Greetings from the PCI SSC 2014 Chair

LIB DE VYRA, Vice President of Emerging Technologies, JCB International

It's great to have the opportunity to take on this role again, especially at this challenging and promising time in global payment security. I'm particularly encouraged by the continued growth of the PCI community in the Asia-Pacific region and look forward to building on the success of our first ever Community Meeting with our gathering in Sydney this year.

Thank you for continuing to be a part of the work we're doing to improve payment security around the world. In the year ahead, we are excited to work side by side with you on implementing PCI DSS 3.0 to make payment security part of business-as-usual practices across our organizations and the payment chain. And as the payments system changes and new technologies evolve, we will once again be looking to you for your expertise and feedback to create standards and resources for the protection of cardholder data across all payments channels.
Reflections from the Board of Advisors

Henrique Kazuhiro Takaki  
*Risk Control Manager, Cielo S.A.*

The technology evolution has leveraged many changes in our way of life. These changes have presented positive and negative sides. Now we are living in a world where information is an asset, as are material goods, and the concern with this asset is growing fast. The development of risk awareness and the need of security for both businesses and government are notable. For example, the Brazilian government recently approved a law that equates card cloning with ID forgery and criminalizes the installation of gadgets that make unauthorized copies of magnetic stripes.

In Brazil, around 90% of transactions are carried out with the use of chip technology and the fraudsters’ focus has moved to card-not-present sales. The PCI DSS is recognized as one of the tools used to reduce security incidents that obtain cardholder data to conduct fraud in this environment.

On the other hand, merchant opposition to fully complying with the PCI DSS and even to complete the self-assessment questionnaire is also increasing. The domestic market has regional characteristics that make the adoption of mandatory rules more difficult and expensive and a challenge to acquirers and brands.

Because of the challenges noted above, I really believe that the joint participation of several countries and business segments will be useful for the exploration of these problems in order to find viable solutions; together we will transform the PCI DSS into a real and applicable global standard.

Lara Nwokedi  
*Head, Information Security, First Bank of Nigeria*

In 2010, Nigeria’s apex bank and financial regulator, Central Bank of Nigeria (CBN), introduced a cashless policy to drive wider adoption of electronic channels and reduce costs associated with processing cash-based transactions in the country. Recognizing that the environment may be unprepared for the sudden and expected significant growth in the adoption of e-payment systems, CBN also mandated the implementation of the Payment Card Industry Data Security Standard (PCI DSS) by all financial institutions in Nigeria. In implementing the PCI DSS at First Bank of Nigeria, the standard was observed to be rigorous, thorough and consisting of well-defined measures that will enable security-focused organizations to see beyond the baseline controls. With the implementation of PCI DSS, it has become evident that the Bank’s processes and technologies have been built to significantly enhance its card data environment and the security of its customers’ funds and payment details. First Bank of Nigeria is proud to be the first African organization to be on the Board of Advisors of the Council. We see this as an opportunity for us to bring the unique challenges and perspectives of the African region to bear on the PCI SSC.

Have you taken a PCI SSC training course this year?  
Would you like to share how your training has enabled you to help your organization on the road to PCI compliance?  
We’d like your insights on the personal and organizational benefits of our instructor-led and eLearning courses.  
To participate, please contact press@pcisecuritystandards.org.

**UPCOMING EVENTS**

- **2014 Smart Card Alliance Payments Summit**  
  4–7 February  
  Salt Lake City, UT

- **ICE Totally Gaming: Cybercrime, Security & Regulatory Compliance in Gaming**  
  5 February  
  London, UK

- **G2 Merchant Risk Summit**  
  10–13 February  
  London, UK

- **MasterCard Global Risk Management Conference/MEA**  
  17–20 March  
  Dubai, UAE

- **MasterCard Global Risk Management Conference/Americas**  
  18–22 May  
  Laguna Beach, CA

- **MasterCard Global Risk Management Conference/LAC Operations Forum**  
  2–5 June  
  Orlando, FL (in Spanish Only)
Meet QIR Mark Weiner

The PCI SSC chatted with Reliant Security’s Mark Weiner to learn more about why he became a Qualified Integrator and Reseller (QIR).™

PCI SSC: What does your company do?
Mark: Reliant’s Redbox Platform transforms the delivery and support of retail systems through an appliance-based converged infrastructure solution, which enables a wide range of applications, PCI security and network configurations. The Redbox Platform solution replaces retail’s traditional, inflexible approach to store systems with an agile model that can be centrally managed across a countless number of stores and eliminates the need for additional dedicated equipment to run each in-store application. The result: retail executives can keep pace with 21st century customer-engaging applications while keeping costs in control by using this highly flexible and secure architecture.

PCI SSC: What do you do for your company?
Mark: My passion is building and leading innovative technology businesses that exceed customer expectations while achieving tough revenue and profit goals. In my current role as Chief Operating Officer, I am responsible for the company’s service offerings, sales, operations and finances. In my infinite spare time, I double as Reliant’s Information Security team leader and am focused on cost-effective solutions for securing payment card transactions in retail and e-commerce.

PCI SSC: What is your professional experience?
Mark: I am a former QSA, turned payment systems integrator. Prior to this, I led the Information Security Practice at a large hosting company, where I was first exposed to the challenges that retailers faced with PCI DSS compliance.

PCI SSC: Was there a personal/corporate issue that prompted you to seek training?
Mark: As a systems guy in a PCI community long dominated by the assessor community, I was frustrated that there was no place in the PCI universe for someone like me. When the Council announced the start of the QIR program, I jumped at the chance to be the first to get the training.

PCI SSC: Why did you choose to get training through the Council?
Mark: We like to go to the source. There is only one universally accepted source of information and training that both our peers and customers will accept, and that is the PCI Security Standards Council.

PCI SSC: How will training benefit you personally/your company?
Mark: While Reliant has always held itself to the highest standards for security and meeting PCI requirements, the training convinced us to apply some new best practices recommended by the Council for remote access of customer sites, project planning and defining deliverables associated with a customer deployment. As a QIR company, we are able to more simply articulate our value proposition and provide a service that is measurably better than our competitors.

