

A SUPPLEMENT TO HOSPITALITY TECHNOLOGY

PCI HOSPITALITY



MARKET UPDATE ON THE TECHNOLOGIES AND TRENDS THAT ARE IMPACTING PCI COMPLIANCE IN HOTELS & RESTAURANTS

- Keeping Up with PCI in 2010
- Network Security Best Practices
- How to Recover from a Security Breach
- Hot Compliance Products

Hospitality
TECHNOLOGY



PUBLISHER

Lenore O'Meara
lomeara@edgellmail.com

EDITORIAL

EDITOR-IN-CHIEF Abigail A. Lorden
alorden@edgellmail.com

ASSOCIATE EDITOR Christina Volpe
cvolpe@edgellmail.com

CONTRIBUTING EDITOR Lisa Terry

SALES

ACCOUNT EXECUTIVE Leah Segarra
lsegarra@edgellmail.com

ASSISTANT TO PUBLISHER Jen Johnson
jjohnson@edgellmail.com

ART/PRODUCTION

CREATIVE DIRECTOR Colette Magliaro
cmagliaro@edgellmail.com

ART DIRECTOR Melissa Mazza
mmazza@edgellmail.com

PRODUCTION MANAGER Jan Miciak
jmiciak@edgellmail.com

ONLINE MEDIA

VP, ONLINE MEDIA Rob Keenan
rkeenan@edgellmail.com

WEB DEVELOPMENT MANAGER Scott Ernst
sernst@edgellmail.com

ON-LINE EVENT PRODUCER Stephanie Gannon
sgannon@edgellmail.com

SUBSCRIPTIONS 978.671.0449

REPRINTS: PARS Int'l, 212.221.9595 x319

CORPORATE

CEO/CHAIRMAN Gabriele A. Edgell
gedgell@edgellmail.com

PRESIDENT Gerald C. Ryerson
gryerson@edgellmail.com

VICE PRESIDENT John Chiego
jchiego@edgellmail.com

CORPORATE OFFICE

4 Middlebury Blvd
Randolph NJ 07869
973.607.1300 FAX: 973.607.1395

FOUNDER DOUGLAS C. EDGELL 1951-1998



www.edgellcommunications.com

Contents

STANDARDS UPDATE

4 Evolving Standards: Keeping Up with 2010 PCI Changes
The PCI Standards Council is altering its approach to the often-confusing process of keeping up with requirement changes. Get the full scoop on the 2010 updates plus responses from the vendor community.

SECURITY SPOTLIGHT

6 Breach-Proof your Network
Stolen customer data often starts with breaches related to poor network security. Learn how to close network loopholes with these best practices.

INDUSTRY INSIGHT

8 You've Been Breached, Now What?
An industry expert offers a step-by-step guide for hotel and restaurant operators who have experienced a data security breach.

HOT PRODUCTS

12 Tech Vendors' Solutions to Aid PCI Compliance
Hospitality Technology rounds up some of the hottest transaction processing, POS and networking solutions to aid hotels and restaurants in achieving PCI compliance.

Copyright © 2010 *Hospitality Technology*. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or information storage and retrieval systems, without permission in writing from the publishers.



STANDARDS UPDATE

By Lisa Terry, Contributing Editor

Evolving Standards: Keeping Up with 2010 PCI Changes

The PCI Security Standards Council is altering its approach to the often-confusing process of keeping up with requirements changes to the PCI DSS (Payment Card Industry Data Security Standard). In addition to clarifying some regulations, they're also offering plenty of previews and feedback opportunity to upcoming changes, and are extending out the update timetable from every two years to every three.

"The standards are really strong at this point, and quite mature," says Bob Russo, general manager of the PCI Security Standards Council, launched in 2006, which develops and maintains awareness of PCI Security Standards on behalf of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. "There will not be such major changes going forward."

Here are changes for 2010, and how vendors are responding: PIN Pad changes

In May 2010, PCI announced version 3.0 of the PIN Transaction Security Point of Interaction requirements, unifying three formerly separate standards. This applies mostly to integrators, helping to ensure that separate components of a solution, for example a PIN pad, card reader, touch-screen, printer and enclosure pulled together for an unattended ticket machine, are each secure.

