PCI Perspectives

JULY 2014

IN THIS ISSUE

Welcome!

Dear Participating Organization,

Welcome to *PCI Perspectives* – the newsletter written by you and for you.

The Council, and I'm sure many of your organizations, had a busy first half of the year. Data breach incidents left many in government here in the U.S. asking what the industry is doing to reduce the risk of payment data compromise.

The Council was invited to participate in several U.S. Congressional hearings to address this topic. The goal was to demonstrate that the PCI Standards remain a critical component of any layered security strategy. PCI Standards are so valuable because they are developed with the input of the community and those that actually face the challenges of protecting payment card data on a daily basis.

Looking ahead to our three Community Meetings, our theme for this year's events is "securing payments together". There are a number of ways you can be involved in protecting and enhancing the value of PCI Standards as a Participating Organization. Here are some ways you can contribute:

- Share your implementation experiences during Q&A sessions, open forums and office hours
- Help each other by networking with your industry peers and using the mobile app, social media and our 'birds of a feather' opportunities to share your successes and challenges and help raise the bar for payment security across the industry
- Propose, vote for and participate in a Special Interest Group for a PCI topic you think is important the industry tackle together
- Find out more about nominating your organization for the 2015 Board of Advisors and provide your expertise and feedback on some of the most pressing issues we face in payment security

If you are new to the Council, I hope you will consider the many opportunities that membership offers to you. If you are a veteran Participating Organization, thank you. Please consider how to share the benefits of your expertise with the SSC and your peers.

As always, if you have any suggestions for *PCI Perspectives* content, please contact me.

Sincerely,
ELLA NEVILL
Vice President of Global Stakeholder Engagement • enevill@pcisecuritystandards.org

PCI SSC Welcomes New General Manager, Stephen Orfei

LIB DE VEYRA, Vice President, Emerging Technologies, JCB International and Chairperson, PCI Security Standards Council

We are excited to welcome Stephen Orfei to the role of PCI SSC General Manager, starting in September of this year. As you know, Bob Russo, who has led the Council in building a strong and diverse membership of payment security leaders around the world over the past 8 years, will retire as General Manager at the end of 2014.

We are pleased to be able to bring someone with Steve's level of payment industry knowledge and technology expertise to this leadership role at the Council. With his background in innovative technology, product development and management and partnership building, he represents an exciting move forward for the Council as we focus on delivering standards, solutions and services to secure the future of payments. His diverse experience means he sees the opportunities and challenges of our community from a number of perspectives. We look forward to his start in September and encourage you to attend the annual Community Meetings to have the opportunity to meet and talk with him in person.

Stephen Orfei

Reflections from the Board of Advisors

ED RITTER, Senior Vice President, Information Security Policy and Governance Executive, Bank of America North America

Most challenges and issues are best resolved by individuals willing to share ideas, collaborate on solutions and take action. In April, Bank of America was proud to host the first Acquirer Forum. More than 30 professionals gathered to share experiences, ideas and approaches to improving the quality of the QSA program and increasing security awareness of small merchants. The discussions covered a wide range of topics from tokenization and point-to-point encryption to discussions on the quality of training programs and the potential to integrate PCI content into acquirer 'on boarding' programs. These ideas will be incorporated into existing work efforts and may launch new ones in the near future. However, as often is the case, I was reminded how small and simple things can make a big difference. I'd like to share three simple actions each of our readers can take which will collectively make a positive impact in the broader PCI community:

1. Take five minutes to provide feedback on a QSA and/or a recent assessment experience via the PCI website
2. In every professional and personal conversation with a small merchant, remind them to reset passwords frequently and certainly to ensure default passwords have been changed
3. Acquirers should remind small merchants to use qualified professionals to install software and equipment; an available option is the QIR program

Protection of card holder data continues to be our collective challenge. To meet that challenge, let's continue the dialogue and working together to provide solutions. Most importantly, let's remember to take simple actions every day which can make an immediate difference.

CHRISTIAN JANOFF, Enterprise Architect, Cisco

The Payment Card Industry (PCI) has come a long way. The journey has had a lot of twists and turns, but, there has been tremendous global progress, learning how to work together to defend ourselves against the baddies. Whether you are a merchant, a bank, a vendor, or even a hacker, there is no denying that the culture has changed.

I joined the PCI Council in 2007 representing Cisco. Back then, the Council meetings were much different. The formation of the standard and the first blush interpretations gave way to some vigorous debate. Vigorous, in the sense, that either a punch or a pie was about to be thrown at any moment. In those days, the assessors were less uniform and seemed to be wearing either a badge and a gun or a red nose and floppy shoes. I remember the Council meeting in Brussels in 2008 where someone brought up the fact that one assessor recommended building a 50 foot wall complete with barbed wire around a merchant's data center as a method of physical protection!

What a change. From yesteryear to today, I have seen people's attitudes evolve, along with the companies that they work for. Some of the companies that I spoke to in 2007 told me that they would never comply with PCI. Then the TJ Maxx breach occurred and suddenly they were saying, "What was the solution that Cisco created around PCI?" Companies that used to view compliance as unnecessary investment are now hiring network engineers with compliance titles. Clearly, the new threats of today have affected how the globe views compliance and security.

CONTINUED ON NEXT PAGE

UPCOMING EVENTS

RetailNOW!
Orlando, Florida • 3 August – 6 August

MasterCard Global Risk Management Conference
Kuala Lumpur, Malaysia • 5 August – 8 August

PCI SSC North American Community Meeting
Orlando, Florida • 9 September –11 September

MasterCard Global Risk Management Conference
Dublin, Ireland • 29 September – 2 October

PCI SSC European Community Meeting
Berlin, Germany • 7 October –9 October

PCI SSC Asia-Pacific Community Meeting
Sydney, Australia • 18 November –19 November

Announcing New eLearning Course

Insider's Guide to PCI DSS 3.0

PCI DSS 3.0 is here and there are only a few short months remaining before it will need to be fully implemented.

Are you up to speed? You can be, in just 90 minutes. Take this affordable eLearning course today – offered through Security Innovation.

As the hackers continued to develop new attacks, the PCI Standard has matured to respond to them. Today, the Council meetings are much different from those early days. I am always impressed with the amount of participation. It is exciting to see how many people travel from all over the globe, forming a federation that we all benefit from. New PCI programs and expanding reach demonstrate how mature we have become. The PCI Standard provides a method of securing credit card data that no one government mandate or regulation can equal.

