Retail credit card breaches and evolving security threats motivate organizations to increase compliance efforts

Target, Home Depot, and Albertsons have at least one thing common: hacked networks resulted in in millions of credit card number being stolen, costing millions.

SEATTLE, WA, USA, September 21, 2014 /EINPresswire.com/ -- Organizations that accept credit cards are required to comply with the Payment Card Industry Data Security Standard (PCI DSS). In some states, compliance is the law of the land. In those states that haven't passed similar legislation, compliance is a contractual requirement that merchants have with banks and credit card processors. Simply put: compliance is required, but security is essential.

In the last several years, credit card breaches have dominated the headlines. In 2007, TJ Maxx's lax security resulted in the theft of over 45 million credit card numbers. More recently, well known stores such as Target, Home Depot, Good Will, Albertsons, Neiman Marcus, and Michaels have all been breached, losing millions of credit card numbers. These breaches cost organizations hundreds of millions in remediation and fraud loss. Luckily, they were big enough to recover and continue business operations, but it's hard to regain public trust in the face of such injury.
For smaller organizations, the risk of credit card breach remains high, but the final result could be much more dramatic. In the event of a breach, merchants are responsible for a forensic investigation, remediation cost, fraud loss, and the more difficult to determine cost: loss of consumer confidence. To add insult to injury, they will face increased transaction costs and in some cases, the revocation of credit card acceptance privileges. This could force a smaller organization out of business.

Recently, InfoSecurePCI released the latest revision of its PCI DSS v3.0 security policies and procedures package. The new version offers expanded detail and updates designed to help organizations counter the ever-evolving threat of credit card data breach. "Credit card security and compliance, while necessary, is often confusing and difficult to implement, even for tenured security professionals," Patrick said, "InfoSecurePCI is a professionally developed package that helps organizations accelerate compliance and provides a consistent platform from which businesses can protect their most valuable data."

Everything an organization needs to understand and comply with PCI DSS v3.0 is included in an easy to implement package:

- PCI DSS v3.0 policy and procedure document
- User-level information security policy
- Business continuity plan and disaster recovery template
- Computer security incident response plan
- PCI operational security procedures document
- Risk assessment methodology
- Industry accepted configuration standards and guidelines
- Security awareness training program with PowerPoint slides, 15 minute video, and self-awarded training certificate

• PCI DSS compliance security matrix and cross-reference spreadsheet
• 60 days of unlimited support
• Future proofed security with free upgrades to subsequent policy revisions
• Money back guarantee

“All of our existing clients received this update free of charge and new clients will receive future updates as well. At InfoSecurePCI, customer service is mandatory, not a luxury. Every client receives personal attention: If my clients aren’t happy, I’m not happy, and that doesn’t happen,” Patrick stated.

The digital product is delivered immediately for only $249. For more information, visit www.pcisecuritypolicies.com

ABOUT INFOSECUREPCI
InfoSecurePCI, an organization founded by credit card security expert, Patrick Bass. He has been helping businesses navigate the risky waters of security and compliance for over 20 years. “I’ve helped major organizations create and implement complex information security programs focused on securing credit card data and complying with PCI DSS all over the country,” said Bass. Patrick is a former chief security officer for a major credit card processor and has been certified by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA), Internal Security Assessor, and PCI Professional. “Security is a passion for me,” said Bass, “I’ve dedicated my life and education to the pursuance of assimilating and expanding the security body of knowledge.” Bass has earned over 25 professional certifications including CISSP, CISA, CEH, CHFI, CCNP, and CCDP. He has an undergraduate degree in information security, an MBA, and a master’s degree in information assurance. Currently, he is completing a doctoral dissertation focused on business and information security, and is a university professor teaching graduate students the nuances of information technology.

Patrick Bass
InfoSecurePCI
425-460-4980 x 101
email us here