PCI SSC: How long would you estimate before the average employee is faced with a situation on the job where this training applies?
Mark: Since we are system integrators, the training applies to most everything we do, so not long.
Global Security Insights: The Turkish payment industry – security and innovation hand-in-hand

Turkey is regarded as an emerging market in the payments industry. As of October 2013, the total number of credit and debit cards in Turkey was 155 million, ranking as the second largest market in Europe. Credit and debit cards have become a vital component of the Turkish economy with annual card transactions in 2012 totaling 3.83 billion, accounting for 36% of consumer spending.

Development of innovative loyalty programs and interest-free purchase options have helped increase the penetration of credit cards in all levels of the Turkish society. Between January and October 2013, 28% of all credit card purchases were paid through installments, with an average period of 9 months.

BKM of Turkey is a significant stakeholder in Turkish payments industry, aiming at improving the card payments system for the benefit of all member banks with efficient, cost-effective and secure solutions. Founded in 1990, BKM’s core business is to operate a Message Switching System and perform clearing and settlement. Along with clearing and settlement, BKM sets and oversees application of domestic rules in the local market. The role of BKM both as a payment service provider and as a rule maker is another distinctive feature of the Turkish payment industry.

BKM’s vision is to increase the penetration of payment cards, to eventually create a “cashless society” in Turkey by 2023. In order to realize this vision, BKM launched a digital wallet, called “BKM Express”. The most striking security feature of BKM Express resides in that upon card registration, the cardholder only enters first 6 and last 4 digits of Primary Account Number (PAN) to the system, and authentication is performed by BKM Express infrastructure and the Bank system respectively. Online payment features, mobile payments and P2P money transfer are supported on mobile devices on iOS, Android and HTML5 platforms. Within the scope of the strategic Digital Wallet Roadmap, more will follow such as supporting of loyalty programs, usage of coupons, e-invoice payments and inclusion of contactless technology, including Near Field Communication (NFC).

In June 2012, BKM Express, the secure and convenient payment platform that has started a new era in e-commerce in Turkey, was awarded in the “Best Channel” category of Merchant Payments Ecosystem Awards in Berlin. As of October 2013, the annual volume generated via e-commerce increased by 37%. As of end of October 2013, BKM Express covers 200,000 cardholders, 185 merchants and 15 member banks. With those 15 banks, 92% of all payment cards of Turkish market will be covered.

Turkey is positioned to be one of the largest credit and debit card markets of Europe. With a good track record in fraud prevention coupled with CHIP & PIN experience as an early adaptor, Turkey will continue to be an innovative and secure market in the global payments world.

BERNA SIREL
PCI SSC Board of Advisors, Bankalararasi Kart Merkezi (BKM), IT Compliance, Risk and Information Security Vice President

“With a good track record in fraud prevention coupled with CHIP & PIN experience as an early adaptor, Turkey will continue to be an innovative and secure market in the global payments world.”

Interested in contributing to the July issue of PCI Perspectives?
Submit to pcinewsletter@pcisecuritystandards.org by 16 May!
As we launch into this new year it is worthwhile to reflect on the end of 2013 to help gain an understanding of what will be happening in 2014.

We held our European Community Meeting in Nice with excellent speakers, fantastic attendance and even better weather. The launch of PCI DSS version 3.0 was a key topic of discussion at the event. Effective as of 1 January, the standard is available on the website, with supporting documents including Self-Assessment Questionnaires (SAQ) coming shortly thereafter.

It was at this meeting that we announced another significant milestone – the first validated Point-to-Point Encryption (P2PE) solution. Not surprisingly, given the EMV chip and PIN environment, it came out of Europe, and was closely followed by a second in November. We are expecting many other solutions to achieve validation in 2014, and are excited about merchants being able to take advantage of this technology in their payment security efforts.

On a macro level there were some developments taking place that have an impact on the larger data security landscape. In the UK specifically, the government which had earlier in the year sent out an RFP for a Cyber Security Standard, determined that no one standard could address the issue and that it would undertake the effort to craft its own. We are encouraged about the involvement of many UK data security experts and organizations in this process and that the government is aware of the PCI Standards and the benefits of these resources for data protection.

On top of this the Financial Conduct Authority, (FCA) has released a document relating to the security of mobile banking. This document highlights some of the security issues that mobile commerce users should be aware of. Additionally, the European Central Bank, (ECB) has released a draft of its SecurePay Group “Recommendations for Securing Mobile Payments.”

Talking of the ECB, their other SecurePay document, “Recommendations for Securing Internet Payments,” has been incorporated into the latest version of the Payment Service Directive. We can expect the European Parliament to be trying to push this through before the next set of elections in May. What this will mean is that organisations will be expected to meet the Key Recommendations, and the key date for this is February 2015. Having spoken to the FCA they are very likely to ratify this if it is approved by the EU.

In November, it was Cartes for Europe, which means all of the payments industry moves into Paris for a few days. Having a chance to walk around the biggest payments exhibition, I was struck by how many Asia Pacific based organisations were exhibiting at Cartes, and that every terminal vendor had a blue tooth paired PIN Pad on stand which would be linked to mobile acceptance device to enable chip and PIN using mobile.

So it is clear to me that 2014 in Europe is going to be even more about mobile and mobile commerce, and for us at the Council we will be continuing our efforts in this area through our mobile taskforce.

Additionally, with 2014 being an implementation year for the new version of the PCI DSS and PA-DSS, we will focus on driving adoption of the new standards. Also we will continue efforts to reach new markets that are busy in the card space but have not yet fully adopted PCI, and even more time supporting developments and progress within the various European governments.

In addition, a new task formed for 2014 will be visiting all our European Affiliate members to ensure they are getting everything they expected out of their involvement in PCI. The new membership structure has been a great move forward for the Council and helps drive continued industry involvement in our efforts to improve payment security.