The future will certainly be fraught with new challenges as the thieves escalate. I am confident that the PCI Council is the best place to address how we can all help each other to become more secure and learn best practices. Over the course of these years, I have had the privilege of serving on the Board of Advisors. I have been elected by all of you three terms in a row and have reached my term limit. I have tried my best to represent the industry, you all, my company, and myself, with much vigor and participation as possible. Thank you very much for the opportunity and I look forward to speaking with you at the coming Community Meetings.

SAVE 10% on PCIP eLearning course

Help us reach 2000 PCI Professionals. Enroll on or before 15 August and use promo code: **2000PCIP** to get the discounted rate.

Have You Registered Yet? You Don't Want to Miss the PCI SSC Community Meetings this Year

NORTH AMERICA

9 September –11 September
Orlando, Florida

REGISTER HERE

EUROPE

7 October – 9 October
Berlin, Germany

REGISTER HERE

ASIA-PACIFIC

18 November –19 November
Sydney, Australia

REGISTER HERE

Interested in contributing to the January 2015 issue of ***PCI Perspectives***?
Submit to pcinewsletter@pcisecuritystandards.org by 4 December 2014!

Special Interest Group (SIG) Benefits

What's been your favorite part about being involved in a PCI SIG?

The best part of being involved with a PCI SIG is the opportunity to materially contribute to the guidance papers that help clarify the standards and the intent behind them. You have a voice! A secondary benefit is the ability to work with and learn from peers from all slices of the payments industry, which helps broaden your view and understanding.

Pete Campbell
Company: Board of Trustees of the University of Arkansas
Job title: Director of Payment Tech/ Compliance
SIG: Penetration Testing Guidance

I have always really enjoyed the opportunity to interact with other facets of the PCI world outside of our QSA view. Working with a group can be challenging, especially for writing, but it is fun to see the discussions eventually coalesce into a pertinent document to provide guidance to the community as a whole.

Gary Glover
Company: Security Metrics
Job title: Director, Security Assessments
SIG: Penetration Testing Guidance

My favorite part of being involved in the PCI Penetration Testing Guidance SIG has been the opportunity to work with cutting-edge penetration testing professionals in developing and clarifying the penetration testing requirements to make sure any company, big or small, can unambiguously perform the necessary penetration testing activities to secure their online business and payments.

Kim Halavakoski
Company: Crosskey Banking Solutions
Job title: CSO
SIG: Penetration Testing Guidance

Participation in the SIG has given me a much better understanding and appreciation for the work that went into the formation of the Standard. When you have the opportunity to work with a wider variety of Merchants and Service Providers, you realize how difficult it is to create guidance that is appropriate and effective for most situations.

Joseph Pierini
Company: PSC
Job title: Director of Technical Services
SIG: Penetration Testing Guidance

My favorite part was the meetings with all the groups, getting their input and ideas, and listening to their presentations. This was my first experience in a SIG group, and I have learned how important it is to be involved in the PCI DSS SIG groups and get opinions from people in the industry, from many different entities in many different regions. I will definitely join SIG groups in the future.

Dale Flahive
Company: Elavon, Inc.
Job title: Sr. Director, Large Merchant PCI Compliance
SIG: Security Awareness Program

I've enjoyed working with other industry representatives, which has helped me to appreciate that PCI DSS isn't only taken seriously by the big merchants and banks like my own.

Jim Roberts
Company: Clydesdale Bank
Job title: Information Risk Consultant
SIG: Penetration Testing Guidance and Security Awareness Program

2015 SIG Timeline

- **SIG Election** 13–23 October 2014
- **2015 SIG Winners Announced** 6 November 2014
- **2015 SIG Registration Opens** 8 December 2014
- **2015 SIG Kick-off** January 2015

Interested in contributing to the January 2015 issue of ***PCI Perspectives***?
Submit to pcinewsletter@pcisecuritystandards.org by 4 December 2014!

Global Security Insights: The Journey to Cashless Payments, A Middle East and North Africa Regional Update

IZDEHAR SAFARINI,
Deputy CEO –Technical and Operation, Middle East Payment Services (MEPS), PCI SSC Board of Advisor

Some countries in the Middle East and North Africa (MENA) region are shifting from cash to cashless at a rapid pace. This is driven largely by government mandates, leadership and initiatives that provide focus and momentum for the cashless journey to overcome macroeconomic, structural and cultural barriers to promote electronic payments. A combination of payments system innovations, increasingly sophisticated non-cash products, education of consumers, regional expansion, and improved service and offerings by domestic banks is also contributing to this momentum around cashless payments.

Many markets in the region have made real progress on their journeys by establishing basic infrastructure. Affordable and broadly available financial products, a vibrant and competitive merchant market place, a transparent and productive business environment—all of these basics are strongly correlated with progress in the cashless journey.

Volume growth in global non-cash payments transactions accelerated during 2011, while volume growth in non-cash payments transactions in the Middle East also accelerated during 2011, growing more than 21.9 %. The non-cash payments were estimated to continue their growth in most markets in the region primarily as a result of consumers moving away from cash. Initial estimates suggest the number of non-cash transactions will grow by 25.5% in the CEMEA region (*World Payment Report 2013/ Capgemini*).

It is worthwhile mentioning that the Middle East payments market is fragmented and diverse. Currencies, regulatory frameworks and governance, infrastructure, economic situations, and use of non-cash instruments are specific to each market. The region includes both the oil-rich economies in the Gulf and countries that are resource-scarce in relation to population, such as Egypt, Morocco, and Yemen. This reflects on the penetration rate and advancement in this area.

Many Arab countries are undertaking payment system reforms, often supported by the Arab Payment Initiative (World Bank, Arab Monetary Fund, IMF). Countries including Jordan, United Arab Emirates, Bahrain, Saudi Arabia and others are working to improve the legal framework, payment system oversight, transparent governance and proactive policies such as the mandatory requirements of many central banks in the region around PCI DSS compliance and EMV card adoption to ensure a high level of security, customer confidence and to minimize fraud.

Payment cards are the basis for innovation and growth in non-cash payments (as they are elsewhere in the world). A number of card-based developments have taken place in the region during the past year.

Egypt came in first place in number of cards, with 18.3 million cards followed by Saudi Arabia with 15 million cards; Morocco with 10.2 million cards; UAE with 8.8 million cards; Kuwait with 6.3 million cards; and the lowest number of cards was in Syria, Palestine, Libya and Mauritania with card numbers of 340k, 310k, 30k and 10k and it was mainly ATM cards. (*Unified Arab Economic report 2011)*.

