Wounds from cybertheft take long to heal

May 6 2014

Credit: George Hodan/Public Domain

For shadowy cybercriminals who find backdoor access to stores of personal data, the process of hijacking identities and pocketing stolen cash can be instantaneous. For institutions hit by cybertheft, however, discovering that a breach exists, finding the source and stopping the bleeding is usually a monthslong process of investigation that leaves the identities and bank accounts of those affected at the mercy of the thieves.

"Companies want to figure out exactly how a breach happened, but it's not so simple," said Charles Wood, Duquesne University assistant professor of information systems management. "Target found out there were problems after some of their customers had credit cards issued under their name in Eastern Europe. (Target) didn't know how it happened until they launched an investigation and eventually found the vulnerability."

Thousands of employees of the University of Pittsburgh Medical Center discovered the frustrating aftermath of cybercrime firsthand after a February data breach exposed their names, addresses, Social Security numbers and other W-2 information during the peak of tax season.

What UPMC officials said they initially believed was tax fraud involving a few dozen employees turned out to be an attack that affected approximately 27,000 employees, 788 of whom had false tax returns filed in their names. Last week, UPMC sent out paper and email notices to more than 12,000 employees telling them personal information from their W-2 forms was definitely extracted during the breach. The information of an additional 14,000 may have been viewed during the breach.

A lawsuit seeking class-action status on behalf of employees impacted by the breach was filed in February by Michael Kraemer of Pittsburgh law firm Kraemer, Manes & Associates LLC.

UPMC's response of notifying all 62,000 hospital employees of the breach and offering professional services and reimbursement to individuals impacted falls in line with industry standards established during massive breaches at retailers Target, Neiman Marcus and, most recently, craft store Michael's.

But with the scope of UPMC's breach involving critical Social Security

data rather than easily canceled credit card information, some employees are wondering if the company should have found a way to warn those who were directly impacted sooner.

According to Doug Pollack, chief strategy officer for Portland, Ore.-based data breach prevention and response company ID Experts, deciding between the earliest possible notification of those directly affected and blanket notification of all who potentially could be impacted is a tough call.

"It can become a judgment call between speed vs. accuracy," Pollack said. "It took some time to understand the total scope of the population affected, so that sacrificed immediate notification and might have caused employees to go through troubling issues they could have avoided if they had known sooner."

On the other hand, Pollack said, the opposite approach of informing victims immediately after discovering data were stolen could have caused panic among thousands of employees who still are waiting on a final verdict regarding the safety of their personal information.

"Most practitioners would prefer not to do creeping notification," he said. "Best practices tend to be to do enough analysis to understand what happened, then make a judgment call about who to notify. Out of an abundance of caution, most want to notify as broad an audience as they can so they can take steps to protect themselves, whether they are affected or not."

Saying that UPMC did a "decent job" of providing recourse for its employees once the breach was uncovered, Pollack nonetheless said UPMC's response could have been partially dictated by the threat of litigation.

"There are two drivers when you have a data breach. How do I take care of people affected in the most appropriate way? And the other driver is: How do I avoid increasing my liability? Unfortunately, they're in a position where they have got to be extremely aware of everything they do and how it impacts them as the lawsuit evolves," he said.

When UPMC first learned one of its employees was a victim of tax fraud Feb. 19, officials said, they presumed the matter was related to a fraud scheme common during tax time and not part of a larger internal data breach. By Feb. 24, 22 employees reported similar fraud and UPMC contacted federal authorities to initiate an investigation, according to UPMC spokeswoman Gloria Kreps.

When two days of investigations showed the organization had been hit by a widespread breach, UPMC began informing employees of the potential for theft and warning them to take actions.

By the first week in March, when the number of employees experiencing tax fraud shot up to 322, all employees were being offered free tax help to file identity fraud forms with the Internal Revenue Service, reimbursement up to $400 to hire accountants, reimbursement for copies of police reports and complimentary credit monitoring service through Tempe, Ariz.-based LifeLock.

On April 17, UPMC informed 12,624 employees that their names, addresses, W-2 information and Social Security numbers were taken by thieves.

With or without early notification, impacted employees must initiate a relationship with the IRS that begins with identity theft forms and continues for years with an identity theft PIN number used to confirm that future tax filings are made by the right person.

Beyond taxes, Pollack said, victims must be on constant guard of bank accounts and credit reports for the foreseeable future to ensure their personal information isn't funding someone else's mortgage or luxury vacation.

For corporations hoping to avoid similar attacks, Duquesne's Wood said old-school paper storage could be the best solution for personal data because it isn't a question of if a copycat cyberattack will occur; it's a question of when.

"Companies are going to get hacked. It's something they can try to fight against, but if you think about the number of hacking attempts, (larger companies) probably get thousands per day. If just 0.001 percent of those succeed, that's two or three successful attacks per year."