FS/TEC panel offers insights into revised PCI security standards

BY PAUL FRUMKIN

ORLANDO, FLA. — Even as the foodservice industry and other businesses digest the latest version of the Payment Card Industry Data Security Standards, experts agree that operators will have difficulty achieving full PCI compliance and completely protecting credit and debit card information.

Payment card security stakeholders speaking at the 14th annual International Foodservice Technology Exposition, or FS/TEC, here in February acknowledged that PCI DSS Version 1.2, while improving on the initial release, nonetheless is no silver bullet.

"One-hundred-percent compliance is almost impossible, at least as far as I'm concerned," said Cihan Cobanoglu, associate professor of hospitality technology at the University of Delaware.

The standards were established to help ensure the adoption of consistent data security measures and enhance payment account security. Noncompliance by businesses accepting card payments can result in stiff financial penalties from card organizations.

Underscoring the difficulty businesses have protecting sensitive credit-card data from hackers and other thieves, Cobanoglu cited a study that found the number of events in which card data were compromised more than doubled in 2007 compared with 2006. The vast majority of those problems, he continued, involved track data, which has a credit card number and an expiration date.

Other experts taking part in the payment card security panel discussion pointed to the recent breach of Heartland Payment Systems. In that breach, intruders hacked into the computers used by Heartland to process payment card transactions for 175,000 merchants, including approximately 60,000 restaurants.

They also referred to an earlier breach at the Dallas-based Dave & Buster's casual-dining chain, in which three men allegedly hacked into multiple cash registers to steal data from thousands of credit and debit cards. Associated losses from that breach have been estimated at $600,000.

Cobanoglu said fine-dining restaurants suffered the most in the restaurant industry from not being PCI-compliant. He pointed out some common barriers to compliance, including limited budget, lack of education, lack of tools to manage PCI, lack of qualified staff, and lack of details with the standards.

PCI DSS Version 1.2 clarifies some of the confusion among merchants raised by the initial release, but not all of it, observed David Starmer, vice president of information technology for Back Bay Restaurant Group in Boston.

The largest rewrite, he said, occurs in Requirement 1 — the standards have 12 requirements or standards — which states that routers are now included and should be treated the same as firewalls. Moreover, the new requirement restricts WEP, or wired equivalent privacy, deployments. According to the new regulations, new WEP implementation was banned as of March 31, 2009, while current implementation is banned after June 30, 2010.

Under the first release of PCI DSS Requirement 6, patches to software needed to be applied in 30 days. Now the standards condone a risk-based approach, which Starmer called "a little more prudent and realistic." At the same time, he noted, "they tell you that you have to validate input, proper error handling, secure storage and others." What's more, the BBRG executive indicated, Requirement 6 now requires code review for common vulnerabilities or an application layer firewall in front of any Web-facing application.

Other changes incorporated into Version 1.2 mandate that operators set up cameras or other access control mechanisms in any data center or server room, and test for the presence of wireless points using a wireless analyzer on at least a quarterly basis, Starmer said.

David Denney, a practicing restaurant and hospitality industry attorney with The Law Offices of David Denney in Dallas, warned attendees, "The cost of noncompliance is incredibly high."

From left: David Starmer, Back Bay Restaurant Group; David Denney, hospitality attorney; and Cihan Cobanoglu, University of Delaware.

He said that under the standards, restaurateurs retain virtually all liabilities, including responsibility for charge backs, cardholder damages, the cost of reissuing stolen cards, credit card company attorneys fees, and fines and penalties for not being compliant.

"It can end up costing hundreds of thousands of dollars," Denney said. "You know things are bad when insurance companies are writing policies for the problem."

Denney advised attendees to conduct a background check on employees who have access to cardholder data, but acknowledged that the practice can become "a paperwork mess" because of turnover. He also said franchise agreements generally shift the burden of compliance to the franchisee, but often franchisors fail to sufficiently educate the licensee about credit card security.

If a credit card system is breached, Denney advised, operators should immediately inform their legal counsel or counsel for their franchisor, begin an investigation, take immediate steps to remedy the perceived threat and draft a press release utilizing the counsel's input.

In general, though, panel participants advised attendees to review the policies and procedures in Version 1.2, and make sure they have adopted the changes.

"If you're not compliant, you're probably in good company because that's most organizations," Starmer said. "If you're compliant today, you may not be tomorrow. It's a moving target we're after." ■

pfrumkin@nrn.com

**Scenes or words from the annual International Foodservice Technology Exposition, or FS/TEC, produced and managed by Nation's Restaurant News with Robert N. Grimes of Accuvia. FS/TEC 2010 is Feb. 21-24 at the Long Beach Convention & Entertainment Center in Long Beach, Calif. More information is available at www.fstec.com*