The number of ATM transactions in 2011, in Saudi Arabia exceeded 1.25 billion transactions, with a growth recorded 18%, from 2010, boosted mainly by a sharp increase in the use of cards and credit transfers.

CONTINUED ON NEXT PAGE

TRAINING AT THE EUROPEAN COMMUNITY MEETING

Lack of education and awareness is a lead contributor to data breaches.

Don't miss these educational opportunities before the Community Meeting in Berlin:

- **2–4 October:** P2PE New/Requalification
- **3–4 October:** QSA
- **5–6 October:** PA-QSA
- **5–6 October:** ISA

> *"Security measures and PCI DSS compliance is highly appreciated and pursued to meet the mandatory regulatory requirements and to ensure customer confidence and acceptance."*

In Kuwait, the volume of card transactions for the first 6 months of 2013 reached 8 billion KWD, (~ 30 billion USD), as per central bank of Kuwait published statistics, noting that there are 1200 ATM and 33,000 POS in Kuwait to serve the population of 3.5 million.

The e-commerce transactions are expected to reach an estimated $15 billion by 2015, up from $9 billion in 2012.

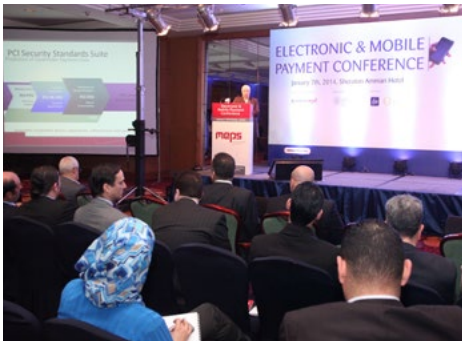
The mobile payment user base in the region is expected to rise from $53.3 million in 2009 to $154.3 million by 2015. The value of m-commerce could reach up to $4.9 billion by 2015.

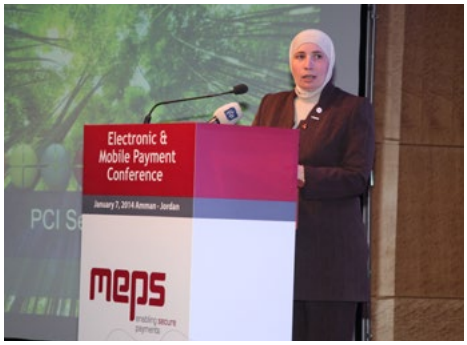
56% of consumers expressed concerns regarding payment cards fraud. This is the main barrier to e-commerce, and the offering of cash on delivery services for most e-commerce sites in the region. Cash on delivery is 70% of e-commerce volume in the Middle East.

Security measures and PCI DSS compliance is highly appreciated and pursued to meet the mandatory regulatory requirements and to ensure customer confidence and acceptance. Many conferences are held every year in the region to promote e-commerce, e-payments and card usage, PCI DSS awareness and training.

The high number of running PCI DSS compliance projects and the need for ongoing PCI DSS compliance, created the demand for qualified and certified PCI DSS local expertise, as currently, this is mostly fulfilled by foreign vendors and consultants. Local companies are investing to build the needed local capacity and awareness.

Photos from the Electronic & Mobile Payment Conference – January 2014





TRAINING AT THE ASIA-PACIFIC COMMUNITY MEETING

Did you know that one of the leading causes of data breaches in Asia Pacific is employee negligence?

Organizations need to focus on processes, policies and technologies that address threats from the negligent employee and the malicious insider or hacker. (*Ponemon Institute, March 2012*)

Take a PCI training class before or after the Community Meeting:

- **13–14 November:** ISA
- **15–16 November:** QSA
- **17 November:** PCI Awareness
- **20–21 November:** PA-QSA

Global demand for PCI expertise is growing

USA/CANADA	
PO companies	478
ISA companies	624
PCIP individuals	1198

EUROPE	
PO companies	131
ISA companies	108
PCIP individuals	299

ASIA-PACIFIC	
PO companies	44
ISA companies	37
PCIP individuals	167

LAC	
PO companies	16
ISA companies	6
PCIP individuals	30

CEMEA	
PO companies	20
ISA companies	35
PCIP individuals	74

* reflects data as of June 2014

Interested in contributing to the January 2015 issue of ***PCI Perspectives***?
Submit to pcinewsletter@pcisecuritystandards.org by 4 December 2014!

Global Payment Landscape: Expanding PCI Awareness in Asia-Pacific

The Asia-Pacific (APAC) market is an exciting and fast-moving market where new technology is always at the forefront, especially in the payments space. Building on the success of last year's inaugural Community Meeting in Kuala Lumpur and working with the PCI community in the region, we've had a number of opportunities in 2014 to continue growing relationships and awareness with visits to China, Hong Kong, Singapore and Japan.

JEREMY KING, International Director, PCI Security Standards Council

China

PCI Qualified Security Assessor (QSA) Atsec Information Security Company hosted us at their security conference, along with Visa and The Payments and Clearing Association of China. It was very positive to see not only the level of attendance, but also the level of knowledge and interest in the PCI Standards.

The conference benefited from having real-time translators along with translated slides which really helped the attendees get the most out of the program.

It was clear from listening to the discussions and questions that many of the challenges and concerns that exist in Europe and the U.S. also exist in China and the rest of the Asia-Pacific region. Securing internet payments and the migration toward mobile commerce were just two of the hot topics. Fortunately the Council has excellent guidance documents that provide detailed and helpful resources for both of these topics. There is support for merchants, vendors and acquirers, and in addition, PCI DSS v3.0 updates focus on improving security for e-commerce merchants as well as third-party providers.

Hong Kong

We also had the opportunity to present at Cartes Asia in Hong Kong. Cartes Asia is an exhibition and conference focused on the payments industry. It was encouraging to see much increased participation in our session over last year when we spoke at this same event, reflecting the growing awareness and understanding in the region of the importance of PCI Security Standards in securing payments.

As in China, the key topics of interest were e-commerce and m-commerce, as well as the release of the new standards and the key changes that were made to them.

Singapore

PCI SSC Chief Technology Officer Troy Leach visited Singapore in May, a region we've continued to build relationships in following our inaugural PCI SSC Town Hall Meeting there in 2012. He provided the latest updates on PCI Standards at Visa's Security Summit.

Join us at the 2014 APAC Community Meeting

Improving cardholder security whilst enabling new technology is critical for merchants globally, and the best way of achieving this is to be actively involved within the PCI community. Our Special Interest Groups look at the topics important to the community as the topics are submitted, elected and supported by our community.

