The New IP

Data Breaches: The New Normal?

Ariella Brown, technology writer, 10/21/2015

Email This Print Comment 6 comments

Login

50% 50%

Hacking is so common today that even major data breaches may be filed under the "hack du jour," but what's the answer -- laws and stronger penalties, threat-intelligence sharing or sharing responsibility across the business all the way to the top?

Reality bites

October 1, 2015, was not a good day for T-Mobile's CEO John Legere. That's when the Experian data breach made the news -- hackers stole 15 million T-Mobile US Inc. customers' social security numbers, names and addresses.

As consolation, Experian is offering two years of free credit monitoring for those affected, which has become standard practice since similar breaches, such as Target Corp. and Home Depot. But perhaps it's time to question such attempts to pacify people after the fact.

Seattle-based cyber security consultant Bryan Seely said in the Seattle Times that offering credit monitoring is no better than putting a person across the street from you in charge of letting you know when your house is on fire. The real goal should be to "have someone stop my house from being on fire."

There's the rub, particularly with the type of information that serves identity thieves. While the credit card accounts can always be closed, you can't just replace your address and social security number.

For that reason, people may be justifiably upset about this breach. Certainly, T-Mobile's CEO John Legere claims to be. In a letter notifying customers of the breach, he declared that he was "incredibly angry." But all he promised was "a thorough review of our relationship with Experian."

That won't really solve the fundamental problem because it's not just a matter of vulnerability within a particular system but a problem with the system.

Paying the price

The T-Mobile/Experian breach "is the hack du jour," declares, Al Berman, president of DRI International (Disaster Recovery Institute), a certification and education nonprofit organization. In a phone interview with The New IP, he said, "We just take it for granted that there will be hacks."

That's the real problem: the acceptance that prevents pressure to take truly effective proactive steps like passing necessary legislation to raise the stakes for companies that fail to secure customer data, or making internal changes to prevent attacks from happening.

As for the cost to companies that have to pay penalties or compensation to customers affected, that, too, is not enough to motivate them to take the necessary steps to secure the data as much as possible. For example, Berman said that Target was hit with a $10 million first penalty for the hacked credit card information at its stores in 2014. That's just 25 cents for each credit card, he says, hardly a major hit for such a large retailer.

In fact, Target probably had those millions covered by insurance, as businesses work the possibility of hacking losses in their pricing model. The real proof of the businesses emerging from such breaches virtually unscathed is their stock prices, Berman says. Target, like Home Depot and Sony Corp. (NYSE: SNE), which all got major media attention for being hacked, all ended the year with their stock prices in positive territory. Based on that, Berman doesn't predict any serious losses for T-Mobile in the wake of this event.

Where to start?

In order to tackle the cyber security challenges all companies face today, cyber security must be a shared responsibility -- from the CISO to the CEO to the board, Jason Porter, vice president, security solutions, AT&T told The New IP on a recent radio show. However, that is not happening in just over 50% of enterprises today, according to AT&T Inc. (NYSE: T), which recently reported that 51% of CEOs and boards do not review or change their security protocols after a breach. Currently, the service provider is working to get the C-suite to be proactive about cyber security. (Listen to Cyber Security: What CEOs Need to Know Now.)

Instead, current conditions favor the hackers. Their tools are readily available on the open market for as little as $100, and the hackers work through a "joint venture" that separates the hacker from the criminal who applies the fraudulent charges. Consequently, some who are apprehended are let go due to lack of evidence linking them to the crime.

Among Berman's suggestions to quelling cyber-attacks is raising the status for hacking to a felony. But he also believes that it's necessary to come up with a comprehensive, integrated plan, though he doesn't see it happening. As an example, he points out that the National Cybersecurity Protection Advancement Act of 2015 has been languishing in the Senate since April. This law calls for both the private sector and government to share information about the threats they encounter from hackers so that they can all benefit from improved protection.

In the absence of such legislation, the only advances in protection come from within the credit card industry. So his best advice is "pure vigilance."

For now, it seems we're still stuck at that point that Seely complained of: the best we can do is put out the flames before they spread, but we can't prevent our homes from catching fire. If the T-Mobile hack is to have a positive effect, it would not just raise awareness of points of vulnerability but get businesses, large and small, to resolve to combat it more effectively.

— Ariella Brown, Freelance Contributor, special to The New IP