Evan Schuman's
StorefrontBacktalk
Techniques, Tools and Tirades about Retail Technology and E-Commerce

Retail Lessons From South Carolina's Data Breach

Written by Walter Conway
December 3rd, 2012

A 403 Labs QSA, PCI Columnist Walt Conway has worked in payments and technology for more than 30 years, 10 of them with Visa.

I've been thinking about South Carolina, which is living through a major data breach involving millions of personal and corporate records, and a few hundred thousand payment-card numbers. The State is doing some things well. Governor Nikki Haley has been a visible public face of the State's response, and my guess is that she is finding out more about data security than she ever thought she needed—or wanted—to learn. The State also is making it clear there are consequences from the breach. Published reports indicate the head of the Department of Revenue will be resigning as a result.

The question for every retailer is: "What can my company learn from South Carolina's experience?"

Lesson #1: Don't skimp on training. PCI DSS Requirement 12.6 requires all merchants to "implement a formal security awareness program to make all personnel aware of the importance of cardholder data security." In South Carolina's case, published reports indicate the hackers broke into the State's systems by sending an E-mail with the malware attached. Once an employee clicked on the attachment, the malware was downloaded and started grabbing user IDs and passwords.

This attack vector should sound familiar. Training can't prevent every social-engineering or spam attack from being successful, but effective training (and enforcement) can go a long way in reducing the effectiveness of such attacks. Such malware-laden E-mails tend to increase after natural disasters and during the holidays. We can expect to receive a few "click on this great Santa video" E-mails, so it may be a good time to reinforce the training with all your employees.

Lesson #2: Strong user authentication is your friend. The PCI requirements may be pretty complicated, but unique IDs coupled with strong, regularly changed passwords for everyone with access to sensitive data (Requirement 8.5 and its 16 sub-sub-requirements) strengthen security.

The same lesson holds for requiring two-factor authentication for all remote access (Requirement 8.3). Two-factor authentication is not the same as multiple passwords. It means using two completely separate methods of identification, from among the following: Something you know (user ID and strong password); something you have (e.g., token or other physical device); or something you are (fingerprint or handprint). Pick any two you like. But it doesn't count to use just one of them twice!

Lesson #3: Protect your sensitive data. PCI DSS makes you encrypt or otherwise protect electronic cardholder data (Requirement 3). South Carolina has said the compromised records were, for the most part, not encrypted. I wrote about using PCI DSS to protect all an organization's sensitive data two years ago and again last year. The present events should tell us that this recommendation is as relevant now as it was then.

A lot of South Carolina's problems might have been eliminated had the data been protected with strong encryption accompanied by solid key management procedures. Not only that, one state employee—and possibly others, too—might still have a job. Some people criticize PCI DSS as being too detailed and prescriptive. Looking at it through another lens, that level of detail is also a strength. The standard tells you not just to protect the data but *how* to protect it. Following PCI Requirement 3 might possibly have avoided a lot of South Carolina's current headaches (and the estimated $12 million bill).

Actually, following all the relevant PCI DSS requirements provides the type of defense-in-depth that can help stop attackers. Keep in mind that the issue is not "if" your organization is going to be attacked but "when."

You may love or hate PCI DSS, but the idea behind it is to protect your cardholder data and to keep your organization out of the headlines for reasons you really don't want to be there. PCI DSS is not a total security program. There are, however, elements and specific requirements that should be part of any organization's security program. That is one of the lessons the State of South Carolina is learning. It should be a lesson that every retailer and merchant learns, as well.

What do you think? I'd like to hear your thoughts. Either leave a comment or E-mail me.