Our Community Meeting also offers a fantastic opportunity to learn from the leading industry experts, and to have face-to-face discussions with PCI SSC staff and the global brands. This year's Community Meeting in Sydney will be bigger and better, with a much larger and wide-ranging agenda. In fact, it really is a must-attend for those working in payments security in the region.

PCI in Practice: Positive Security – Merging Security and Compliance in the Retail Environment

INTRODUCTION

In my role, I have helped many companies realize the benefit of Bit9's approach to merging security and compliance via the trust policy. Implementing that paradigm is key to positive security, and has multiple advantages and benefits for any company that needs to ensure that they are secure from threats and in continuous compliance. By phasing in a security policy based on trust, I have helped a multitude of companies change the way they protect their enterprise, while also giving them valuable real time insight into their compliance risk, particularly for PCI DSS. These positive security benefits are often of most interest to the retail industry. Retail companies have specific challenges when it comes to keeping their endpoints secure and within full compliance with PCI DSS.

CHALLENGE

Common challenges within the retail sector are of particular interest to Bit9's Compliance practice, as retailers face multiple barriers when it comes to security and PCI DSS compliance. The retail industry also tends to be widely distributed and geographically diverse. For years now it has also been the most highly targeted industry when it comes to advanced attacks. To compound the problem, many of these retail systems tend to consist of aging operating system software and applications that can't necessarily be updated overnight. The proliferation of Windows XP within retail systems is a good example of this type of issue, and one that represents problems for both security and also for PCI DSS compliance, (Requirement 6.2 – installing applicable vendor-supplied security patches). With the Bit9 Positive Security Solution, I have been able to offer a viable solution and solve these problems on numerous occasions. In one such case, the merchant, a large retailer across North America, was in need of a solution to address multiple security and compliance issues. They needed to reduce the administrative and performance strain on their POS endpoints, find a way to protect their unsupported endpoints that were still required to run Windows XP, and introduce active monitoring and control to reduce the amount of data logs that they were manually analyzing on a daily basis, in order to meet their FIM requirement (PCI requirement 11.5).

APPROACH

The approach for this client was straightforward and involved implementing Bit9's positive security model though a trust policy into the retailer's environment for three specific use cases. The first step was to solve the performance and administrative burden that was hampering the customer's ability to ensure security and also report and track their PCI DSS in-scope endpoints. Bit9 was first introduced in a lower level of enforcement, while they utilized and started the phase out of their existing security solution. This gave the company time to adjust and fine-tune their trust policy, which was mirrored against their standard business process for the POS endpoints. The introduction of the trust policy also gave the retailer immediate real time visibility of threat intelligence and measure on their POS environment that they had never had previously. The ability to avoid having to constantly scan their POS endpoints to collect data on their security and compliance risk was a huge benefit to an already overburdened system. This added a whole new level of security coverage and risk measure that the company had never experienced before. The addition of the Bit9 positive security solution to their POS endpoints provided real time threat and trust rankings that immediately enabled them to speed up their PCI assessment pre-compliance data gathering.

CONTINUED ON NEXT PAGE

Name: Christopher Strand

Title: Sr. Director of Compliance, Bit9

Contact: cstrand@bit9.com

For the past three years Christopher Strand has served as the Director of Compliance Programs at Bit9. With over 20 years of information technology experience, Strand is the subject matter expert on Bit9's IT Governance, Audit, and Compliance programs. He oversees the development of enterprise network and application security solutions that help organizations deploy positive security to maintain and improve their compliance posture.

Previously, Strand held security/compliance positions at Trustwave, Tripwire, EMC/RSA and Compuware. Strand is a PCI Professional (PCIP) and has completed QSA training. He has been trained on and is proficient with other regulatory disciplines including HIPAA, North American Electrical Reliability Corporation (NERC) and Gramm-Leach-Bliley Act (GLBA).

Chris often speaks on security and compliance issues and best practices on webinars and is a keynote speaker at many industry conferences and seminars. He has also authored several white papers and has published articles in various security trade journals.

In his spare time, when he is not immersed in security and compliance, Strand is an avid musician, giving in to his rock star alter ego, playing drums with North America's premier Rush tribute band, YYZ.

Once the trust policy was defined, we moved the retailer's POS endpoints into high enforcement mode where we had the ability to enforce control within the environment and stop unauthorized processes and executions. Particular attention was paid to their existing unsupported XP systems. For these systems we had to address the problem of locking the endpoints down and ensuring security through a compensating control for PCI requirement 6.2. We took examples of the retailer's standard business processes and business as usual activities, as prescribed by the new version of PCI DSS 3.0. This allowed us to tune a unique trust policy against the critical functions of the XP systems and stop any other unauthorized process from running on the systems. The trust policy allowed the retailer to encapsulate the critical functions on the XP endpoints, and ensure they had adequate control proof that these systems were completely protected. They also had additional focused monitoring and auditing intelligence in order to meet PCI DSS compliance, but also protect and secure the vulnerable XP endpoints from the litany of possibly attacks.

Lastly, we applied a file integrity template to the retail POS infrastructure in order to save them from manually reviewing the huge number of log files that they were tasked with monitoring. They were constantly analyzing log events for compelling events and unauthorized change in order to meet PCI requirement 11.5. The introduction of the trust policy in high enforcement had a great benefit for their file integrity requirement in that it automatically introduced control to their POS endpoints and allowed them to focus on the data that was associated with the critical business process of the systems. The high enforcement trust policy would stop unauthorized change, which immediately reduced the number of events that their administrative security staff had to review. With the addition of the file control template rules, they were able to quickly focus in on the file sets that they were required to collect data on to meet their PCI requirement and ensure focused reporting and analysis of concern areas on their systems.

LESSONS LEARNED

As it is in all cases where we have helped clients embrace the benefits of positive security through a trust policy, it is still very apparent that the work towards getting systems aligned with security and ensuring complete coverage of PCI DSS still tends to be two separate ventures. Regardless if it is retailers trying to find safety and compliance for their overburdened endpoints, finance trying to ensure the integrity and validity of their critical credit card data, or healthcare trying to protect and apply risk measure against their systems, there always seems to be duplication of effort between disparate teams. At the end of the day they both need to achieve the same goals. One thing is clear in all the cases we've dealt with and all verticals we work within, and that's the sensitive data that all of these types of organizations are trying to harness and control is always at risk of being compromised. Regardless of how these companies attempt to merge their security programs with their PCI DSS compliance objectives, the need to ensure that they situate their endpoints in a proactive state of measure, as prescribed in one of the major themes of the PCI DSS version 3.0, is of critical importance. Aligning better with the newest version of the Data Security Standard has helped many organizations understand the need for a new security approach when they go about protecting their critical data. The introduction of control and proactive measure to the PCI DSS is a good step in aligning and recognizing both the need to converge security and compliance metrics. We have found that it has had a positive effect by encouraging organizations to look at PCI compliance from a different angle and consider solutions that can provide the level of real time proactive intelligence that ensures they are able to achieve their goals of real continuous PCI security compliance.