Process and software changes

At presstime, the Council had previewed, but not yet released, new versions of PCI DSS and PA-DSS (the Payment Application-Data Security Standard). Proposed standards were discussed at the North American Community Meeting Sept. 21-23, released

on Oct. 28, and become effective Jan. 1, 2011. Russo describes these as straightforward and not introducing significant changes. "If you were compliant last year, you should not have any difficulty complying this year." Hospitality executives should check with their Quality Security Assessors and acquiring banks to ensure that's the case for them, vendors urge.

Reducing PCI scope is a key goal, one that vendors are addressing by offering secure payment technology suites exclusively for payment, such as Mercury Payment's TranSecure, or DD Guard, a monthly service from Digital Dining and Vendor Safe that keeps restaurateurs on top of most PCI-DSS requirements and offers a \$50,000 insurance policy toward a PCI investigation.

With regulations just in preview, vendors haven't had much chance to assess their potential impact. However, most of the vendors consulted for this story, including Digital Dining, Hypercom, [Merchant Link](#), Mercury Payment, Motorola, Radiant Systems, Shift4, Vendor Safe and VeriFone, anticipate few, if any, changes to their respective products. Vendor Safe and Radiant Systems expect some of this guidance to reduce the compliance burden in general.

Highlights of the new regulations include:

1) Methodology: Merchants need to understand how to discover hidden cardholder data stores prior to assessments. This might include using data recovery tools, data leakage prevention measures and/or setting up a task force to look for cardholder data.

2) Centralized logging: This was a part of PCI-DSS but not PA-DSS; now it is. This regulation requires use of one central

data log instead of multiple logs.

3) External threats: Internal and Web-facing application developers were already required to check for coding vulnerabilities against the external OWASP list; that's been expanded to include CWE and CERT.

4) Clarifying applicability: Among other clarifications, the revisions confirm that only account numbers must be made unreadable, not name, expiration, etc.

5) Risk: Merchants are urged to work with assessors to prioritize individual compliance projects according to their own levels of risk.

Guidance documents to provide examples

The new regulations for October include guidance documents to help line up end-to-end encryption (the Council prefers the term point-to-point), tokenization and chip and PIN against PCI standards to note the particular features and capabilities required for these to be compliant.

This task is challenging with technologies such as tokenization because there are so many ways to do it. "We will take a sample tokenization environment and line it up with the standards" as an example, says Russo. The vendor community awaits these with interest. According to Shift4, which says it coined the term, in order to be a token the data needs to be random and not derived from the PAN (primary account number). If a watered-down definition appears in a PCI-DSS tokenization standard, such as one allowing certain types of encryption and hashing to be treated as tokens, they feel it would undermine the security and benefit of tokens and, most likely, bring tokens into PCI scope. Which is not what people want. **IT**



SECURITY SPOTLIGHT

By Lisa Terry, Contributing Editor

Breach-Proof your Network

Stolen data often starts with poor network security, follow these tips to safeguard yours

The secret to securing networks for PCI compliance is simplicity. But hospitality networks are complex, and growing more so. The geographic spread of many hospitality organizations, combined with diversifying uses of networks, including public Internet access, poses a challenge to securing these networks, protecting cardholder data and attaining PCI compliance. Add to that the growing number of third party hosted services connected to hospitality operators' networks; on top of all that is the complexity imposed by hospitality business models, which frequently include multiple franchisees, who are often operating under multiple brands.

Brands and franchises are connected not only through networks to exchange data, but in reputation. If an individual franchisee is impacted, it affects the whole brand; they're tainted by the publicity. According to Verizon's 2010 Data Breach Investigations Report, produced with the U.S. Secret Service, hospitality experienced 23% of the 141 confirmed breach cases worked by Verizon and the U.S. Secret Service in 2009,

second only to financial services.

Smaller hospitality organizations may be the most vulnerable to attack, yet often lack the IT resources necessary to fully attain and maintain PCI compliance. But with PCI enforcement increasing and the Ponemon Institute (www.ponemon.org) reporting data breach incidents costing U.S. companies \$204 per compromised customer record in 2009 and an average \$6.75 million per incident, the risk is high. Many brands are stepping in by educating franchisees and offering packaged solutions to address PCI.

