

## 'Low Impact' Breaches Can Signal More Badness To Come

By Ericka Chickowski

25 February 2011

*DarkReading.com*

*Just because a database breach doesn't expose PII doesn't necessarily mean the ultimate damage is inconsequential*

When is a database breach not a breach at all? If you're a stickler for the letter of the law, then perhaps it's when that breach doesn't expose regulated information, such as Social Security numbers or credit card numbers. But if your organization is a victim of a seemingly inconsequential hit that exposes items, such as e-mail addresses or passwords, that can be reset, it could mean more problems for you than you think.

"One of the problems that we see is that the term 'data breach' has become, in many people's minds, synonymous with the exposure of personally identifiable information (PII). Our case experience shows that certainly some data breaches involve PII, but a high percentage of cases involve financial fraud or sensitive corporate information, ranging from customer data, including e-mail addresses and passwords, to valuable intellectual property and trade secrets to financial results before they are announced," says Alan Brill, senior managing director of secure information services for Kroll. "While any form of a data breach can be devastating to an organization, the loss of sensitive corporation information can have significant reputational and financial implications."

Take the recent breach of an e-mail database held by St. George's University of London medical school that contained information for an online directory for doctors and nurses in the U.K., the Primary Care Electronic Library [PCEL]. Someone broke into the database and e-mailed everyone contained within a number of offensive e-mails.

Among the illicit communications sent by hackers were the following gems: "Dear PCEL user, if you were ever once a patient of ours, we regret to inform you that the Primary Care Electronic Library is closed due to AIDS. Thank you for your attention," and "Dear PCEL user, You're all ---. F—yourself." (Profanity redacted for this post.)

It's an awkward situation and, yet, no PII has seemed to have been molested in the making of these e-mail messages. But, clearly, some sort of damage was done.

These types of borderline breaches happen all of the time, to varying degrees of institutional embarrassment. Consider the rash of breaches in December that hit heavy-hitters such as Gawker and Silverpop, which, similar to this PCEL breach, did not affect PII. According to some experts, one of the big problems posed by breaches of less sensitive databases is that it's usually symptomatic of a corporate culture problem.

"If the companies aren't worried about protecting the e-mail and the passwords, that's kind of a red flag that they don't actually care a whole lot about protecting any of it," says John Sileo, a data breach expert and author of the book *Privacy Means Profit*. "Compliance-wise they may actually do more to protect socials or a credit card number or a bank account number, but what it signals is that the underlying culture is not there. They do the minimum necessary to comply and they don't actually care about this topic yet."

The difficulty, too, with a breach of e-mails or passwords is that this exposed information may actually put customer information at risk and will most definitely put the offending company's reputation at risk.

"Will visitors trust you going forward? The impact may be felt for months following the breach, as registration numbers fall off," warns Slavik Markovich, CTO of Sentrigo. "E-mail addresses are often used for usernames, and in many cases at less sensitive sites users may utilize less secure passwords. With a list of known registered users at a site, and some time for brute force attacks, it is likely that hackers could breach a high percentage of these accounts, gaining access to other PII that may have been provided on registration. With the addition of password data either from the breach itself or brute force techniques against the site, hackers could then try using this same combination at other popular sites, where the user may have used the same password."

As Sileo puts it, these breaches are not only a cultural red flag, but also a signal that the company is ripe for future, more serious breaches.

"When you see a company who loses e-mails and takes it lightly, I can almost guarantee in the next two year period you'll see them experience a larger breach," he says.

And from a technical perspective, these "isolated" database break-ins may not be as isolated as the targeted company thinks.

"Until the details of how the email database was breached [are known], organizations should be on high alert for additional threats. If someone has made it into one database server, they may be able to use the same or similar techniques to exploit weaknesses on more sensitive systems," Markovich explains. "In some cases, if the initial breach involved privilege escalation on one database, it may be possible to use those to access other databases using those improperly obtained privileges. This is exactly how the largest breach in history [Heartland Payment Systems] occurred -- hackers first penetrated a low security database, and then jumped from there through numerous other systems, ultimately reaching the payment card data."