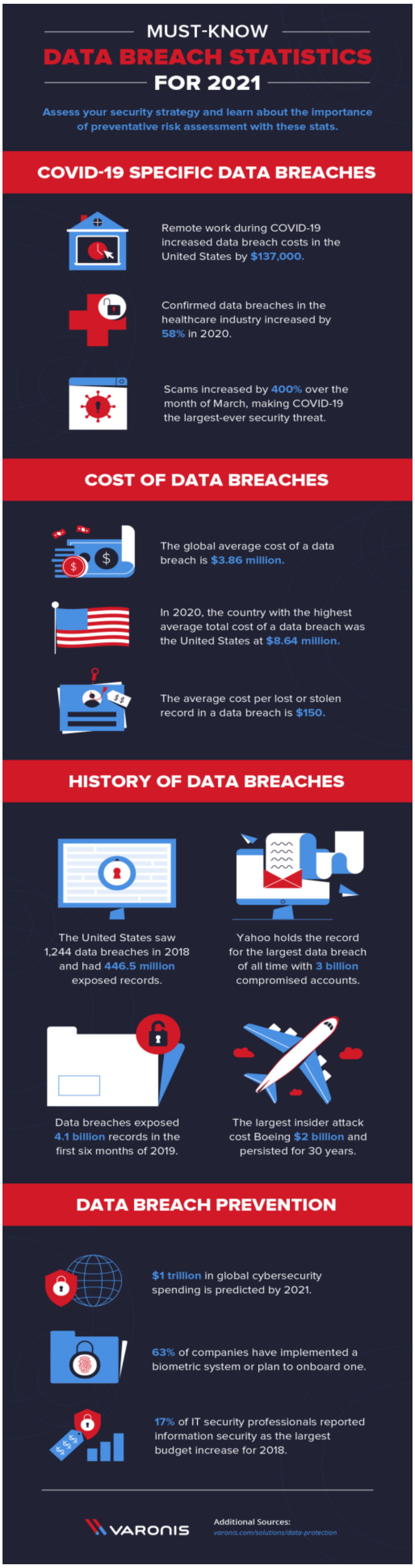
It is predicted that global cybersecurity spending will exceed $1 trillion cumulatively from 2017 to 2021.

Cybersecurity Ventures

There are also proactive approaches security professionals can take in order to lower their chances of experiencing a breach.

See how companies are shifting their budgets and priorities to protect their assets and customers from cyberattacks.

1. 63% of companies have implemented a biometric system or plan to onboard one (Veridium).
2. 17% of IT security professionals reported information security as the largest budget increase for 2018 (ZDNet).
3. 80% of organizations planned to increase security spending for 2018 (ZDNet).
4. It is predicted that global cybersecurity spending will exceed $1 trillion cumulatively from 2017 to 2021 (Cybersecurity Ventures).
5. Worldwide, IT security spending in 2019 was projected to grow 8.7% over 2018's figure (Gartner).
6. For the first time since 2013, ransomware declined, down 20% overall, but up 12% for enterprises (Symantec).
7. Budget allocation to hardware-based security services, which generally lack both portability and the ability to effectively function in virtual infrastructure, has fallen from 20% in 2015 to 17% with a further predicted decline to 15.5% in 2019 (451 Research).
8. MSSPs, which can replicate certain security operational functions, saw modest budget allocation growth at the end of 2017 to 14.7%, but security professionals expect that stake to grow to 17.3% by 2019 (451 Research).



MUST-KNOW

DATA BREACH STATISTICS FOR 2021

Assess your security strategy and learn about the importance of preventative risk assessment with these stats.

COVID-19 SPECIFIC DATA BREACHES

Remote work during COVID-19 increased data breach costs in the United States by **$137,000.**

Confirmed data breaches in the healthcare industry increased by **58%** in 2020.

Scams increased by **400%** over the month of March, making COVID-19 the largest-ever security threat.

COST OF DATA BREACHES

The global average cost of a data breach is **$3.86 million.**

In 2020, the country with the highest average total cost of a data breach was the United States at **$8.64 million.**

The average cost per lost or stolen record in a data breach is **$150.**

HISTORY OF DATA BREACHES

The United States saw 1,244 data breaches in 2018 and had **446.5 million** exposed records.

Yahoo holds the record for the largest data breach of all time with **3 billion** compromised accounts.

Data breaches exposed **4.1 billion** records in the first six months of 2019.

The largest insider attack cost Boeing **$2 billion** and persisted for 30 years.

DATA BREACH PREVENTION

$1 trillion in global cybersecurity spending is predicted by 2021.

63% of companies have implemented a biometric system or plan to onboard one.

17% of IT security professionals reported information security as the largest budget increase for 2018.

VARONIS

Additional Sources:
varonis.com/solutions/data-protection

Data Breach Defense + Prevention Resources

The following resources offer additional information on the improvement of data protection and tips for data breach prevention.

Data Breach Insurance

In order to mitigate the risk that comes along with data loss, many companies are now purchasing data breach insurance to support their data breach prevention and mitigation plans.

Data breach insurance helps cover the costs associated with a data security breach. It can be used to support and protect a wide range of components, such as public relations crises, protection solutions and liability.

Common types of data breach insurance are:

First-Party Insurance

With many different kinds of consequences that occur due to a data breach, significant time and money will be spent to recover. From recovering data and notifying stakeholders, first-party insurance covers the following:

- Investigating costs
- Notifying all affected parties
- Fielding inquiries
- Tools to help affected parties

Third-Party Insurance

Third-party insurance is primarily used by contractors and IT professionals to lessen their liability. The covered expenses may include things such as the following:

- Lawyers' fees
- Settlements
- Judgments and liability
- Other court costs such as witness fees, docket fees, etc.