I am quite excited for this coming year and the work that we’ll accomplish together not just in Europe but globally. Thanks for your continued support and participation.
INTRODUCTION:
Capita’s Payment Gateway is one of the largest payment processors in the UK, processing well over two million card transactions a month, servicing over 310 separate merchant organizations with e-commerce, face-to-face, and both automated and call-agent-managed telephone payments. Capita’s clients benefit from highly customized and seamlessly integrated payment applications and solutions, which significantly reduce their cardholder data touch and scope, therefore limiting their risk and their involvement in meeting PCI compliance. Capita’s highly flexible and configurable solutions provide secure and mission-critical payment collection services across a variety of markets, including education, health, insurance, local government and social housing across the public and private sectors.

As a large payment processor, Capita was required to undertake an independent security assessment on an annual basis – a QSA assessment. The security of Capita’s payment processing operations had always been a top priority for the business, which had used its economies of scale in order to invest in levels of IT security and staff expertise that most merchants can only ever dream of obtaining. Even though a “bank-like” security posture had been achieved in 2006, the prospect of a third-party security assessment against a new set of highly prescriptive security requirements challenged the business to re-examine its entire security operations from top to bottom. The review found the business had a few, mostly minor gaps, but also areas where it exceeded the requirements.

CHALLENGE:
Where the business exceeded PCI DSS requirements, the most notable example was around requirement 11.2.2, to perform an external vulnerability scan conducted by an Approved Scanning Vendor (ASV), on an at least quarterly basis. Capita had already adopted external vulnerability scanning by an ASV, with scans undertaken on a daily basis, well beyond the PCI DSS requirement. The business considered that the potential of vulnerability exploitation from the Internet carried a higher degree of risk than the standard’s minimum level requirement. Capita also exceeded the standard requirements through providing stronger levels of encryption and key management. The business already assessed and understood the value of cardholder data and risk in its compromise, and had adopted an approach to keep it secure at all times.

The gaps in complying with the PCI DSS tended to be where the standard is geared. So file integrity monitoring was something new and was duly introduced, and the business’s centralized auditing and monitoring routine was completely rebuilt from scratch. Wireless networking was not permitted on the Capita premises, as back in 2006 most wireless networks were deployed insecurely using WEP, while the successor technology at the time, WPA, was still unproven, so Capita opted to avoid wireless networking risks and banned all usage at sites that had cardholder data. Despite wireless networking being prohibited, there was still a PCI DSS requirement to be met in that the business had to check for the presence of rogue wireless devices at its in-scope sites. At the time there was little guidance on how to meet this requirement; however, the business had just signed up as a PCI SSC Participating Organization.

APPROACH
Capita’s involvement as a PCI Participating Organization presented an opportunity to provide feedback to the PCI SSC and provided an opportunity for Capita’s Security Officer, Dave Whitelegg, to join a Special Interest Group (SIG) on Wireless Networking. The SIG held several meetings, which allowed sharing of knowledge and ideas with wireless and security experts.
from similar minded organizations from around the world. The outcome of the Wireless Networking SIG was the creation of the PCI DSS Wireless Guidelines, which has provided clarity on PCI wireless networking requirements and has helped others in the industry to achieve compliance.

In 2007 Capita was assessed for PCI DSS compliance by an independent QSA. It became one of the first businesses to achieve QSA validated PCI DSS compliance in Europe and has maintained compliance ever since. After the initial assessment, the business took the view that PCI DSS compliance was a continued state to be maintained 24 hours a day, 7 days a week, 365 days a year, and not just once a year when the QSA is on site. This approach ensured that processes were put into place to maintain a continued level of compliance, which helped the business not only to pass all future QSA compliance assessments with ease, but to limit the business impact caused by onsite assessments to a minimum.

LESSONS LEARNED

One of the secrets of Capita’s Payment Gateway compliance success is the adoption of ISO27001 security management. All the PCI DSS requirements and related processes were incorporated into the business’s information security management system. Even though PCI DSS is a good and prescriptive information security standard, the standard does not cover all aspects of risk and information security. For instance, the PCI DSS has no focus on availability; instead the standard is predominately focused on cardholder data confidentiality and less on integrity. As a payment service provider, providing payment services relied upon by millions of cardholders, the availability of the payment system is extremely important. Therefore a raft of security controls and disaster recovery practices is in place. These are not listed as requirements within the PCI DSS standard, yet they are equally vital measures for both Capita and its many clients.

The vast majority of the requirements set out within PCI DSS are industry best practice information. The standard is very prescriptive and can be beneficial beyond the protection of cardholder data, but the advice is not to let the tail wag the dog, and ensure that the business has its own holistic approach to information security that encompasses PCI DSS requirements.

For further information, please refer to www.capita-software.co.uk/payments.

After the initial assessment, the business took the view that PCI DSS compliance was a continued state to be maintained 24 hours a day, 7 days a week, 365 days a year, and not just once a year when the QSA is on site.

The vast majority of the requirements set out within PCI DSS are industry best practice information. The standard is very prescriptive and can be beneficial beyond the protection of cardholder data, but the advice is not to let the tail wag the dog, and ensure that the business has its own holistic approach to information security that encompasses PCI DSS requirements.

Interested in speaking at the 2014 Community Meetings?

Email us at pcinewsletter@pcisecuritystandards.org to find out about opportunities!
PCI Standards and EMV Chip, A Powerful Combination

Together, PCI Standards and EMV chip provide the best protection for cardholder data across the entire transaction. The following PCI SSC resources can assist organizations planning for EMV chip adoption in their payment security efforts:

- **PCI DSS Applicability in an EMV Environment guidance** – This information supplement is a primer for understanding how PCI Standards apply in an EMV chip environment to ensure the protection of cardholder data.

- **PCI PTS approved devices** – EMV chip migration is a great opportunity to look at overall terminal security, and for merchants to invest in a terminal that meets various security standards and needs. When thinking about your terminal infrastructure for EMV chip, take advantage of the PCI PTS listing on the PCI SSC website and consider a V3 terminal. Also consider any future Point-to-Point Encryption (P2PE) plans and what additional layers of security you may want.