Managed private networks are a common approach offered by brands to franchisees, such as New Edge Networks' (www.newedgenetworks.com) MPLS product, which will soon include a security platform. Ideally, there are two networks: one for non-payment data including guest Internet access, and a second one dedicated to payment traffic. Using this approach, instead of individual site connections to processors, payment data travels from individual properties through the private corporate network and then out to the

processor via a single connection, lowering individual site costs. A less costly option is a brand-sponsored, shared private network with additional security to separate the data. Franchisees may operate their own internal portions of the larger network behind a firewall.

Similarly, hospitality operators are leveraging managed network capabilities from Hughes Electronics (www.hughes.com) to offer customized packages of services designed to address franchisee needs, whether PCI specifically or full network management including PCI DSS-compliant WAN services, wireless PCI intrusion and detection services, encryption, and managed firewall security features.

For its part, BHI Advanced Internet has an extensive solution set called Secure Connect (www.secureconnect.com) that includes firewall, VPN, antivirus and more. Unique in the industry, BHI also offers customers a breach protection program that covers up to \$100,000 in merchant fines, assessments and related expenses attributed to a qualified PCI data breach. **HT**

HERE ARE SOME NETWORKING BEST PRACTICES:

1 Basic block and tackle moves. It should go without saying, but unfortunately many breaches occur due to neglect of basics like changing default security settings and using strong passwords and one- or two-factor authentication, increasingly a feature of POS systems. Breaches in the hospitality industry are often the result of hacking and malware, according to the Verizon report.

2 LAN segmentation. The idea of segmentation is to wall off payment processing from the rest of the network, thereby placing the rest of that network outside the scope of PCI assessment. But there is some disagreement as to what methods of segmentation truly attain the goal of complete separation; PCI watchers are hoping that upcoming new regulations clear up those uncertainties.

3 Scanning. Any exposure to the network needs to be scanned internally and externally; another benefit to architectures that funnel all of a hotel chain's network traffic through a central point, then out to the Internet, is the ability to scan in only one place.

4 Encryption and tokenization. Point to point encryption of data at rest and as it travels across the network, as well as use of tokens to replace live data, are becoming musts.

5 Port matrices. Obtaining port matrices of any applications riding on the network is essential to understanding potential vulnerabilities. Avaya (www.avaya.com), for example, is frequently asked to provide an application port matrix for its voice applications, revealing the addresses, assignments and ports they use.



INDUSTRY INSIGHT

By Gary Palgon, PCI Security Standards Council Lead Chair, Tokenization Scoping Special Interest Group

You've Been Breached, Now What?

Best practices for handling a data security breach

Hackers are becoming more sophisticated and targeted in their attacks, finding what works and then repeating it. And according to Trustwave's (www.trustwave.com) Global Security Report 2010, they're going after the hospitality industry in a big way. In fact, 38 percent of all attacks in 2009 were against hotels and resorts. Most of these breaches involved credit card numbers, yet the personal information hotels collect and store for participation in loyalty programs is equally vulnerable. If your hotel or restaurant experiences a breach, there are several things you can do to prevent it from happening again.

Step 1: Don't touch anything

Although it may be tempting immediately following a breach to make changes to your IT infrastructure, this is absolutely the wrong approach. Changing anything, including turning off the compromised machine, accessing it or altering it in any way, can destroy or contaminate evidence, which forensic auditors will need to determine what happened, how it happened and the scope of the breach. Preserve the logs and electronic evidence and document all actions you take. Next, notify the local office of the U.S. Secret Service. Visa's "What to do if Compromised" (<http://usa.visa.com>) guide is a good resource that contains step-by-step instructions on how to respond to a security incident.

Step 2: Determine what needs to be fixed

Once you know the scope of the breach and how it occurred, you can determine how to remediate it. To do this, first decide the best approach for your unique situation. Is

it enough to simply shore up the obvious weak spots in your IT infrastructure, or is a more strategic approach warranted? Performing a risk-based analysis may take longer, but for many companies it's the most effective approach because it will identify exactly where security gaps exist. Once you know the extent of the problem, you can prioritize which steps to take first.

