Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Most Significant Data Breaches Of 2016

By **Steven Trader**

Law360, New York (December 22, 2016, 5:38 PM EST) -- By themselves, the hack of a thousand payment card systems at a fast-food chain or the theft of three million patient files would have been significant, but when a single company loses more than a billion users' account information, you know 2016 was a big year for data breaches.

While the size and scope of the perhaps more "traditional" system hacks reached new heights, privacy attorneys say that in the past year they have also noticed an uptick in phishing schemes and ransomware, as well as the emergence of more diabolical attacks whose sole purpose seemed to be to wield power and cause disruption, a scary notion in itself.

"This was the year the earth moved with respect to the sheer number and size of data breaches, and a realization by companies of all sizes and sectors that the era of data breaches is here to stay," said Mary Hildebrand, chair of Lowenstein Sandler LLP's privacy and data security practice.

Without further ado, here's a Law360 recount of some of the most significant data breaches that occurred in 2016.

Account Information

At one point, the largest disclosed attack this year constituted 2.2 million lost medical records, which we'll get to later. But then LinkedIn let everyone know in May that the email addresses and passwords stolen from **roughly 100 million people** four years ago had been posted online.

Yahoo Inc. then blew that number out of the water when it **disclosed in late September** that hackers had infiltrated its systems in late 2014 and lifted names, phone numbers, dates of birth, passwords and other data tied to at least 500 million users.

The breach was deemed the largest in history — until Yahoo **revealed** in December that hackers had stolen a billion users' data during a separate 2013 incident. In between Yahoo's two colossal missteps, online dating service AdultFriendFinder **announced in November** it may have lost more than 412 million website accounts to cybercriminals.

While one might be tempted to think a stolen email address doesn't mean much, Sharon Klein, chair of Pepper Hamilton LLP's privacy practice, says that after a while these seemingly insignificant data points can start to add up.

"The dark web loves this stuff because then they have another data point to be able to compare against, to be able to hack into bank accounts or financial records, so it could have some trickle-down damage to consumers," Klein said.

Personal Data Through Phishing

For proof that hackers are starting to connect the data dots, look no further than the rash of attacks carried out in 2016 through seemingly innocent emails that dupe employees into clicking a malware link or sharing confidential information.

On March 7, an Advanced Auto Parts employee was **tricked into sharing** potentially 75,000 of their co-workers' W2 tax return information. A week later, Sprouts Farmers Market Inc. **announced** it had wrongly shared similar data on 21,000 of its employees.

At one point early in the year, Experian said it was handling **more than 70 data breaches each week** tied to phishing schemes.

"This is an area where everyone is falling down," said Cynthia Larose, chair of Mintz Levin Cohn Ferris Glovsky & Popeo PC's privacy practice. "Cybersecurity is not all about IT, it's about people. You can spend all the money you want on perimeter security, endpoint security, firewalls, but if you don't train your people not to click on things, you're still going to be a victim."

Health Care Data

National cancer treatment center 21st Century Oncology **disclosed in March** that 2.2 million patients' medical records had been compromised. Nonprofit hospital system Banner Health then **topped that number** in August by losing both the records and payment card information for 3.7 million customers to a cyberattack.

These numbers aren't staggering when compared to the likes of Yahoo and LinkedIn, but privacy experts say these types of files are a gold mine for hackers because they contain all the most sensitive consumer data, and the risk of attack isn't going away anytime soon, either.

"Health care is such a complex infrastructure, it's becoming even more difficult to secure all the endpoints," Larose said. "While doctors are scientific, they're not always the greatest users of technology in the world, and there's a lot of physicians in small practices that connect out to bigger organizations. So you've got endpoints that, shall we say, are less than ideal from a security perspective."

Payment Card Data

Just a few years removed from the notorious theft of 100 million payment card numbers from Target and Home Depot, point-of-sale breaches were relatively low-key this year in comparison to some of the larger hacks, privacy experts say.

Wendy's **announced in January** it was investigating suspicious activity, then reported in May that the malware used by attackers had affected only one particular point-of-sale system used at fewer than 300 of its 5,000-plus locations, before finally revealing in July that **more than 1,000** of its stores had been hit.

Fast-casual restaurant Noodles & Co. in May **disclosed** a breach affecting 300 locations. Hard Rock Hotel and Casino Las Vegas in June **announced** their second payment card security lapse in a little more than a year. And the Madison Square Garden Co. told customers in November that, over the past year, card numbers **had been lifted** through malware from five of its major venues, including Madison Square Garden and Radio City Music Hall.

Chaos Theory

These are the types of hacks that can't really be quantified and are hard to categorize because they seem less about money or personal data, and more about wielding power and influence.

At the height of the election season, the FBI **revealed** a massive data breach at the Democratic National Committee, which led to the exposure and online publication of nearly 20,000 emails, some of which appeared to bash primary contender Vermont Sen. Bernie Sanders. The hack also revealed personal donor information, including their Social Security numbers and credit card information.

DNC Chairwoman Debbie Wasserman Schultz resigned her position following the hack, which also carried untold election consequences. Lowenstein Sandler's Hildebrand likened it to a "really bad form of reality television."

"Hackers had the capability of influencing the campaigns on a daily basis, and that's very troubling," Hildebrand said. "Once they had that data, they had the ability of what and when to disclose, so the disruption didn't just start and end with that hack, it continued and it still has the potential to impact events."

The other significant attack of this nature occurred over Thanksgiving, when San Francisco's Municipal Transportation Agency was **hit by ransomware** that hobbled internal computer systems and shut down its station ticket machines in exchange for $70,000 worth of bitcoin.

While extortion through cyber attacks isn't anything new, this one felt like a weapon of fear, Klein says, which is hard to protect against.

"Hacking into infrastructure scares me more than anything else because it has such an immediate impact," Klein said. "That's really not about money, that's about causing havoc. That's not good."

--Additional reporting by Allison Grande, Shayna Posses, Kat Green and Y. Peter Kang. Editing by Rebecca Flanagan and Kelly Duncan.