- **PCI DSS E-commerce Guidelines** – EMV chip provides excellent protection against fraud in a face-to-face environment. But in preparing for this migration, multi-channel organizations need to consider their entire payment infrastructure, not just brick and mortar, and specifically e-commerce environments. Put together by a dedicated Special Interest Group (SIG) of industry practitioners, this information supplement provides recommendations for applying PCI DSS to e-commerce environments.

The PCI Security Standards Council is an active member of the EMV Migration Forum (EMF). For additional information and resources on EMV chip migration in the U.S., organizations can visit the EMF website at EMV Connections.

Also, don’t miss PCI Security Standard’s Council Chief Technology Officer, Troy Leach, speaking on EMV chip and PCI at the Smart Card Alliance 2014 Payments Summit, 5-7 February in Salt Lake City, Utah. Troy is speaking on Thursday, 6 February at 3:15 p.m. – 4:15 p.m. on “After EMV: What Comes Next?” panel session.

---

No single solution addresses all security challenges. EMV is a valuable technology with embedded security features. The use of EMV, compliance with PCI standards and integration with solutions that devalue data all play an important role in a multi-layered strategy for protecting data and preventing compromise across all acceptance channels.

– Diana Greenhaw, Global Payment System Risk, Visa, Inc.

EMV chip technology is a strong tool that, when used in combination with PCI Standards and other security-related technologies, provides a layered solution for organizations that are responsible for the security of their customer’s payment data. What’s more, by deploying EMV, businesses can also establish a secure foundation to accept new payment technologies, such as contactless and mobile.

– Mike Mitchell, Vice President Global Policy Compliance & Program Management, American Express

MasterCard has been a pioneer in developing new payments technologies to create smarter and safer ways to pay. Technological advancements, such as EMV, tokenization, and end-to-end encryption, combined with the effective implementation of the PCI Standards is the best approach to enabling a safe and secure payments environment for all stakeholders.

– Bruce Rutherford, Group Head, Fraud Management Solutions of MasterCard

---

Interested in contributing to the July issue of **PCI Perspectives**?
Submit to pcinewsletter@pcisecuritystandards.org by 16 May!
As you’re probably aware, the PCI Security Standards Council published version 3.0 of its Data Security Standard (DSS) on 7 November. If your business stores, processes, or transmits payment cardholder data in a virtual environment, you will want to carefully study the new standard for updates. I’ll touch on the high points here for requirements that affect the Cardholder Data Environment (CDE).

Scoping – All virtualization technology in the CDE is in scope for a PCI DSS assessment. For purposes of an audit, the Council added: “To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE” (PCI DSS 3.0, pp. 10-11). If your implementation of the virtualized CDE does not do this, be prepared for pushback from the Qualified Security Assessor (QSA).

Network Diagram – You’ve got to know what you’re protecting before you can ensure that adequate controls are applied to a virtualized CDE. PCI DSS 1.1.2 modifies and adds a new requirement for a “current network diagram that identifies all connections between the cardholder data environment and other networks, including wireless networks.” To comply with PCI DSS, you will require an automated solution that has 24/7, 100% visibility on the virtual CDE – and can immediately produce these data in a network diagram that documents relevant connections for your security team, and for a QSA.

Data Flows Diagram – Another new requirement especially relevant for virtualized CDEs is in 1.1.3: “current network diagram that shows all cardholder data flows across systems and networks.” PCI DSS is all about the cardholder data. The key idea is similar to winning the three-cups-and-a-ball “shell game” used by con artists; you must keep your eye on the ball to see where it ends up. Likewise, you must know where cardholder data is at all times in order to protect it. The new requirement for diagramming all virtualized cardholder data flows is a means to the endgame of protecting cardholder data – and passing the PCI DSS audit. Given the dynamic nature of a virtual CDE, you will need an automated solution to fulfill this requirement.

System Components Inventory – Another significant new requirement is in 2.4: “maintain an inventory of system components that are in scope for PCI DSS.” This requirement may well make you break out into a cold sweat and lose sleep! Keeping track of physical components is hard enough, and with the dynamic nature of virtual components, complying with this requirement will be nearly impossible without an automated solution.

I encourage you to read the standards thoroughly, review your current infrastructure security, and determine how you can remain compliant (and prove compliance) in 2014. It is possible and can be relatively painless with the right systems in place.

PCI DSS Virtualization Guidelines v2.0

Virtualization separates applications, desktops, machines, networks, data and services from their physical constraints. Virtualization is an evolving concept, encompassing a broad range of technologies, tools, and methods, and can bring significant operational benefits to organizations that choose to leverage them. As with any evolving technology, however, the risks also continue to evolve and are often less understood than risks associated with more traditional technologies. The intent of this Information Supplement is to provide guidance on the use of virtualization in accordance with the Payment Card Industry Data Security Standard (PCI DSS). For the purposes of this paper, all references are made to the PCI DSS version 2.0. Click here to view.
PCI DSS and the Franchisor

LEO BOIKE, Manager, Global Compliance Reporting, Carlson Wagonlit Travel (Board of Advisor, Alternate)

To a franchisor, trying to manage PCI DSS compliance with franchised locations is like teaching your teenaged child how to drive a car while you sit in the passenger seat with a blindfold on. This, by the way, is how my father taught me to drive. The point being, if you have limited visibility and limited control – it is very difficult to get results when it comes to PCI DSS compliance.

According to the last available Economic Census Report, 2007, by the United States Census Bureau, 10.5% of US businesses surveyed were part of a franchise. According to the International Franchise Association, franchised businesses were responsible for $1.2 trillion in GDP (9.7%) in the United States. I'm willing to bet that a substantial amount of that is processed through credit cards.

Most individual franchised businesses fall under the category of small or mid-sized business (SMB). As per a research report published by Control Scan and Merchant Warehouse, November 2013, titled "Payment Security and the SMB: the fifth Annual Survey of Level 4 Merchant PCI Compliance Trends," 70% of the 615 businesses surveyed stated that they are either not familiar (31%) or only somewhat familiar (39%) with PCI DSS.