Step 3: Fix the problem

Fixing the problem that enabled the breach to happen in the first place can

require a number of adjustments to both best practices and technology. Complying with the Payment Card Industry's Data Security Standard (PCI DSS) is a good first step toward protecting credit card data, but recent breaches of PCI-compliant businesses illustrate that compliance doesn't equate to security. Rather than taking the "check-list approach" to data security that compliance often fosters, adopt the position that data security is an ongoing process that requires continual adaptations to best practices, technology, and





employee and franchisee education.

Data security technology solutions are effective and continue to evolve. Traditional approaches encompass strong, local encryption and encryption key management to protect cardholder information. In addition, a new data security model, tokenization, is emerging. Unlike traditional encryption methods where the encrypted data or “cipher text” is stored in databases and applications throughout the

HACKERS ARE BECOMING MORE SOPHISTICATED AND TARGETED IN THEIR ATTACKS, FINDING WHAT WORKS AND THEN REPEATING IT.

enterprise, tokens, or surrogate values, take the place of the original data, rendering the data useless in the event of a breach. The entire credit card number can only be viewed by authorized employees who have the encryption key.

Technologies to minimize risk

The Payment Card Industry recommends that to minimize risk companies should first get rid of any stored payment card data that isn't truly required for the business. By limiting occurrences of encrypted data to a central vault, hotels can reduce the number of systems, applications and processes where payment card numbers are stored. This has the added advantage of reducing the scope and costs for compliance audits. Tokenization takes that “footprint reduction” concept one step further while also adding another level of security; key reasons why the technology is gaining traction with chief security officers and IT

executives in the hospitality industry, and with industry analysts who follow security technology. It offers the hospitality industry the same benefits.

When a token is generated, certain portions of the data, such as the last four digits of a credit card number, can be maintained to provide a business context of the original value so that applications work the same as when full credit numbers are displayed. The encrypted data the token repre-

sents is then locked in a central data vault. Because a token is not mathematically derived from the original data, it cannot be reversed using an algorithm like cipher text. Authorized applications that need access to encrypted data can only retrieve the data using a token issued from a token server.

Be aware of technologies that use the term tokenization more loosely, in that they might modify cardholder data, but don't necessarily replace it completely at the swipe and fully remove it from the system. Security vendor Shift4 (www.shift4.com), which credits itself with first coining the term tokenization, offers what it calls a TrueTokenization technology solution that replaces cardholder data with the TrueToken and stores the actual encrypted data on the Shift4 gateway.

One data security vendor, nuBridges (www.nubridges.com), offers a variation of tokenization, called “Format Preserving Tokenization.” Under this tokenization model, the token uses the same amount of

storage as the original clear text data instead of the larger amount of storage required by encrypted data. This reduces data storage requirements and preserves storage space on point-of-sale systems. Format preserving tokenization can also be used to protect any type of personal information required by hospitality loyalty programs or by other countries, such as passport numbers, without modifying data fields.

Localized encryption is the default when hotels in the chain are not always connected to a central data vault. In instances where hotels are electronically connected to the data vault, tokenization may be the best solution. For many hospitality companies, using a combination of localized encryption and tokenization, along with centralized key management, is the most practical approach for protecting cardholder and personal information. **Merchant Link** (www.merchantlink.com) just announced its E2EE solution, for end-to-end encryption along with its TransactionVault tokenization solutions. According to the vendor, from the point of swipe to transaction completion this solution secures both “data in-flight” and “data at rest,” meaning both stored credit card data and transaction data flowing through networks will be protected from hackers and cyber criminals.

Whichever technology approach is right for your company, it's equally important to initiate a lifecycle data security program that incorporates best practices for protecting data wherever it resides or travels throughout your enterprise to stay ahead of the bad guys and prevent another breach. **HT**

Additional reporting by Abigail A. Lorden, editor-in-chief, Hospitality Technology & Vertical Systems Reseller.

