TECH HACKING OF AMERICA JAN 30 2017, 7:31 AM ET

More Than 4 Billion Data Records Were Stolen Globally in 2016

by HERB WEISBAUM

Cybercriminals are stealing data at an alarming rate. Both the number of breaches and the number of files stolen globally in these hacks rose dramatically to set a new record in 2016, according to a new report from Risk Based Security. The 4,149 confirmed breaches exposed more than 4.2 billion records. That's approximately 3.2 billion more records than were exposed in 2013, the previous all-time high.

Businesses were the prime targets, with more than half (55 percent) of the reported breaches. But hackers also attacked medical institutions and government agencies.

"The number of records compromised just went completely off the charts," said Inga Goddijn, executive vice president of Risk Based Security. "And as staggering as they are, our numbers probably underestimate the actual criminal activity that's taking place."

Yahoo's Mega Breaches

The big breaches at Yahoo reported last year — 500,000 records involved in one and more than a billion in the other — did drive up the numbers. But the Risk Based Security report shows that hundreds of other organizations had sizable breaches that impacted anywhere from 500,000 to more than 10 million records.

"So unfortunately, while the number of incidents doesn't really seem to be on the rise, the success of stealing or compromising large amounts of information is going up," Goddijn told NBC News.

The U.S. (1,971 incidents) and the United Kingdom (204) accounted for slightly more than half of all the reported breaches last year. Also in the top 10: Canada (119), Brazil (75), India (71), Australia (59), and Russia (49).

Breaches vary in their severity. Stealing user names and passwords or even credit card numbers is bad, but not as harmful as stealing Social Security numbers, date of birth and mother's maiden name, or sensitive medical records.

The Risk Based Security report rated breaches for severity, based on the number of records stolen, the type of information compromised and the potential fallout from the intrusion. The ten biggest breaches last year rated an average severity score of 9.96 out of 10.

"Clearly, we are not winning the war when it comes to cyber security," Goddijn said. "The criminals are enjoying a high degree of success right now."

The Hackers Are Getting Better

The non-profit Online Trust Alliance (OTA) just published its 2017 Cyber Incident & Breach Response Guide, which warns that the "cyber landscape has changed dramatically over the past 12 months," with organizations large and small being the victims of attacks that "stole, published or manipulated sensitive, personal information." These incidents include the hack attack on the Democratic National Committee and the theft of confidential medical records of world-class athletes from the Olympic Anti-Doping Agency's database.

Craig Spiezle, OTA's executive director, told NBC News that no organization or government entity is immune from today's skilled adversaries who have created highly sophisticated methods of attack.

"In the past, a lot of the breaches were opportunistic," Spiezle said. "Now we're seeing much more precision. They're targeting specific companies and industry sectors and not just for consumer data, but for business data, data regarding acquisition and mergers, data that may also harm a company's reputation."

The Problem with Social Security Numbers

Hackers were very successful last year at getting social security numbers — the master key that unlocks our lives. It's estimated that more than 19 million were compromised last year, according to a recent analysis of U.S. breaches by the Identity Theft Resource Center and CyberScout. The report noted that the number of breaches involving stolen SSNs is on the rise. More than half (52 percent) of the reported breaches included SSNs last year, up from 44 percent in 2015.

"While credit and debit card numbers can be changed, Social Security numbers cannot," noted Adam Levin, chairman and founder of CyberScout. "Hackers and identity thieves continue to evolve. They are very sophisticated, extremely creative and dogged in their pursuit of what is ours."

The ITRC/CyberScout report found that many of the corporate breaches that involve the theft of Social Security numbers result from what's called "spear-phishing."

These attacks start with a bogus email to a corporate executive that appears to be from a trusted employee asking to be sent all the W-2 records or some other confidential business files. If successful, the criminals will get highly sensitive data, typically information required for state and federal tax filings, as well as employee records.

"We were surprised by the scale of how successful these spear-phishing efforts were and how many of these types of breaches were reported last year," said Eva Velasquez, president and CEO of the Identity Theft Resource Center.

The Art of 'Spear Fishing'

Here's how it's done. Crooks learn the names and titles of corporate employees from online profiles. Then they create a spoofed email address that looks very similar to the real one — maybe add a letter or drop one from the company name.

Now they're ready to pose as an executive in the company — maybe John, the HR director — and send an email to the CEO requesting corporate records that John has the authority to see. The boss gets so much email from John that he doesn't catch the misspelling in the URL and sends the requested files.

"Spear-phishing is such an easy thing for companies to fix because all it requires is a process in place to handle these types of requests for sensitive data," Velasquez told NBC News. "Companies need to make sure they're not only protecting customer data, but also employee data. They need to have mechanisms in place to ensure that requests for sensitive employee information are legitimate."

Just last week, a hacker used a spear-phishing attack to impersonate the CEO of Sunrun, a solar company in San Francisco. The successful scam netted the crook W-2 forms for some company employees, according to a report in the San Francisco Chronicle.

Email Addresses and Passwords

Breach notifications often downplay the significance of the data stolen, noting that the hackers "only" gained access to email addresses and passwords.

But in many cases, that's all they need to steal personally identifiable information that enables them to commit other crimes. That's because so many people now keep financial and medical documents in their email accounts or store them via a cloud-based service.

"This is much more than a change-your-password problem," said Haywood Talcove, CEO of LexisNexis Special Services.

A survey of 1,000 adults done by LexisNexis Risk Solutions found that more than 35 percent store highly sensitive documents — from mortgage statements to student loan information — on their email services or with cloud-based document storage services. The survey showed that 42 percent of the respondents stored

tax records, 40 percent stored bank records, and 35 percent stored health records this way. A sizable number (21 percent) even saved a list of PINS and passwords digitally — a very risky thing to do.

“It’s frightening,” Talcove told NBC News. “If the criminals have access to your user name and password, they have whatever is in there, not just the email between you and your spouse, not just the email between you and a work colleague, but important information that is absolutely critical to defrauding government and commercial entities.”

What You Can Do

Most companies, organizations and government agencies collect personal information that is valuable to a hacker and that makes them a target. Security experts tell NBC News there must be a concerted effort to appreciate the growing threat and a commitment to fighting it.

“While there is no perfect security, there’s really no excuse for not having a well-thought out plan to help protect that information and mitigate the impact of an incident if it happens,” Craig Spiezle of the Online Trust Alliance told NBC News.

Spiezle believes business incentives are needed to accelerate “security by design” — a policy where security is built into systems from the ground up and not dealt with later. And he advises companies both large and small to adopt a corporate culture of security, where employees are made aware of the threats and trained on how to deal with them.

Inga Goddijn with Risk Based Solutions hopes corporate leaders will empower their IT teams to deal with the ever-changing threats and give them the financial support they need to be successful.

“We simply have to recognize that we’re not going to solve this problem with one handy new tool or one shiny new appliance,” Goddijn said. “I am a little bit pessimistic to be honest with you. I think we might see the situation get a little

worse before we see it get better.”

Herb Weisbaum is The ConsumerMan. Follow him on Facebook and Twitter or visit The ConsumerMan website.
