The 10 most important cyberattacks of the decade

by Jonathan Greig in Decade in Review on December 4, 2019, techrepublic.com

After a number of devastating breaches and hacks, the sheer size of data lost is no longer the only indicator of severity. Since 2010, billions of sensitive files, personal information and account details have been leaked thanks to devastating hacks and damaging breaches.

As more sensitive personal data has made its way online, the size and impact of breaches has steadily increased throughout the decade. Attacks have hit almost every sector and show no signs of slowing down as more people are forced to entrust the safety of personal information to various websites.

"For me, the largest hacks of the decade are not just the ones that were the biggest, but the ones that were game-changers in how we approach security. If we had this talk 10 years ago, we would be blown away by the numbers, but now, the numbers don't really affect us that much," said Etay Maor, chief security officer at the cybersecurity firm IntSights.

"All of a sudden, we're in the age of career-ending or career-altering hack. Honestly in 2011, if you had a hack with over a million credentials, everyone would lose their mind," Maor said. "Today, you probably won't even read about hacks that happen with a couple million credentials stolen."

Yahoo - 2013

Yahoo deserves the first mention because of the sheer size of its breach and the damaging effect it had on the company's ability to compete as an email and search engine platform.

In 2013, all three billion of Yahoo's accounts were compromised, making the breach the largest in the history of the internet. It took the company three years to notify the public that everyone's names, email addresses, passwords, birth dates, phone numbers and security answers had been sold on the Dark Web by hackers.

Security experts say the Yahoo breach is notable because of how it was mishandled by the company and the devastating effect it had on Verizon's $4.8 billion acquisition. Yahoo initially discovered that a breach occurred in 2015 exposing 500 million accounts.

It was later confirmed by American security agencies that the attack was perpetrated by a group affiliated with the Russian government. While looking into the 2015 attack, Yahoo officials realized more than one billion accounts had been exposed in the breach.

The company then admitted in 2017 that all of its accounts had been breached. Verizon removed nearly $400 million from the buying price and signed an intricate deal that allowed both companies to share the financial liabilities associated with the breach.

Equifax - 2017

The size of the Equifax breach pales in comparison to the value of the data exposed to hackers. As one of America's largest credit bureaus, the company had the most sensitive data on hundreds of millions of people.

Hackers gained access to the information of 143 million Equifax customers, including their names, birth dates, drivers' license numbers, Social Security numbers and addresses. More than 200,000 credit card numbers were released and 182,000 documents with personally identifying information was accessed by cybercriminals.

Equifax's CEO, Richard Smith, was forced to testify at four hearings before Congress, where he asserted that one employee was responsible for failing to process a necessary update.

"Equifax would probably rank as the most careless given that it as due to an unpatched Struts vulnerability, which might have been prevented using even the most rudimentary protection measure," said Ameesh Divatia, co-founder and CEO of the cybersecurity firm Baffle.

It was later revealed that hackers were able to gain access to passport information from affected Equifax users. The Government Accountability Office released a detailed report about the breach.

Sony Pictures - 2014

The hack of Sony Pictures in 2014 made the news for a bunch of reasons that made it different from most breaches. The situation originated with the controversial Seth Rogen film "The Interview," which revolves around a plot to assassinate North Korean leader Kim Jong-un. The North Korean leader was incensed by the film and his government threatened to attack US theaters if the film was released.

Sony tried a number of things to quell the controversy, agreeing to recut the movie to make it less offensive and push back the release date. Because of the threats against theaters, executives eventually decided to pull the film from theaters and release it digitally.

This did little to calm North Korean anger about the film and in November 2014, a group that the FBI later said was tied to the North Korean military apparatus attacked Sony Pictures' servers, wreaking havoc on the company's internal systems. Some Sony executives, and even Rogen himself, still question whether it was truly North Korea that was behind the attack, hinting at either a disgruntled insider or the Russian government.

While Sony feared the leak of its films, what ended up hurting the company most were the millions emails of film executives discussing their true feelings about some of the world's biggest movie stars.

The attack also launched North Korea into international prominence, kickstarting a new generation of small countries punching above their weight through devastating, yet low-cost, cyberattacks.

Charity Wright, cyber threat intelligence adviser at IntSights, worked for the NSA in the Asia-Pacific theater and said previously, North Korea had mostly focused efforts on attacking South Korea and Japan.

"The Sony hack was incredible because it really showed the world that North Korea can hack legitimately. They are legit. They really put themselves on the map as a legitimate threat actor with that hack," Wright said.
Gossip sites spent months digging through the nearly 200,000 emails of Sony executives, highlighting negative comments about stars like Tom Cruise, Angelina Jolie, Leonardo DiCaprio and Kevin Hart.