From the above, and expanded to a global view, we can conclude that individual franchised businesses worldwide are potentially at risk when it comes to having their customers' credit cards compromised. A solution is to find them additional assistance and education in order to achieve PCI DSS understanding and compliance. A good source for such assistance and education is the franchisor.

Visa published a Data Security Bulletin on 14 March 2008, titled "Payment System Security Best Practices for Franchises". In this bulletin they offer a strategy comprised of five areas of best practice and supplement them with real life situations and comments.

Adopt Secure Payment Applications

One of the points of this recommendation is that the franchisor should implement the best practice of vetting Point of Sale (POS) applications to validate that they are PA-DSS compliant. I replaced the bulletin's PAB validation with PA-DSS).

While I agree with this under the circumstances where a franchisor is requiring the franchisee to use a specific application, in many cases franchised locations are free to use any applications they choose. You may also have situations such as a hotel chain where the franchise is the hotel but the franchisee also has one or more restaurants at its location. The franchisor cannot dictate what POS goes in the restaurant in this case. But if a compromise happens — the customer associates the restaurant with the hotel chain.

Even if a POS system is vetted by the franchisor, and particularly when third-party resellers are involved on a global scale, unless the installation, configuration, and maintenance are done in a PCI DSS compliant manner – the franchisee is still vulnerable.

Enforce Network Security

As a franchisor you may not have access to the individual franchisee's network. And to limit your liability, you most likely do not want this type of access. So, beyond securing what is in...
interested in contributing to the July issue of PCI Perspectives?
Submit to pcinewsletter@pcisecuritystandards.org by 16 May!
In response to requests from the PCI Community two important new training initiatives are set to be launched in the first quarter.

In February, PCI 3.0 Insider, an affordable eLearning training course will be available online. It is a comprehensive update focusing on the intent, interpretation and implementation of the major changes in DSS v3.0. This definitive professional and technical training has been developed for professionals who need to understand and implement the important changes to the PCI DSS and PA-DSS. The course has been built by Security Innovation, a longtime eLearning provider to the Council. With an emphasis on security as the new “Business as Usual,” this course is one of the best ways to get up to speed on what the changes will mean to you and your organization.

In addition, an exciting new series of PCI Security Awareness Education courses will be rolling out in March. Designed to help satisfy Requirement 12.6 and reduce the impact of today’s threats to payment card security, we have named this series PCI Essentials: ten highly interactive, engaging online eLearning modules that can be combined to provide almost two hours of training for all levels of employee. The training is designed to be engaging, relevant and memorable, ensuring that it will have a tangible impact on information security.

These courses, developed on our behalf by Security Innovation, leverage state-of-the-art educational design techniques to deliver a best-of-breed experience for large and small organizations alike. Both the “Insider” and “Essentials” will be available directly from Security Innovation. Stay tuned for updates over the next few weeks.

**Findings from a worldwide Ponemon Study on PCI awareness and security training**

- **64%** are not sufficiently satisfied with their current training
- **66%** are currently training less than a quarter of the workforce
- **40%** of companies without a formal security training program plan to have one 60% of which will implemented in 2014
- **75%** expect to invest over $100,000 on SAE in 2014. Over a third will spend more than $500,000
- **57%** train primarily for compliance reasons
- **60%** update their training annually
- **58%** of employees are not satisfied with current training

Sample size of over 3,000 and decision makers

---

**PAYMENT SECURITY BOOKSHELF**

- We hope you enjoy these book recommendations from a Qualified Security Assessor.
- **Andy Barratt**, QSA, QSA (P2PE), ISO27001, MBCS, Managing Director, Europe, Coalfire
    (Requirement 1)
  - *Hardening Linux* by James Turnbull
    (Requirement 2)
  - *Practical Cryptography* by Niels Ferguson & Bruce Schneier
    (Requirements 3 & 4)
    (Requirement 6)
  - *Active Directory: Designing, Deploying, and Running Active Directory* by Brian Desmond, Joe Richards, Robbie Allen & Alistair G. Lowe-Norris
    (Requirements 7 & 8)
  - *Watch My Back* by Geoff Thompson
    (Requirement 9)
    (Requirement 10)
  - *Hacking Exposed Series* by various authors
    (Requirements 4 & 11)
  - *ISO2700x Series Standards List. Click here to view.*
    (Requirement 12)
PCI SIG Updates

2014 Projects

Special Interest Groups (SIG) are PCI community-led initiatives that address specific areas or security challenges in relation to the PCI Standards. This year Participating Organizations selected Security Awareness Program and Penetration Testing Guidance as the two topics to explore in 2014. Those responsible for proposing these projects share their thoughts here on why these topics are important and the benefit of participating in these groups.

2014 SIG Topic: Security Awareness Program

This SIG will work to provide guidance on how to develop formal security awareness training to satisfy PCI DSS Requirement 12.6. The SIG will develop best practices in organizational security awareness training for protecting cardholder data, develop best practices for a consistent, uniform approach to provide personnel in various roles the appropriate level of awareness training for cardholder data security, develop best practices on the type of content and depth of content an organization can use to train personnel to meet the intent of PCI DSS requirement 12.6, and develop a best practices checklist to help organizations manage their awareness training and educate their personnel on the importance of cardholder data security.

RANDY GUNDLACH, Compliance and Quality Manager, American Family Insurance

Why do you feel that this is an important topic to be addressed as a SIG?

Security awareness and PCI compliance are closely tied together. The core of successful PCI compliance is in-depth knowledge of security as it applies to systems, networks, processes, and people. Yet in the end, it is people at the center: they handle PCI data in call centers, they build the systems that process or store PCI data, they configure the networks that handle the transactions. A successful security awareness program is one that leads individuals to understand the relevance of being secure and the impacts to company and customer data.

What would you tell POs that are considering getting involved in a SIG?