About the Author

Gary Palgon is a Certified Information Systems Security Professional (CISSP) and serves as the Lead Chair on the Tokenization Scoping Special Interest Group for the PCI Security Standards Council. He is a frequent contributor to industry publications and a speaker at conferences on eBusiness security issues and solutions.



HOT PRODUCTS

Vendor Solutions to Aid PCI Compliance

TRANSACTION PROCESSING

DIGITAL DINING / VENDOR SAFE

Table-side ordering and payment vendor Digital Dining (www.digitaldining.com) has teamed up with Vendor Safe Technologies (www.vendorsafe.com) to offer a joint payment security solution, DD Guard. Using Vendor Safe's PCI Managed Security Suite, this solution enables Digital Dining end-users to achieve Payment Card Industry (PCI DSS) compliance standards within 30 days.

ELAVON

Elavon's (www.elavon.com) payment and gateway hospitality solutions promise to help secure cardholder data, protect against breaches, and reduce the scope and resources associated with card association compliance standards. Elavon's solutions interface with all leading PMS systems, and support tokenization and end-to-end encryption technologies. Tokenization services are supported on ProtoBase, Fusebox and Elavon's network. End-to-end encryption services encrypt card account numbers and mag-stripe data at the POS to Elavon's network. Elavon also offers PCI compliance support and PCI audit analysis to identify de-scoping opportunities.

FIFTH THIRD

Fifth Third Processing Solutions (www.ftpsllc.com) has designed a solution that encrypts critical payment and cardholder data at the front-end of the payment process and maintains the security of that data through all of the processor systems. This data security solution provides a single platform for both end-to-end encryption and tokenization to help merchants remove sensitive card data from authorization systems as well as back-office business applications. Fifth Third Processing Solutions is working with Voltage Security, Inc. (www.voltage.com) to offer several new

customer solutions focused on the protection of sensitive cardholder information.

FIRST DATA

First Data's (www.firstdata.com) TransArmor protects consumer payment card data from the moment it enters the merchant environment, and replaces it with a token number that preserves the value of card data for merchant business operations while removing all value for fraudsters. As a result, merchants are able to reduce the scope, risk and costs associated with PCI compliance without requiring new hardware or extensive changes to existing business processes. According to the vendor, the TransArmor solution meets all of Visa Inc.'s recently released best practices for card data tokenization.

HYPERCOM

Designed for self-service guest registration or customer-facing checkouts, Hypercom's (www.hypercom.com) PCI-approved L5300 features a full VGA color 5.7" screen, interactive multimedia display and signature capture, integrated keypad with side lighting, audio speaker and audio jack, modular communications and optional Contactless and EMV smart card readers. The L5300 is a member of Hypercom's L5000 family of multipurpose terminals featuring a broad range of communications capabilities. The family also features data encryption technology, Hypercom's X509 PKI HyperSafe security layer, to protect from hacking, malware attacks and more.

MERCHANT LINK

Merchant Link (www.merchantlink.com) now offers a combined end-to-end encryption (E2EE) and tokenization solution. Hotels can use Merchant Link's E2EE product coupled with TransactionVault, a solution that replaces credit card numbers with format-preserving tokens compatible with

existing business processes and systems. The tokens remain associated with customer cards for folio consolidation, customer analytics and marketing purposes. The combined solution secures both data at rest and data in-flight, enhancing security while reducing PCI scope and compliance cost. Additionally, Merchant Link's payment gateway offers support for all transactions.

MERCURY PAYMENT SYSTEMS

Mercury Payment Systems (www.mercurypay.com) offers multiple solutions for operators including: MercuryShield, a suite of security technology solutions for POS systems that reduce the risk and cost of PCI standards compliance; and TranSentry, a solution that removes the POS from the scope of PA-DSS by eliminating the handling of sensitive card data at the POS. Other solutions include TranSecure, which combines Mercury's end-to-end encryption and proprietary tokenization technology, and MToken, Mercury's advanced tokenization technology.

SHIFT4

Shift4 Corporation's (www.shift4.com) 4Go technology captures cardholder data (CHD) immediately following the swipe and replaces it with false data to prevent the merchant's system from storing, processing, or transmitting actual CHD. It is included at no additional cost with Shift4's DOLLARS ON THE NET solution, and can also be combined with Shift4's TrueTokenization and Fraud Sentry technologies.