"One thing is clear in all the cases we've dealt with and all verticals we work within, and that's the sensitive data that all of these types of organizations are trying to harness and control is always at risk of being compromised. Regardless of how these companies attempt to merge their security programs with their PCI DSS compliance objectives, the need to ensure that they situate their endpoints in a proactive state of measure, as prescribed in one of the major themes of the PCI DSS version 3.0, is of critical importance."

Web Payments – World Wide Web Consortium

STÉPHANE BOYERA,
W3C Staff

Payment is an essential element of trade and commerce, and the explosion of e-commerce in the last two decades has led to sales on the web topping $1 trillion in 2012. However, behind these impressive numbers, the payment landscape is quickly changing, and new challenges are appearing. For instance, the average shopping cart abandonment rate is 72% across all devices, and 97% on mobile. A variety of factors are limiting the potential of e-commerce, from the high level fraud related to credit card payments (Target's cautionary tale), to the fragmentation of payment solutions available on the web but not available on all merchant sites or on all devices.

Wherever there is fragmentation on the web, the World Wide Web Consortium (W3C) seeks to bring stakeholders together to develop open standards. For greater interoperability in the area of payments, W3C's vision is to enable:

- Users to choose their preferred payment solutions across all their devices,
- Merchants to transparently support a growing number of payment solutions,
- Developers to monetize applications more easily,
- New payment solution providers to enter the market more easily with innovative solutions and payment schemes,
- Society to decrease online fraud.

To understand how we might realize this vision, W3C organized in March 2014 a Web Payments Workshop in Paris, France. During this event, more than 100 people from the banking industry, payment service providers, virtual currencies providers, financial institutions, mobile industry, browser vendors, payment regulators, and payment standardization bodies discussed web payment use cases, business requirements, and standardization priorities. Participants recorded key outputs from the meeting, including a recommendation that W3C establish a "steering group" to formulate a strategy and roadmap of Web Payments, including existing work at W3C and potential new work.

At a high level, W3C will coordinate the development of new standards, or the adaptation of existing ones, to ease the interaction between the different actors of the payment ecosystem. Three areas of work will help bridge the app and payments ecosystems:

1. **Payment transaction messaging:** In order to increase interoperability, it will be essential to standardize the protocols and messages between web applications and payment providers. This includes information about the transaction (such as merchant ID, amount, and currency) and the digital receipt (proof of payments) for both merchants and customers.
2. **Wallet and Wallet API:** A "wallet" is an application that facilitates the installation and selection of specific payment solutions. Standardizing the interface between web applications and wallets will allow web application developers to support any current and future payments solutions transparently.
3. **Identity, Authentication and Security:** To decrease fraud, we will look for building blocks for verifiable identity and secure authentication of the different parties on a payment transaction.

In a few months, W3C will charter a Web Payments steering group to elaborate use cases and requirements for these topics in more detail. That charter is currently in development and open for public comment, to ensure that all stakeholders have an opportunity to shape the scope of activities.

Stéphane has been on the W3C Staff since 1995. Since 1 January 2014, he has been leading W3C work on Web Payments, part of the HTML5Apps EU-Funded project. He can be contacted at boyera@w3.org.

Ramping Up Payment Security with EMV Chip Technology

RANDY VANDERHOOF,
Director,
EMV Migration Forum

Recent retail data breaches have thrust the U.S. payments industry into the media spotlight and highlighted the need for improved security measures. Now, the spotlight is focusing in on EMV chip payment cards, which the U.S. has been migrating toward for a little over two years now.

EMV chip payments are a key piece in upgrading payments security due to their ability to prevent in-store counterfeit card fraud and devalue U.S. payment data present in retail systems in the eyes of criminals. U.S. magnetic stripe payment card information is easily cloned and is highly valuable, as it can be sold on the black market to other criminals for large profits.

EMV chip payments are a critical technology in implementing a layered security approach that will best secure our payments infrastructure, along with complementary tools such as PCI DSS compliance, tokenization and encryption.

While EMV chip technology *devalues* the payment data, the PCI DSS limits the amount of and access to the cardholder data within the payment ecosystem, making the two tools very complementary.

EMV chip prevents counterfeit card fraud in two ways:

The first way is by storing the cardholder data and security keys inside the chip. Even if chip data were to be copied, it could not be used to create another chip card using the same data. Also, EMV transaction data replaces other data needed for magnetic stripe transactions, so it cannot be used to make a fraudulent transaction in an EMV or magnetic stripe environment.

The second way is by having a cryptogram generated by the chip during each payment transaction. The cryptogram proves that the card is authentic and that the transaction data was unique to that card. Therefore, any data breach and re-use of the same unique card data would be detected and the transaction denied.

To put these security benefits into perspective: if EMV chip data had been present in the retailers' systems that were recently victimized, the impact of the data breach would have been significantly lessened for the merchant, the card issuers and the consumers due to the greatly reduced risk of counterfeiting and the resulting card fraud.

The migration to chip cards in the U.S. is complex, expensive and difficult to coordinate. The U.S. market is the largest individual market to convert to chip cards. With over 12,000 financial institutions that issue cards, an estimated one billion cards in the market, over 12 million POS devices in retail stores, and another 100,000 ATMs installed, the U.S. payments market is larger than all of Europe's payments markets combined.

A successful move to chip technology necessitates cooperation and coordination on the parts of every member of our payments ecosystem. To help facilitate this transition, the Smart Card Alliance created the EMV Migration Forum in 2012.

The Forum was formed specifically to address issues that require broad cooperation and coordination across many constituents in the payments space to ensure the timely, effective and successful adoption of EMV-enabled cards, devices and terminals across the U.S. market. The Forum has more than 150 members, including global payments brands, financial institutions, merchants, processors, acquirers, regional debit networks, industry associations and industry suppliers.

CONTINUED ON NEXT PAGE

Helpful resources to check out on the EMV Migration website:

- EMV and U.S. Chip Migration FAQ (note PCI and EMV chip question)
- EMV 101 Webinar
- Standardization of Terms
- Slideshow: What are Chip-enabled EMV Payment Cards?