We are looking for people willing to share their security training plans, scope, targeting, and metrics. We are looking for people willing to share their insight on market products and services. Do they build their own? We are looking for people willing to share insight on their successes and opportunities for improvement. It is a great networking opportunity.

GARY GLOVER, Director, Security Assessment, SecurityMetrics

Why do you feel that this is an important topic to be addressed as a SIG?

I believe there is a lot of free interpretation of PCI DSS penetration testing requirements that results in a wide range of penetration test quality (and therefore pricing). This SIG will clarify what an acceptable penetration test scope is as well as provide clear guidance on the components of an acceptable penetration test engagement and its resulting report. The hope is that this type of guidance will help level the field a bit more and ensure that merchants and service providers know what to look for when engaging a firm for PCI DSS penetration testing (internal or external).

What would you tell POs that are considering getting involved in a SIG?

I would hope that merchants and service providers who have been confused with service quote diversity or have experienced a QSA not accepting a penetration test would participate in the SIG to help provide feedback on penetration testing services. It would also be great to get participants with various types of environments (normal POS layout, web-based POS, eCommerce, large and small networks, etc.). It would be great to hear feedback from merchants on the scope of penetration testing that has been done from an internal perspective. The real goal is to improve the penetration test experience from multiple perspectives (merchant, QSA, Pen test team).

For more information about the Special Interest Groups, and to register to join a group, please visit the SIG webpage.
2013 SIG Deliverables Update

More than 200 organizations collectively have been involved in the 2013 PCI SIGs.

In this section the groups' lead contributors talk about why these projects are important to the PCI community and how Participating Organizations can use the guidance from these groups in their payment security efforts.

Maintaining PCI DSS Compliance SIG

- 273 participating individuals
- Objective is to provide guidance to merchants and service providers on best practices for long-term maintenance of PCI DSS compliance.
- Guidance slated for publication in February 2014


Why is this topic important to you?

My personal mantra – Compliance: A byproduct of good security. Having built a PCI compliance program based on good security and a continuous monitoring approach, I wanted to share my experiences as well as learn from others in my field.

What would be your advice to organizations on how to use the guidance from this group once it’s released?

1. Read it! 2. Use it! I think many will find the guidance on best practices helpful. The important message is that process-driven compliance is a sustainable approach to compliance.

What’s been the most beneficial part of participating in this SIG?

The people. Each of us has different experiences to share. The different points of view come out during the collaboration processes.

Third Party Security Assurance SIG

- 258 participating individuals
- Objective is to provide guidance to merchants, service providers, and banks on third party service provider assurance for PCI DSS Requirement 12.8
- Guidance slated for publication in the March/April 2014 timeframe

ROBERT SPIVAK, CISSP QSA & PA-QSA, Sr. Consultant, Security, Risk, & PCI Compliance, Control Gap Inc

Why is this topic important to you?

As a QSA there are many different interpretations of third-party service providers and how customers need to fulfill DSS requirements. Having guidance for customers and service providers that is consistent and comprehensive is vital to ensuring that all entities have a common understanding.

What would be your advice to organizations on how to use the guidance from this group once it’s released?

This guidance should be considered a foundation for creating or improving third-party engagement and monitoring processes and procedures to meet compliance.

What’s been the most beneficial part of participating in this SIG?

Discussing and understanding the different perspectives that each entity has when dealing with third parties. Also, getting a perspective from the Council on what their concerns are around engaging third parties and ensuring that they fit correctly into the PCI compliance puzzle.

Global demand for PCI expertise is growing

<table>
<thead>
<tr>
<th>USA/CANADA</th>
<th>LAC</th>
<th>CEMEA</th>
<th>EUROPE</th>
<th>ASIA-PACIFIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO companies</td>
<td>469</td>
<td>PO companies</td>
<td>14</td>
<td>PO companies</td>
</tr>
<tr>
<td>ISA companies</td>
<td>589</td>
<td>ISA companies</td>
<td>9</td>
<td>ISA companies</td>
</tr>
<tr>
<td>PCIP individuals</td>
<td>1073</td>
<td>PCIP individuals</td>
<td>28</td>
<td>PCIP individuals</td>
</tr>
</tbody>
</table>

USA/CANADA
- PO companies: 469
- ISA companies: 589
- PCIP individuals: 1073

LAC
- PO companies: 14
- ISA companies: 9
- PCIP individuals: 28

CEMEA
- PO companies: 22
- ISA companies: 10
- PCIP individuals: 60

EUROPE
- PO companies: 127
- ISA companies: 103
- PCIP individuals: 244

ASIA-PACIFIC
- PO companies: 45
- ISA companies: 33
- PCIP individuals: 147

* reflects data as of January 2014

Interested in contributing to the July issue of PCI Perspectives?
Submit to pcinewsletter@pcisecuritystandards.org by 16 May!
Now that the Payment Card Industry Professional (PCIP)™ program has celebrated its first birthday, it seems like a good time to look back at why the program was created and, more importantly, how it is helping improve security. We have over 1,550 PCIPs registered on the Council website and interest in the program continues to grow.

The PCIP program was developed to support the Council’s mission to enhance payment account data security by driving education and awareness of the PCI Security Standards in two ways. First, PCIP provides an entry-level credential for people involved in payment account data security to demonstrate a level of knowledge about the PCI DSS. For candidates who are relatively new to security, PCIP provides them with a broad introduction to the work of the Council with a focus on PCI DSS. Some PCIPs have significant industry experience but work in roles or organizations that aren’t eligible to join the Internal Security Assessor (ISA) or Qualified Security Assessor (QSA) programs. Typically these people move straight to taking the PCIP exam without taking the training course.

Second, PCIP provides existing ISAs and QSAs with a qualification that remains with them if they change roles or employers. We had lots of feedback from assessors that, because their status is linked to their employment, when they changed roles they were left without a credential that demonstrates their knowledge, and we see PCIP as a way to address this gap.