TABLETOP MEDIA

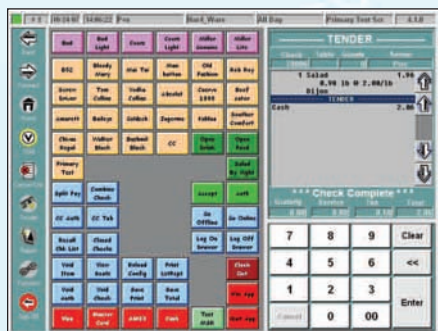
TableTop Media's (www.tabletopmedia.com) Ziosk is a seven-inch wireless touch screen device that offers a number of applications including digital interactive table tents, e-club enrollment, surveys, games, news, and pay-at-the-table. Guests are able to pay with a variety of payment options, and the

payment is immediately authorized and settled by the merchant using the existing POS system. In full compliance with PCI, the controller includes a firewall that prevents any external source from gaining access to the system.

VERIFONE

Criminals are becoming increasingly sophisticated at exploiting gaps in the implementation of environmental security requirements. To counter these attacks, VeriFone (www.verifone.com) is extending the security perimeter with the VeriFone PED Authentication Service (VPAS). VPAS utilizes a highly secure Unique Manufacturers Authentication Key (UMAK) that binds each device with a physical location at the POS. If a device is installed without a matching UMAK, VPAS will rapidly notify the merchant, processor or bank.

POS SOFTWARE AND HARDWARE



AGILYSYS

Designed for multi-unit operations, Agilysys' (www.agilysys.com) InfoGenesis is an enterprise-ready POS solution that combines powerful reporting and configuration capabilities with an easy-to-use touch-screen terminal application. The system's Service-Oriented Architecture (SOA) enables interfaces to a wide range of host systems, such as payment card processors and guest management solution providers. InfoGenesis POS v4.1 is certified by the PCI Security Standards Council as PA-DSS compliant.

ALDELO SYSTEMS

Aldelo System Inc.'s (www.aldelo.com) PCI compliant EDC software combines AES256 bit encryption with uniquely created card encryption passwords. Encrypted card data is stored only for the short time needed to complete the transaction. Aldelo EDC and Aldelo For Restaurants products are developed in-house

ASI / RESTAURANT MANAGER

Restaurant Manager's (www.rmpos.com) Write-On Handheld is PCI compliant and offers an integrated table-side ordering and payment solution that utilizes an iPod Touch fitted to an integrated MSR reader from Infinite Peripherals (www.ipcprint.com). Settling a customer's check via credit card is done without the actual card ever leaving his/her sight. Servers select the credit card settlement option on the Write-On Handheld, take the customer's card, swipe it directly in front of the customer, and hand the card back. There is no opportunity for skimming or copying the card information.



FUTURE POS

Future POS (www.futurepos.com) has incorporated end-to-end encryption and credit card tokenization processing. By using MagTek's (www.magtek.com) encrypted Magnetic Card Reader and Mercury Payment Systems (www.mercurypay.com) for credit card processing, a merchant can protect themselves from having a POS related credit card security breach. All of the credit card data is encrypted as soon as it's swiped through the MagTek MSR, and it is only readable by the credit card processing servers at Mercury Payment Systems.



MAITRE'D BY POSERA

The Electronic Funds Transfer Module within the Maitre'D (www.maitredpos.com) Software Suite allows merchants to communicate directly with financial institutions to authorize credit and debit card transactions. A proprietary algorithm embedded within Maitre'D automatically generates new encryption keys for every single transaction that takes place. This means that rather than have the same encryption key protecting all of a merchant's information over an entire year, (the minimum requirement stipulated in the strict PCI guidelines) each and every transaction is encrypted with brand new keys, every time.

MICROS

Micros (www.micros.com) is now an authorized reseller of the Trustwave (www.trustwave.com) Unified Threat Management (UTM) security and the TrustKeeper (external vulnerability) PCI scanning package (the "Security Program"). The Security Program consists of a comprehensive suite of security hardware, software and services to safeguard critical business information delivered by Trustwave. The Security Program meets many of the PCI DSS compliance requirements and includes a custom-configured and managed firewall, anti-virus application with updates, PCI DSS compliant logging and log monitoring, intrusion detection, file integrity management, scanning for unencrypted cardholder data, and much more. Security Program customers are also protected by a \$50,000 breach insurance policy.