Latest EMV chip-related PCI resources:

- Infographic
- Video
- PCI SSC Congressional Testimony

Getting ready for EMV Chip:

- EMV chip needs PCI DSS
- Don't forget e-commerce security
- Upgrading terminals? Make sure your EMV chip terminal meets PCI PTS requirements

Give Us the Scoop

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.

In the less than two years since its inception, the Forum and its six working committees have developed white papers, webinars and other deliverables that help the industry work through issues and move forward in its migration. Most recently, we released an industry-supported debit framework to help further propel EMV debit implementations. This framework provides a "future-proofed" approach for the debit card processing scenarios we know of today, so that debit industry organizations can build their own detailed specifications and continue on the way to chip implementation with confidence.

I am encouraged by the productivity of the Forum and the payments industry's recognition that we need to move to chip technology quickly, and by the fact that chip cards are being issued now and retailers are moving to put in place the chip-enabled terminals to begin accepting chip transactions by the industry's target dates.

Today, the chip card manufacturing market is ramping up to produce up to one billion new EMV chip cards in the next three to five years. By year-end, I expect to see 100 million cards in the market, and by this time next year the U.S. market will have issued more EMV chip cards than the UK and Canada combined. The ultimate measure of success is in the number of chip-on-chip transactions, or transactions that involve a chip card on a chip-enabled payments device.

If you want to get your organization moving quickly towards chip payments and keeping pace with the industry, I invite you to join the EMV Migration Forum and start listening to and learning from your colleagues with more EMV knowledge and experience.

PCI People on the Move

Caitlin Cavanagh

Nancy Rodriguez

Rob Martin

Allen Friedman

- Introducing **Caitlin Cavanagh**, the newest member of the PCI Security Standards Council team. Serving as Program Specialist for the Participating Organization Program and the PCI Professional (PCIP) Program, she has 10 years of experience as a Program Director and Member Services Professional at a non-profit. Feel free to drop Caitlin a line at participation@pcisecuritystandards.org at any time with any questions you may have about these programs.
- **Nancy Rodriguez**, CISSP, CRISC, is now the Global Payment Card Industry (PCI) Program Director, Treasury Information Security at Philips.
- **John Spence**, former Security Strategist for Ingenico North America, retired in December of 2013 after more than 20 years with the company. Replacing him as VP of Security Solutions is **Rob Martin**. Rob has been involved in the technical and product end of the payments business since 2000. From 2010 until this year, Rob led the terminal and mobile product line of business at Apriva.
- Also new to Ingenico is **Allen Friedman**, Director of Payment Solutions. Allen has over 30 years of experience in the payment industry in various roles including management, product management and technical business communications. Allen's new role at Ingenico will facilitate a more expansive promotion of our EMV capabilities as well as expert consultation with our clients and prospects.

TRAINING AT THE NORTH AMERICAN COMMUNITY MEETING

Make Your Trip to Orlando More Magical

Take a training class before or after the Community Meeting in September:

3–4 September: QSA

3–4 September: ISA

5–6 September: PA-QSA

6 September: PCI Awareness

12–14 September: P2PE New/Requalification

PCI Training – In Your Own Words

Meet Adam Griffith, ISA

The PCI Security Standards Council interviewed Café Rio's Adam Griffith to discover why becoming an Internal Security Assessor (ISA) was important to him – and how it's helping him and his company solidify their payment security efforts.

PCI SSC: What do you do for your company?

Griffith: I've been in this position for four years now – I lead the development of innovative systems that ensure that customers have a great dining experience. All the restaurant systems analytics, development, deployment and security roll up under my team. These systems and procedures have helped to take the company from 20 stores when I first started, to 67 today – and more locations are scheduled to open later this year.

PCI SSC: How does this training benefit you – and your company?

Griffith: Being a fast-growing company, we're always looking to stay in front of security requirements. Café Rio is approaching level one merchant designation, and being PCI DSS compliant is very important to us – especially as we prepare to have a Report on Compliance prepared by a QSA. The ISA training was an excellent way to learn how to incorporate the extensive PCI DSS requirements into our everyday business. It's given us immediate credibility with our processor and has made the process of working hand-in-hand with our external auditors much easier, too.

PCI SSC: How have you applied what you learned in this course, in your job?

Griffith: I use the knowledge from the training and certification daily. With almost 75% of our payments in our restaurants being credit cards, we wanted to make sure our customers and our business are well protected. The ISA training has allowed us to proactively look at our business and procedures and adjust them to incorporate the current PCI Standards. The qualification also has given me added credibility in the organization to make the changes necessary to be PCI DSS compliant.

PCI SSC: How do others view your new ISA status?

Griffith: During the decision-making process, there is an added level of credibility provided by my ISA qualification. In addition people now solicit my advice in how future changes could affect our continued PCI Standard compliance efforts.

PCI SSC: If you had to pick one thing that you liked best about the training, what would that be?

Griffith: During the two-day course, I had the chance to interact directly with the instructor during breaks and ask specific questions pertinent to my business. I also met a number of people across different industries and got to compare our PCI efforts. It's always great to meet other industry professionals and learn from their experiences.

PCI SSC: Why did you choose to get training through the Council?

Griffith: After doing research on available courses, it made the most sense to go directly to the PCI Security Standards Council for the training. Because it's the issuing body, I thought the Council would be able to provide the best information on how to adapt to the increasing need for security in our business.

PCI SSC: Do you feel the training was worthwhile?

Griffith: Yes, and I would absolutely recommend it!

Name: Adam Griffith

Title: Manager of Operations Systems

Company: Café Rio Mexican Grill

Key training take-away: The training around network configuration and monitoring requirements provided an immediate benefit in helping to implement new systems appropriately. It has saved us countless hours of internal rework and saved us billable hours with our external auditors. The payoff is quick and easily apparent.

Company background: Café Rio is an award-winning, casual restaurant chain prominent in the western United States, serving a variety of fresh Mexican-style recipes.

Our executive team has over 161 years of combined restaurant industry know-how, working for such industry giants as McDonalds, KFC, Taco Bell, and Burger King – coupled with broader corporate experience with Intel, Kodak, and Pixar Studios.

We have the Zagat stamp of approval, and for the past three years we've won Sandelman and Associates awards for being the #1 overall quick service restaurant in the country. In addition, Café Rio has won over 60 awards from groups such as Best of City Search, City Weekly, INC 500, Utah Business Magazine, Utah's Best of State, Alfred P. Sloan Awards, and the Oxnard Salsa Festival, just to name a few.