PCIP can help improve security within organizations by ensuring that individuals have a broad understanding of the PCI DSS. Security knowledge and awareness are crucial in ensuring that good security controls are maintained. In large organizations, PCIPs may be responsible for operating PCI DSS controls. Being PCIP qualified helps these people understand the context for those controls and how they contribute to the overall security of the organization. PCIPs may be responsible for reporting ongoing activities to an ISA who in turn liaises with a QSA. So, for example, IT staff responsible for completing daily log reviews may confirm to an ISA that those reviews really are taking place, and in turn the ISA facilitates the annual review by the QSA responsible for producing the Report on Compliance.

In smaller organizations, having a PCIP on board helps ensure that the organization understands its PCI DSS responsibilities and can facilitate more informed conversations with acquirers and brands. For organizations that service customers that need to be PCI DSS compliant, having PCIP qualified staff makes for better customer understanding and interactions when customers want to know how a product or service will affect their PCI DSS responsibilities.

PCIP training is available online to enhance global reach and to make it more convenient for individuals to complete. Companies have also expressed interest in Corporate Group Training, where our instructors provide one-day, on-site classroom style training for their staff or clients.

We are always interested in feedback on how we can improve the program. If you have thoughts on future developments, please contact the Program Manager at pcip@pcisecuritystandards.org.
Technology Update: Point-to-Point Encryption

As part of its Point-to-Point Encryption program, at the end of last year the PCI Council announced the availability of the Validated Point-to-Point Encryption (P2PE) solutions listing on the PCI SSC website.

This is the official PCI SSC resource for merchants and acquirers looking to deploy a P2PE solution to help simplify their PCI DSS compliance programs by removing clear-text cardholder data from the payment environment. Merchants can use this resource in coordinating with their acquirer or payment brand to select a solution that meets PCI requirements for PCI DSS scope reduction.

Congratulations to European Payment Services (EPS) and The Logic Group for being the first to have their solutions listed. In this section, hear from them on why they think point-to-point encryption technology is a strong tool for your payment security portfolio. Here are a few of their thoughts:

On benefits to merchants...

The merchant can be happy that its customer’s payment details are transmitted securely from a PED originated transaction, without having to validate, add or manage new security devices within their network.

– ROBIN ADAMS, Director of Technical Strategy & Architecture, The Logic Group

Whether you are a small or large merchant, P2PE solution service providers take the responsibility of compliance from the merchant to the service provider: it’s “all-in;” all the merchant needs to do is to complete the QSA form and follow the P2PE Instruction Manual (PIM).

– DELIA PEDERSOLI, International Sales Director, EPS

On getting a P2PE solution PCI validated...

I would recommend that anyone planning to submit such a solution work closely with a good pragmatic P2PE QSA in advance of submission and invest in a thorough gap analysis at some point early in the project. No matter how good your team, having an independent view about your approach and assumptions is invaluable.

– ROBIN ADAMS, Director of Technical Strategy & Architecture, The Logic Group

P2PE is a combination of hardware component and process. The journey to achieve P2PE is a longterm plan that involves all the stakeholders in the value chain of the payment solution. Before adventuring into the journey of the certification process, make sure you have all the “ingredients in place” for all six domains.

– DELIA PEDERSOLI, International Sales Director, EPS

On how P2PE can help address payment security challenges...

Many merchants we deal with have expressed an interest in a P2PE solution validated by the Council. The reasons for this are clear: merchants want to spend their time enhancing their products and services; providing a secure infrastructure, they understand, is a fundamental requirement on them but one that they wish to achieve as simply and easily as possible. Being able to take a validated solution that reduces the scope of a PCI DSS audit and significantly reduces the Business As Usual (BAU) activities required to maintain security is a real value-add for them.

– ROBIN ADAMS, Director of Technical Strategy & Architecture, The Logic Group

The challenge I see in organizations to implement a P2PE Solution with a certified service provider is overcoming fear. Fear of changing the current process (it works now, why change?), fear of “what if...,” and the most common thinking is that the current system is so complex that none can replace the years of bespoken development. After all, there are only a few on the list. The more validated solutions are available, the more organizations will make the step forward.

– DELIA PEDERSOLI, International Sales Director, EPS

Interested in contributing to the July issue of PCI Perspectives? Submit to pcinewsletter@pcisecuritystandards.org by 16 May!
PCI SSC Obtains ISO 9001:2008 Registration

We did it! On 13 November, 2013, the PCI Council’s programs completed and passed an ISO 9001:2008 external audit by American Standards Registrar, ASR. We received our Certificate of Registration in early January.

The ISO 9001:2008 standard is an international standard related to quality management systems. Organizations must demonstrate an ability to consistently provide product that meets both customer and applicable statutory and regulatory requirements. The standard is based on eight quality management principles that are fundamentally good business practice. These principles include:

1. customer focus  
2. leadership  
3. involvement of people  
4. process approach  
5. system approach to management  
6. continual improvement  
7. fact based decision-making  
8. mutually beneficial supplier relationships.

There are many benefits for implementing the ISO 9001:2008 standard but our main goal was to improve the efficiency and effectiveness of our programs operations.

As a result of this process we have implemented new procedures, designed new processes and worked on improvements that will help us increase customer satisfaction. As we move forward with maturing our processes, we will continue to pull together, strengthening our teams and looking for new ways to improve the service that we provide to our stakeholders and the industry as a whole.

