5 COMMON PCI COMPLIANCE MYTHS/FACTS

Myth #1: Breaches only happen to big-box retailers.

Fact: Small- to medium-sized merchants are highly vulnerable and a frequent target. Based on most of the news coverage, security breaches may seem to happen only to huge corporations such as the TJX security breach that compromised more than 94 million T.J. Maxx and Marshall's accounts. But, in reality, cardholder data compromises affect small online store owners far more frequently. Why? Because, the sheer number of them (according to Visa more than 6 million) makes them a more frequent target. Also, they are typically the least sophisticated technologically making them an easier target for hackers and carders.

Myth #2: PCI compliant merchants cannot be breached.

Fact: While it is a critical step, PCI DSS compliance is only a periodic measurement at a point in time – not a guarantee. Just ask Hannaford Brothers groceries if PCI compliant merchants can't be breached. They were thought to be PCI compliant, but were still affected by a very public breach. There's a danger that organizations can develop tunnel vision dealing with PCI at the expense of building a sound security program. We recommend that companies develop a consistently high security posture, and in doing so, they will achieve PCI compliance. Any system involving people is vulnerable, either from accidental error or intentional acts of theft.

Myth #3: E-commerce merchants that use PCI compliant shopping carts or payment gateways are by default PCI compliant.

Fact: This may be the case, but PCI guidelines cover not only data security but also the physical security and the existence of written security policies. Once a year, regardless of how the merchant handles card data, every merchant is required to complete an SAQ, to complete the relevant Attestation of Compliance and, in most case, to submit the SAQ and the Attestation of Compliance to their acquirer. While it is important that terminals, gateways and shopping carts are compliant, that doesn't guarantee that merchants are secure from a physical standpoint or that they have employee training programs or security policies in place. SAQ A was specifically developed for merchants who outsource to a secure terminal.

Myth #4: PCI compliance is too expensive.

Fact: Non-compliance can be very expensive if not catastrophic. Non-compliance doesn't just result in costs associated with fines, credit card replacement and audit fees, but also from loss of business reputation and revenue. In fact a recent study stated that 70 percent of the cost of non-compliance was loss of revenue. This is significant for big companies that are crucified in the press, but may be catastrophic for small vendors, putting them out of business.

Myth #5: PCI compliance is getting easier.

Fact: The PCI Security Standards Council is working hard to clarify and simplify the standard. For example, in early 2008, the Council released version 1.1 of the Self-Assessment Questionnaire (SAQ), which now consists of four versions of the SAQ instead of the previous one-size-fits-all approach. While the attempt to segment merchants by validation type is a big step forward, it still presents confusion among many small merchants who are unclear on which SAQ they should complete. For small merchants in particular, protecting card holder data and maintaining a secure environment remains a complex endeavor.
