Payment Security Breaches: Who’s To Blame?

A Special Report

To avoid security vulnerabilities, data breaches, and costly fines, choose your vendor partners wisely.

by Bob Russo, general manager, PCI Security Standards Council

As a retailer, I’m sure you’ve heard about the number of data breaches throughout the years. They’ve hit the headlines and the wallets of companies and their owners, sometimes costing millions of dollars to repair the damage of stolen credit card data and compromised systems.

I know that I have looked at these incidents with concern and I think I know what is going through many of your minds when each of these stories hits the hometown newspaper:

- “Am I next?”
- “Would my business survive if I were breached?”
- “How can I stop this from happening to my business?”

So, with these thoughts in mind, many of you have gone to search for answers — solutions to the security problems that have challenged many organizations. You may have even come across the PCI Standards and begun to understand how they serve as a baseline to protect your business’ payment card transactions. Some of you may have then begun the journey to become PCI compliant and secure your network. Often this involves going to a systems integrator or service provider and getting the validated protections and solutions in place. For some of you, this may have included installing new systems, applications or devices, and may have taken a good deal of time to implement and get up and running.

This is absolutely the right thing to do. Anyone who accepts payment cards for purchases, whether online or in person, is contractually mandated by banks and the major credit cards to be PCI compliant. It is simply part of your obligation to play a role in the protection of this sensitive data.

Cardholder Data Security And Third-Party Vendors

However, there are some challenges in the approach I outlined earlier. In its 2012 Global Security Report, Trustwave reports that 76% of the breaches investigated in 2011 were a result of security vulnerabilities introduced by a third party responsible for system support, development, and/or maintenance.
of business environments. An error introduced into merchant environments during implementation, configuration, and support of validated payment applications by third parties was identified as a significant risk to the security of cardholder data.

Specifically, small businesses in the food and beverage industry that rely heavily on outsourcing are particularly vulnerable, as they made up the bulk of the compromises. What this means is, quite simply, the various pieces that were purchased and implemented in your environment may not have been put together correctly.

Let me give you an example. I am a grandfather, several times over. Over the course of the years, I've purchased a number of toys and furniture items for my grandkids. I know from experience (and a few hammer hits to my thumbs) how challenging these things can be to put together. Things are definitely more complicated these days than when I was raising my boys.

Anyway, imagine you have purchased a new stroller, unassembled. You've tried putting these things together in the past, but you know you are a little out of your league. You know you need to put it together, however, so you hire the person you purchased the stroller from to also assemble it for you.

Let's say this vendor has parts lying around from several different sets of strollers, manufactured by different companies. He grabs the parts he thinks he needs — left wheels from Company A, the frame from Company B, the hood and bassinette from Company C, and right wheels from Company D. And he begins to put these together.

After a while of hammering and banging from the back room, he rolls out a stroller, or rather, something that vaguely resembles a stroller. Except this one doesn’t roll straight, the hood won’t stay up and the bassinette is tilted sideways at a 45-degree angle.

He has all the right parts, but they aren’t assembled properly. Unfortunately, this is a bit of the same thing Trustwave noted in its report. Many integrators and resellers have gathered all the right parts, but they may not be working together in an effective, secure manner. This can cause problems with the overall security of your network and put you at risk of a data breach, even with the right pieces installed.

Don’t Blame The Integrators
To be honest with you, it isn’t necessarily the integrators’ fault. It is tough to be the master of all of these solutions and the hundreds of ways they can be implemented. And when you combine the multiple systems from different manufacturers (or even certain solutions from the same manufacturer), they don’t always work together in a manner that promotes thorough security. The simple fact is that some of these integrators haven’t had the training to understand how to put together disparate parts in a cohesive fashion — until now.

Recently, the PCI Security Standards Council announced plans to train and certify payment software integrators and resellers on the secure installation and maintenance of validated PA-DSS applications into merchant environments to support PCI DSS compliance. The PCI Qualified Integrators and Resellers (QIR) program will be rolled out over the coming months, with training set to begin in late summer and a global list of PCI Qualified Integrators and Resellers to be available later this year.

The QIR program will provide integrators and resellers that sell, install, and/or service payment applications on
Bob Russo brings more than 25 years of high-tech business management, operations, and security experience to his role as the general manager of the PCI Security Standards Council. Russo guides the organization through its crucial charter, which is focused on improving data security standards for merchants, banks, and other key stakeholders involved in the global payment card transaction process. To fulfill this role, Russo works with representatives from American Express, Discover Financial, JCB, MasterCard Worldwide, and Visa International to drive awareness and adoption of the PCI Data Security Standard.

“The PCI Qualified Integrators and Resellers (QIR) program will be rolled out over the coming months, with training set to begin in late summer and a global list of PCI Qualified Integrators and Resellers to be available later this year.”

Bob Russo, general manager, PCI Security Standards Council

behalf of software vendors or others, the opportunity to receive specialized training and certification on the secure installation and maintenance of validated payment applications into merchant environments, in a manner that supports PCI DSS compliance. The PCI SSC will maintain a global list of QIRs, ensuring merchants a trusted resource for selecting PCI approved partners.

At the PCI Council, it has always been our goal to help create resources that help merchants of all sizes develop strong security programs that aid in their ability to protect the integrity of the entire payment process, and help organizations minimize their ongoing risk of experiencing a data breach.

We think this is an important step in making it easier for you to deploy new security controls in your environment in a manner that you can feel confident in. It also will bring confidence to the resellers and integrators who are there to help you address security challenges.

Training will be offered online beginning in late summer 2012, and the validated list of QIRs for merchants will be published on the PCI SSC website shortly thereafter. More details on the program, including eligibility requirements, training course information, and costs will be made available soon. In the meantime, those interested in participating in the program can visit https://www.pcisecuritystandards.org/qir and contact qir@pcisecuritystandards.org with questions.

Your workforce isn’t second best. And your workforce management solution shouldn’t be either. Ceridian Dayforce Workforce Management has been identified as the leading solution in both usability and functionality by Nucleus Research in their Workforce Management Technology Value Matrix for the second year in a row.

Learn how this end-to-end workforce management solution including Time & Attendance, Labor Budgeting, Forecasting & Scheduling, Task Management, Employee Self-Service, Human Resources and Analytics can help your organization maintain a competitive edge.

Discover what sets this solution apart. Download the Nucleus Research report at knowhow.ceridian.com/nucleus, call 877-552-5669 or go to www.ceridian.com/workforce today.