PCI People on the Move

- Vasu Nagendra has moved on after seven and a half years at RSA (including two partial terms as alternate for the BoA) to become CEO of Termtegrity, a Chicago-based startup providing skimming detection solutions to help merchants protect their point-of-sale environments. The company launched its first product, SpotSkim, at the North American Community Meeting this past September. He looks forward to connecting with community members at vasu@termtegrity.com.
- Kathy Orner of Carlson Company assumes additional responsibilities with her promotion to the Global Chief Information Security Officer position with Carlson Wagonlit Travel. This new role expands upon Ms. Orner’s information security accountabilities to include physical security, IT compliance and IT audit, all on a global basis. The core security team reporting to Ms. Orner now includes employees in the United States, Singapore, Manila, Paris, London and Brazil. Carlson Wagonlit Travel is a private company owned by Carlson and JPMorgan Chase. Ms. Orner is a 2013-2015 member of the PCI SSC Board of Advisors. She can be reached at korner@carlsonwagonlit.com.
- Martha Rhine has joined EVO Payments International as Vice President of Worldwide Compliance, responsible for merchant compliance with payment network rules, standards, and regulations impacting its acquiring business. She was most recently with Global Payments for sixteen years, where she was responsible for merchant, agent, and processor compliance on a worldwide basis.
- Angelo Valletta is now the US–Chief Information Officer for EVO Payments International and is responsible for the expanding Information Technology groups based in the United States. Mr. Valletta has held various senior leadership positions for global fortune 500 companies, and most recently was SVP/CIO and Head of Bank Operations for Sun National Bank.
- Jen Mack is joining Virtual as Senior Vice President, Client Services. She will provide management and vision to ensure that Virtual clients, with special focus on the PCI Security Standards Council and Cyber Security clients, effectively deliver on their missions. Prior to Virtual, she ran her own security consultancy, she also served as Managing Director, Global PCI Consulting at Verizon Business; and Vice President, Fraud Management Solutions at MasterCard.

Here are some recent promotions at the Council we’d like you to be aware of:

- Brandy Cumberland has been promoted to AQM Director. Brandy has been with the Council since July 2011 and has served as QA Analyst, AQM Manager and interim AQM Programs Director.
- Jeremy King has been promoted to International Director. Jeremy will now be responsible for building PCI awareness and adoption not only in Europe, but also in Africa, Middle East & Asia Pacific regions.
- Ella Nevill has been promoted to VP Global Stakeholder Engagement. As the Council continues to expand its global reach, Ella will now be responsible for communicating to current POs and continuing to grow participation and involvement with the Council around the world.
- Mauro Nunez has been promoted to Chief Operating Officer and is now responsible for the day to day operations of the Council. Mauro was the driving force behind the Council operations becoming ISO compliant.
- Alicia Marshall has been promoted to AQM Manager. Alicia joined the Council in March 2012 as AQM Analyst and quickly proved to be a dedicated, effective leader and analyst.

Interested in contributing to the July issue of PCI Perspectives?
Submit to pcinewsletter@pcisecuritystandards.org by 16 May!
Interested in contributing to the July issue of PCI Perspectives?
Submit to pcinewsletter@pcisecuritystandards.org by 16 May!

New Participating Organization Spotlight

**Arçelik A.Ş.**
Arçelik A.Ş. was founded in 1955 and is headquartered in Istanbul, Turkey. Operating in the durable consumer goods industry with production, marketing and after-sales services, Arçelik A.Ş. offers products and services worldwide. With 23,000 employees, 14 different production facilities in five countries, sales and marketing companies all over the world and 10 brands, Arçelik A.Ş. is the first and biggest Electronic Cash Register manufacturer in Turkey. Arçelik A.Ş became a PCI SSC Participating Organization to be made aware of the latest technologies and opportunities in the field and also to have the chance to meet future customers and partners.

**DB Networks**
DB Networks is excited to be a PCI SSC Participating Organization. DB Networks is innovating behavioral analysis technology in the field of database security, focusing on organizations that need to protect information from advanced database attacks, including zero-day attacks. DB Networks’ database security solutions provide the ability to detect advanced SQL injection attacks. DB Networks’ unique approach operates in the core of the network and uses behavioral analysis technology to automatically learn each application’s proper SQL statement behavior. Any SQL statement dispatched from the application that deviates from the established behavioral model immediately raises an alarm as an attack.

**Evident.io**
Evident.io is a “cloud first” security company, focused on security challenges arising from the adoption and use of programmatic infrastructure at all levels of scale. The Evident.io Security-as-a-Service platform provides businesses with continuous analysis of the resource security mechanisms distributed across their programmatic infrastructure. We believe the future of infrastructure security is Evident, which is why we jumped at the opportunity to be part of PCI SSC. We can bring our unique perspective on the challenges facing cloud companies in achieving PCI compliance, while engaging the PCI SSC community and encouraging new solutions to be built in response to customer need.
**HighRadius Corporation**

HighRadius Payments OnDemand is a robust PCI DSS compliant electronic payments solution for SAP® applications that enables merchants to accept credit cards and other payment types electronically with full integration into their SAP® systems. This cloud-based solution is available as Software-as-a-Service and leverages modern technologies and processor tokenization services to maximize credit card security. HighRadius is a participant in PCI SSC because it strongly believes in securely protecting cardholder and merchant information.

**Integrity Payment Systems**

Integrity Payment Systems is a national credit card processor located in the Chicagoland area. Integrity helps business owners offer their customers a full range of payment options while keeping the cost of credit card processing low. The company also offers a growing suite of business solutions that can help business owners establish cash reserves for an emergency fund, more quickly eliminate debt, build their retirement funds, and accelerate cash flow, all while enjoying smoother day-to-day operations and better customer service. Integrity Payment Systems also understands the importance of maintaining PCI DSS compliance and implementing solid security practices throughout the entire payment chain. Collaborating with other Participating Organizations, obtaining the latest educational materials, and ongoing communication with the company’s merchant base are all key steps towards accomplishing these goals.

**Seamark International**

Seamark International is the leading supplier of ergonomic, space saving and durable Spacepole® mounts for information technology products. Seamark International understands the various issues, challenges, and concerns facing the integration of new security technology devices. The company’s products and systems are designed to improve productivity, maximize space utilization, increase security and enhance the customer experience. Seamark International is proud to be a PCI SSC Participating Organization, seeing this as a great opportunity to be an influential participant in increasing awareness of security standards on a global level. Seamark International is a company that is passionate about customer success in line with best practices, currently offering a variety of products focusing on the security of the device against theft. With combined resources and efforts, joining PCI SSC will enable Seamark International to better serve its customers and offer the finest solutions in line with standards.