WHITEPAPER

2019 Top Data Breaches and What We Can Learn from Them

February 2020

703.786.8884
sales@appguard.us
www.appguard.us

2019 Top Data Breaches and What We Can Learn from Them

Record-breaking Number of Breaches

2019 broke the record for the most data breaches of any year yet.

According to the Identity Theft Resource Center, the number of data breaches tracked in 2019 (1,473) increased 17% from the total number of breaches reported in 2018 (1,257). Other surveys have reported much higher numbers, showing an increase in both the number of records exposed and breaches.

In this report, we look at 10 of the biggest and most damaging attacks of 2019 and best practices enterprises of any size should incorporate to ensure they are protecting their organization and customers.

Attack Countdown

10	FEMA	*2.3 million disaster survivors' data*	**Leaked**
9	Dominion National	*2.96 million records*	**Hacked**
8	Desjardins Group	*4.2 million customers' records*	**Insider Threat**
7	DoorDash	*4.9 million individuals' records*	**Unauthorized Third-party Access**
6	Hy-Vee	*5.3 million cardholder records*	**Hacked**
5	CafePress	*23 million consumers' data*	**Hacked**
4	American Medical Collection Agency	*25 million customers' data*	**Hacked**
3	Evite	*101 million consumers*	**Hacked/Misconfiguration**
2	Capital One Financial Corporation	*106 million customers' data*	**Hacked/AWS Misconfiguration**
1	First American Financial	*885 million customers' data*	**Website Misconfiguration**

703.786.8884
sales@appguard.us
www.appguard.us

U.S. Federal Emergency Management Agency

Industry: Government

Improper disclosure/leak/human error

Impact: 2.3 million disaster survivors

- FEMA, part of the U.S. Department of Homeland Security, improperly provided personally identifiable information, such as banking details on 2.3 million disaster survivors, to a contractor administering a disaster relief program
- The Department of Homeland Security inspector general said the agency violated federal policy laws by disclosing more information than the contractor needed

Dominion National

Industry: Healthcare

Server Hacked

Impact: 2.96 million patients

- Second-largest healthcare breach of 2019 patient information
- Data from several healthcare providers was exposed after a cyberattack on Dominion National, a health plan and benefits administrator and insurer
- Dominion National discovered in 2019 that a hacker had accessed company servers for nine years
- Potentially exposed records included names, social security numbers, health benefits, and provider information

Desjardins Group

Industry: Financial

Insider threat/admin access

Impact: 4.2 million customers

- Canadian credit union Desjardins Group suffered a data breach due to an employee who gathered customer data and leaked it to an outside party
- The breach exposed names, addresses, birth dates, social insurance numbers, and transaction habits—affecting Desjardins' entire customer base of 4.2 million members

DoorDash

Industry: Hospitality Services

Third-party unauthorized access

Impact: 4.9 million individuals

- Nearly five million users, merchants, and contractors were affected by a data breach of DoorDash, a restaurant delivery service
- Compromised data included names, emails, physical addresses, phone numbers, and partial bank or credit card account information, as well as driver's license data of DoorDash drivers
- The company reported that unauthorized access by an unnamed third-party service caused the breach

Hy-Vee, Inc.

Industry: Retail

POS Malware

Impact: 5:3 million cardholders

- A data breach of supermarket retailer Hy-Vee, Inc. due to malware infection compromised the data of as many as 5.3 million cardholders
- The company's payment systems were affected at fuel pumps, restaurants, and drive-through coffee shops at multiple locations

CafePress

Industry: Retail

Hacked

Impact: 23 million consumers

- CafePress, a popular online retailer, exposed personal data such as names, mailing addresses, phone numbers, and email addresses of 23 million customers
- The e-commerce company reportedly was hacked because of software vulnerabilities, including the use of a cryptographic algorithm, Secure Hash Algorithm 1 (SHA-1), to store passwords in a database
- The company is facing a class-action lawsuit

American Medical Collection Agency

Industry: Healthcare

Hacked

Impact: 25 million consumer data

- Over 25 million consumers' records from 21 healthcare companies were compromised due to a breach of the American Medical Collection Agency (AMCA) a third-party collection service
- The data included birth dates, addresses, social security numbers, and banking details and was the result of "unauthorized access" over a period of eight months
- The company has filed for bankruptcy

Evite

Industry: Online Service

Hacked/Misconfiguration

Impact: 101 million customers

- Popular online social-planning service Evite exposed the data of an estimated 100.98 million consumers due to unauthorized access to an inactive data storage file
- The data included names, emails, mailing addresses, birth dates, and user names of invitation recipients, as well as Evite users before 2014
- An undisclosed party provided the data dump to Have I Been Pwned, a data-breach monitoring website

Capital One Financial Corp.