HOT PRODUCTS CONT'D

PARTECH

ParTech's (www.partech.com) PAR EverServ TSR (Table Service Restaurant) is an enterprise-grade POS solution that enables restaurant operators to efficiently manage operations. EverServ TSR incorporates an open architecture and seamless XML integration, making it easy to integrate other technologies like third-party accounting software or mobile ordering. The solution speeds payment processes with the handheld Pay2Go module, allowing wait staff to settle payments wirelessly at the table. PAR EverServ TSR is PA-DSS validated.

PCAMERICA

pcAmerica (www.pcamerica.com) has upgraded its Restaurant Pro Express (RPE) and Cash Register Express (CRE) POS software to satisfy requirements set forth in the latest PCI standards. Version 12.5 of RPE and CRE fully support now-mandated 3DES pin pad encryption, which protects merchants against security breaches with additional encryption and decryption combinations that are harder for hackers to break. pcAmerica also offers solutions that go beyond PCI-DSS compliance requirements by integrating with encrypted magnetic stripe readers, which encrypt credit card track data before it is sent into the POS terminal.

RADIANT SYSTEMS

Secure Access from Radiant Systems (www.radiantsystems.com) enables restaurant operators to remotely access their Aloha POS back office PC to safely transfer files or run POS reports. Utilizing two-factor authentication, Secure Access requires users to enter a password and a unique code generated on their mobile device or RSA secured to maximize protection of cardholder data. Secure Access provides a variety of alerts that show potential security issues, such as out of date antivirus definitions. Currently in an aggressive beta testing stage, Secure Access is expected to be available by the end of 2010.



SQUIRREL SYSTEMS

Squirrel Professional, a PA DSS certified POS from PCI Participating Organization Squirrel Systems (www.squirrelsistemas.com), aids merchants in becoming PCI compliant by giving them the option to integrate with Pay@Table wireless technology to process credit and debit card payments directly at the table. The Pay@Table devices do not pass any sensitive cardholder data to the Squirrel Professional system, which means the POS does not store, transmit, or process this information.



WAND CORPORATION

WAND SecurePay (www.wandcorp.com) is an application that is included in the Digital Restaurant solution, which offers conversational ordering, Web-based enterprise management, labor savings with Smart Scheduler, real-time consolidated reporting, and integrated digital customer engagement. The solution uses an integrated MSR at the POS, yet it maintains

PCI compliance for the store. With SecurePay, vital cardholder information is handled separately from other POS data, ensuring compliance. The Digital Restaurant unites NextGen POS, Digital Menu Boards, Back Office Software, Enterprise Management, and Analytics.

NETWORKING

BHI ADVANCED INTERNET SOLUTIONS / SECURECONNECT

The fully-managed security solution offered by SecureConnect (www.secureconnect.com) scans the network environment, so that merchants can identify areas of weakness within the network that could be used by a hacker, employee, virus or worm to gain access to and steal cardholder information. Offering security beyond PCI, SecureConnect provides comprehensive, turn-key solutions that save merchants time, money and frustration by working through a single vendor to meet network security needs and PCI compliance requirements.

MOTOROLA

The Motorola AirDefense Security and Compliance Solution (www.motorola.com) is a centralized console that provides complete protection against wireless threats, policy compliance monitoring, robust performance monitoring, and location tracking. Powered by advanced intrusion detection system (IDS) engines, the solution allows users to identify hackers, network attacks and vulnerabilities, and to instantly terminate the connection to any rogue device. The system uses collaborative intelligence with secure sensors that work in tandem with a hardened purpose-built server appliance to monitor all 802.11 (a/b/g/n) wireless traffic in real time. As a key layer of security, Motorola AirDefense complements VPNs, encryption and authentication. **HT**

SECURITY HOSPITALITY



SPONSORED BY:

Hospitality TECHNOLOGY