Cybersecurity Roundtables: U.S. Chamber of Commerce Launches National Series in Chicago

ANN M. BEAUCHESNE,
Vice President, National Security and Emergency Preparedness, U.S. Chamber of Commerce

Many cybersecurity experts say that there are two types of businesses -- those that have been hacked and know it, and those that have been hacked and don't know it yet. As large businesses strengthen their cyber protections, small and medium-sized ones are increasingly the victims of malicious actors.

On May 22 in Chicago, the U.S. Chamber of Commerce launched its national "roundtable" series to promote cybersecurity education and awareness of the Framework for Improving Critical Infrastructure Cybersecurity, which was capably developed by the National Institute of Standards and Technology (NIST) and the business community.

Leading partners included American Express and Splunk, the Chicagoland Chamber of Commerce, the Illinois Chamber of Commerce, and The Latino Coalition. The Chamber is planning to hold at least three more roundtables with local and state chambers prior to the Chamber's *Third Annual Cybersecurity Summit* on October 28. Visit www.cybersecurityadvocacy.com to learn about event details.

The framework features a number of industry-vetted actions that businesses can take to assess and improve their state of security over time. It provides organizations -- including their customers, partners, and suppliers -- with common language for understanding their current cybersecurity posture, setting goals for cybersecurity improvements, and much more.

The Chamber is urging businesses of all sizes and sectors to adopt fundamental Internet security practices to reduce network and system weaknesses and make the price of successful hacking increasingly steep. We recommend that businesses take the following steps:

- **Improve cyber risk management:** All businesses should understand common online risks that can lead them to become victims of cybercrime. Using the framework and similar risk-management tools, such as the Chamber's Internet Security Essentials for Business 2.0 guidebook, is ultimately about making your business more secure and resilient.
- **Report cyber incidents:** Perfect online security is unattainable, even for large businesses. Innovative solutions are regularly being brought to market because cyber threats are always changing. The market offers a wide variety of solutions targeted to businesses of all sizes. Businesses should report cyber incidents and online crime, including to the U.S. Department of Justice and the U.S. Secret Service.
- **Stay engaged:** Cybersecurity is a team sport. Chamber members are welcome to join the Cybersecurity Working Group to stay engaged in the cybersecurity education and framework awareness campaign – *Improving Today. Protecting Tomorrow*™ – and advocate for industry's cyber policy priorities in Washington, D.C.

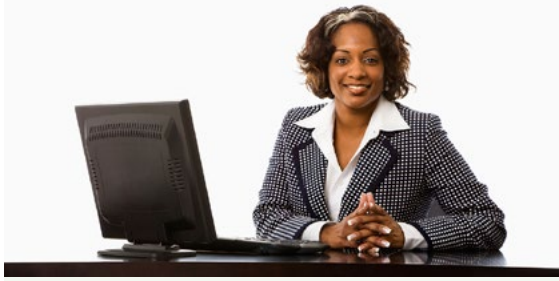
Big picture: A consensus exists among cyber experts that a high percentage (approximately 80%) of unsophisticated or untargeted malicious activity can be stopped by implementing elements of the framework. Using the framework is tantamount to improving one's cyber "fitness."

There are built-in assumptions that an organization's cyber capabilities will weaken if it becomes passive, and that *continual improvement* is necessary for a business to keep pace with threats.

Passing information-sharing legislation is the Chamber's top cyber legislative priority. The framework will be incomplete without the enactment of information-sharing legislation that removes legal and regulatory penalties so that companies and information-sharing organizations can quickly exchange data about evolving threats to U.S. business and economic security.

NIST and industry experts produced a smart framework that cybersecurity stakeholders are proud of. This tool provides a common language around information security and risk management activities. Government and business entities need to leverage it to strengthen collective security and resilience and make ongoing improvements.

PCI Essentials Training



PCI DSS Requirement 12.6 states that a formal security awareness program must be implemented to make all employees aware of the importance of cardholder data security. We have a new eLearning course that just may fit the bill for your organization.

PCI Essentials is an engaging, interactive series of 10 modules, which can be combined to provide approximately two hours of training. Each module focuses on a specific area of cardholder and information security, so as to have a tangible impact on knowledge retention and behavior. Offered through Security Innovation.

Approved Scanning Vendor (ASV) Update

MARK MROTEK, Certification Programs Manager, PCI Security Standards Council

To demonstrate compliance with the PCI DSS, merchants and service providers may be required to have periodic PCI DSS external vulnerability scans conducted as defined by each payment brand, in accordance with PCI DSS Requirement 11.2.2.

PCI DSS external scans are conducted over the Internet by an approved scanning vendor (ASV) and help identify Internet-facing vulnerabilities and misconfigurations of websites, applications, and supporting infrastructures. Vulnerability scan results provide valuable information that supports efficient patch management and other security measures that improve protection against Internet attacks.

Is my organization required to undergo vulnerability scanning?

Merchants and service providers are responsible for maintaining compliance with the PCI DSS at all times, which includes properly maintaining the security of their Internet-facing systems. Even if an entity does not offer Internet-based payment transactions, other services may make systems Internet-accessible. An e-commerce merchant with a website that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data may still be required to have periodic PCI DSS vulnerability scans conducted as defined by each payment brand. We recommend that you contact your acquiring bank or the payment brands to fully understand your compliance validation and reporting obligations.

What is my organization's part in the external vulnerability scanning process?

The scan customer is responsible for things such as defining the scope of the external vulnerability scan and providing the IP addresses and/or domain names of all Internet-facing systems to the ASV so they can conduct a comprehensive scan. The scan customer is also responsible for implementing proper network segmentation for any excluded external-facing IP addresses, and ensuring that active protection systems (such as intrusion prevention technologies) do not interfere with the ASV scan. We recommend reviewing the ASV Scan Scope Definition section of the ASV Program Guide for more information on scoping. The ASV scans all IP address ranges and domains provided by the scan customer to identify active systems, services, and potential vulnerabilities therein. If IP addresses and/or domains not provided by the scan customer are found by the ASV, the ASV consults with the scan customer to determine if they should be included in the scan's scope.

What if I disagree with the ASV's findings?