Industry: Financial

Hacked AWS Misconfiguration

Impact: 106 million customers

- A former Amazon employee downloaded nearly 30GB of data from Capital One credit applications made between 2005 and early 2019
- The hacker, who was subsequently arrested, stole the data of more than 100 million U.S. and Canadian customers, including some of those customers' social security numbers and bank account numbers
- The breach was reportedly due to a misconfiguration of an open-source web application firewall used for AWS

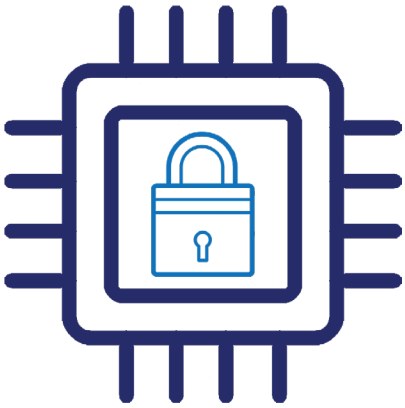
First American Financial

Industry: Financial

Website misconfiguration

Impact: 885 million customers

- First American Financial, a provider of title, mortgage, and real estate settlement services, leaked millions of mortgage-related records dating back as far as 2003
- Bank statements, tax documents, mortgage records, and copies of driver's licenses were left exposed online due to a website misconfiguration error
- A security researcher discovered the data, which could be accessed without a login by anyone with a link



What Enterprises Can Do to Stop Future Attacks

Use Prevention vs. Detect & Respond Solutions

What good is a cybersecurity solution that detects attacks **after** they have happened? Or worse, misses the threat completely, like the Dominion National or AMCA attacks.

Utilizing prevention methods that can stop zero-day and other known and unknown advanced attacks is crucial for a robust security framework. A preventative approach will also take the pressure off IT/Sec-Ops and minimize attacks due to human error.

Arm Employees with Training and the Right Set of Tools

As you noticed from the list of attacks, most attacks occur through online social engineering schemes that manipulate users to open the doors for hackers. One of the most common examples of this is a *fileless attack*.

The bottom line is employees can be the first line of defense against such threats. They must learn how to spot phishing schemes, not download attachments without context, even when sent from an existing contact.

Don't Assume Your System is Secure; Perform Continuous Threat Monitoring

Develop an understanding of the current threat environment and take appropriate measures to protect yourself from attacks. Evaluate your existing security solution stack and practices and periodically employ third-party pen testers to do in-depth vulnerability testing. Gain visibility across your environment, so you know what software and systems have weaknesses. Once identified, prioritize the most critical vulnerabilities so you can mitigate those first.

An average organization has more than 200 apps: there are ample opportunities for bad actors to find weaknesses, and that is just the apps IT knows about—shadow IT increases the risk. Gartner estimates a third of successful attacks next year will involve shadow IT. No organization can address all vulnerabilities, even with the best IT teams and technology in place—therefore, a **preventive** solution is key.

Manage Third-Party Risks

Most companies rely on a variety of vendors, suppliers, and partners—and those relationships bring unwanted exposure to the business.

Even with a strong security posture, attackers can simply find the weakest link in the supply chain and use it to gain access. Segment your network and limit third party access to critical infrastructure. Establish security checks and thresholds for partners and vendors.

Cybersecurity Should Be a Culture, Not a Practice

A strong cybersecurity culture goes beyond employee training and awareness. Everyone in the company—from the board of directors and C-suite executive leadership to every line employee—should view themselves as a critical part of strong security defense.

Board and senior leadership should make cybersecurity a priority. Executive leaders should emphasize a cybersecurity culture of "no-fear" where an employee can raise appropriate alarms if they make a mistake, instead of sweeping it under the rug from the fear of getting fired.

Devise Comprehensive Incident Response Plans

Incident response (IR) should never be treated as an ad-hoc process. Assume that your security parameters are already compromised. Your security team should already have a well-defined methodology and IR playbook that is updated continuously based on new attack vectors that can be quickly implemented to quarantine, block, or eliminate malicious network traffic.

APPGUARD *A Blue Planet-works Company*

How AppGuard Can Help

About AppGuard

AppGuard is a PREVENTION solution, applying a zero-trust approach within the workstations and servers it protects, in real time. AppGuard takes away all applications' ability to harm the operating system.

Protecting Applications with Enforce, Block and Adapt

AppGuard's policy-based, zero-trust solution mitigates application misuse and hijacking risks by:

- *Enforcing policies, so applications do only what they are supposed to do*
- *Blocking actions that do not conform to policies*
- *Adapting in real time to application updates, patches, and other changes to avoid administrative burdens and mitigate unanticipated attack vectors.*

To learn more about AppGuard, visit *www.appguard.us*

VA Office

14170 Newbrook Drive Suite
LL-01
Chantilly, VA 20151
USA

LA Office

530 Wilshire Boulevard
Suite 206
Santa Monica, CA 90401
USA

NY Office

333 Seventh Avenue
10th Floor
New York, NY 10001
USA

Tokyo Office

(Blue Planet-works, Inc.)
Daiwa Jingumae Bldg.,
3Fl2-4-11 Jingumae
Shibuya-Ku Tokyo,
150 - 0002
Japan

703.786.8884
sales@appguard.us
www.appguard.us