Marriott Hotels - 2018

The Marriott Hotel breach was massive both because of the amount of data exposed and the sensitivity of the information accessed.
According to The Washington Post, hackers breached the reservation systems of Starwood Hotels, which was bought by Marriott in 2016 for $13.6 billion. The cybercriminals behind the attack had an astounding four years to move within the Starwood system, which includes the Sheraton, Westin, W Hotels, St. Regis, Four Points, Aloft, Le Méridien, Tribute, Design Hotels, Element, and the Luxury Collection.
Hackers gained access to the names, credit cards, addresses and passport numbers of millions of people who stayed at the hotels between 2014 and 2018.
At first, Marriott said the number of people affected was 500 million but revised that number down to 383 million after an investigation.
"Marriott was significant in that it attacked databases and the content was protected at rest, which demonstrated that traditional database protection methods do not adequately protect sensitive data records," Baffle's Divatia said.

Ashley Madison - 2015

While the information leaked in the hack of discreet extramarital dating website Ashley Madison was not financially significant, its cultural footprint was very wide. More than 30 million email addresses and hundreds of credit cards were leaked in the attack.
The hack also set off months of marital disputes that came from spouses searching for their partner's email address in the leaked database of Ashley Madison.
Debate raged online about the ethics of news outlets reporting on famous people and politicians found in the company's files. There were reports of hackers extorting people based on the information found on the site, demanding people pay a ransom in exchange for hiding evidence of affairs.
In 2017, the company settled a lawsuit filed by users for more than $11 million, but that did little to quell the social furor over the information and messages found on the website. The aftermath was said to have life-altering implications for some.
Police in Toronto attributed two suicides to information that came from the leak and a pastor in New Orleans wrote a suicide note detailing the fear and embarrassment he felt about being implicated in Ashley Madison leaks. The hack was one of the first to lead to real-world deaths.

Target - 2013

The attack on Target is one of the biggest to hit a major retailer and involved a point-of-sale system that was compromised by malware.

The breach highlighted a problem that would come to dominate the cybersecurity conversation for the rest of the decade: third-party partners. Hackers gained access to Target's systems through a heating and air-conditioning contractor working for the company.
With their access, the cybercriminals got payment card details for more than 40 million Target customers. The company was forced to admit that the number was even larger, with the actual amount of impacted customers reaching 110 million.
The attack had a devastating effect on Target, forcing the CIO to resign months after the attack and the company reported that it lost more than $160 million due to the breach.
Both Divatia and Maor said the hack was notable because it became the first of many major breaches involving third-party systems or companies.

Capital One - 2019

In July, Capital One bank acknowledged that from 2005 and 2019, hackers were able to access the personal information of 100 million Americans and six million Canadians.
According to the bank, cybercriminals obtained the information from a trove of credit card applications, including names, addresses, phone numbers, email addresses, dates of birth, and self-reported income.
Capital One also said credit scores, limits, balances, payment history and about one million Canadian Social Insurance numbers, as well as 140,000 American Social Security numbers were also seen by hackers.
Unlike most of the hacks on this list, the culprit behind it was caught and charged in court. Paige Thompson, a former Amazon Web Services employee, posted on GitHub about the attack and was charged in August for the massive breach. Thompson was arraigned in September and pleaded not guilty to all charges.

The United States Office of Personnel Management - 2015

The hack conducted by the Chinese government on the United States Office of Personnel Management is one of the largest attacks to ever hit the government in the country's history.

While officials initially estimated that the records of four million current and former government workers were released, a later analysis found that 21 million records were accessed. The trove of data even included information from background checks on people who were never hired by the government.

The forms accessed by hackers had detailed information about candidates' family members, college roommates, foreign contacts and psychological information. They also stole millions of Social Security numbers, names, dates, places of birth and addresses.

The group also stole a database with nearly six million fingerprints, endangering government officials across the world.

Donna Seymour, CIO for the Office of Personnel Management, was forced to retire because of the scandal and Katherine Archuleta, the director of OPM, resigned. It was later revealed that Chinese government hackers had access to OPM systems for more than a year before they were caught.

First American Financial - 2019

Billion-dollar real estate title insurance company First American Financial had one of the biggest leaks of 2019, exposing 885 million files dating back more than 15 years.

The breach was exposed by the security reporter Brian Krebs, who wrote a lengthy blog post explaining how the massive insurance company exposed millions of mortgage deals, which featured bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts and drivers license images.

He was tipped off by a real estate developer who discovered that you could access any of the company's documents just by changing the URL link. Although it is unclear whether any of the information was accessed and used, First American immediately took down the entire website.

Stuxnet - 2010

The Stuxnet attack, allegedly perpetrated by the governments of the United States and Israel, was relatively minor in its effects but has had wide-ranging implications that will become evermore important in the next decade.

It was one of the first examples of government-led cyberattacks that could destroy physical systems and structures, setting off a growing cascade of attacks that are increasingly blurring the line between military cyberattacks and cyberattacks affecting infrastructure systems.

The Stuxnet worm destroyed Iran's 984 uranium enrichment centrifuges, essentially ruining most of its nuclear program by specifically targeting Siemens SCADA systems.

Outside of a few headlines, the attack had little impact on the US. But it kicked off a decade of attacks by dozens of countries that aimed to destroy architecture systems.

The Russian government later used similar tactics during their alarming 2015 attack on Ukraine. For the first time in history, a government was able to shut down another country's power grid through a cyberattack. Stuxnet and the attack on Ukraine opened the door to increased efforts by adversarial countries to include cyberattacks in their arsenal of military weaponry.