Upon completion of the scan, the ASV prepares the scan report, provides it to the scan customer, and the scan customer submits the report as directed by the payment brands. However, if the ASV report includes hosts and/or domains that the scan customer determines are not in scope for PCI DSS, or vulnerabilities that the scan customer believes may be "false positives" or other potentially-erroneous items, the scan customer works together with the ASV to resolve the matter. The scan customer may dispute the findings in the ASV scan report, such as (but not limited to) false positives, vulnerabilities for which a compensating control is in place or other conclusions of the scan report. The ASV must have a written procedure in place for handling disputes, and the scan customer must be clearly informed on how to report a dispute to the ASV, including how to appeal the findings of the dispute investigation with the ASV. The ASV must explicitly inform the scan customer that disputes in scan results are NOT to be submitted to the PCI SSC (the PCI SSC does not arbitrate on any such matters). Since these topics have many aspects beyond the scope of this article, we recommend reviewing and becoming familiar with each section of the ASV Program Guide, including Resolving Failing Scans, Resolving Inconclusive Scans, Addressing Vulnerabilities with Compensating Controls and Managing False Positives and Other Disputes.

How can I provide feedback about my ASV?

Excellent question – we have an FAQ for that! Please see FAQ article 1036 on the Council's website.

We hope this article provided a decent overview of the ASV program and the various roles and elements within. We are always interested in feedback on how we can improve our programs; if you have comments, questions or thoughts on the ASV program, please contact the ASV program manager at asv@pcisecuritystandards.org.

How are ASVs different from non-PCI approved vulnerability scanning vendors?

An ASV is an organization with a set of security services and tools ("ASV scan solution") to validate adherence to the external scanning requirement of PCI DSS Requirement 11.2.2. Organizations interested in providing vulnerability scanning services in accordance with the PCI DSS must comply with the requirements set forth in the ASV Program Guide as well as the Qualification Requirements for Approved Scanning Vendors, and they must also successfully complete the PCI testing and approval process. All ASV scan solutions are assessed in a testing laboratory against a network environment containing predefined vulnerabilities and misconfigurations. ASV scan solutions must scan for and detect vulnerabilities in the lab environment and produce a sample ASV report to demonstrate their scan solution's capabilities. The ASV report is then evaluated by specialists in the test lab and scored against a strict baseline before the ASV is considered for approval and added to PCI SSC's List of Approved Scanning Vendors.

Where can I find out more about becoming an ASV?

Please see the Become an ASV page on the PCI SSC website.

Where can I find out more about the ASV Program in general?

For more information on the ASV program, we recommend starting with the ASV Program Guide and searching the Documents Library for topics of interest. You can also search our list of Approved Scanning Vendors to find an ASV by company name, product name, place of business and locations served. Additionally, the Council has published the PCI DSS E-commerce Guidelines Information Supplement, which has received very positive feedback from scan customers and other members of the e-commerce and information security communities.

Technology Update: Point-to-Point Encryption

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

This is the official PCI Security Standards Council 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 the newest company to have its solution listed, Bluefin Payment Systems. In this section, learn why they think point-to-point encryption technology is a strong tool for your payment security portfolio.

RUSTON MILES,
Chief Innovation Officer, Bluefin Payment Systems

On benefits to merchants…

The reduction of cardholder data environment (CDE) scope and applicable controls by using a PCI P2PE Solution is the most significant way available for merchants to reduce overall PCI DSS compliance-related costs. Other end-to-end encryption options are available in the market, but only Council-listed P2PE Solutions are recognized as meeting the requirements necessary for reducing CDE scope.

On getting a P2PE solution PCI validated….

We set out to create and receive validation for a PCI P2PE Solution and watched as the six months we planned for the project turned into over a year and a half of highly focused effort. This program requires providers to institute and maintain new human and system processes, including chain of custody and dual control that are not generally required outside of the program. The P2PE Solution is all-encompassing and requires careful planning and a concerted effort to create an ongoing and securely managed workflow among your device manufacturers, key injection facilities, data centers, internal operations, systems, software, and security. Do not underestimate the importance of the word "Solution" in P2PE Solution. P2PE is much more than simply connecting encrypted point-of-entry devices and HSMs.

On how P2PE can help address payment security challenges….

In order to attain and maintain compliance with PCI DSS, organizations must prove to their Qualified Security Assessor (QSA) or attest on their Self-Assessment Questionnaire (SAQ) that each control is either in place or not applicable. Implementing and maintaining many of the policy, system, software, network, database, device and process controls represents an upfront and ongoing cost of compliance with seemingly little ROI. Use of a validated, Council-listed P2PE Solution can limit the scope of the cardholder data environment (CDE), making many of the required controls not applicable, which in turn can reduce the ongoing cost of compliance, improving ROI.

PAYMENT SECURITY BOOKSHELF

- Jacob A. Ansari, CISSP, MSIA, QSA, PA-QSA, 403 Labs, Sikich LLP is reading ***The Cuckoo's Egg*** – Cliff Stoll's account of responding to a computer security incident from the early days of the Internet. Despite its age, it still presents some valuable lessons for incident response and thinking like an adversary in order to protect your own organization.
- Slava Gomzin is a Security and Payments Technologist at Hewlett-Packard, where he helps create products that are integrated into modern payment processing ecosystems using the latest security and payments technologies. As PCI ISA, he focused on security and PA-DSS, PCI DSS, and PCI P2PE compliance of POS systems, payment applications, and gateways. Slava currently holds CISSP, PCIP, ECSP, and Security+ certifications. He blogs about payment security and technology at www.gomzin.com. Slava Gomzin, just wrote ***Hacking Point of Sale***. Available for purchase.

Reducing the Cardholder Data Footprint

TROY LEACH,
Chief Technology Officer,
PCI Security Standards Council

With so much discussion of late about "scope reduction" for both point-to-point encryption and tokenization, it is important to remember the primary purpose of these technologies is to minimize the exposure of cardholder data making merchants and other entities less attractive targets for criminals.

If we can limit the locations of cardholder data (CHD), the smaller subset of systems to protect should improve the focus and overall security of those systems. And better security should then lead to simpler compliance efforts.

While we're excited about these opportunities, there are other ways as well to minimize where cardholder data resides by evaluating existing business process to determine if former ways of accepting payments are still the best way to do so.

In either case, knowing *where* your cardholder data is located is a critical part of your planning. Here are a few things to keep in mind when trying to reduce the cardholder data in your network:

Maintain a CHD dataflow diagram

First, we need to identify how we can **reduce the attack surface**. This is first achieved by maintaining a dataflow diagram showing all locations and flows of cardholder data. This is already required as part of PCI DSS Requirement 1. But how often is that reviewed during the year to confirm it reflects changes? Or is it dusted off only when the QSA comes on site, and then you need to go through a series of mitigation steps because it's not up to date?

Remember the weakest link in your environment are the locations where you DON'T know that cardholder data is there. The majority of compromises occur on systems that the entity didn't even know had access to cardholder data.

Dataflow diagrams help identify which systems require protection and may also help when responding to vulnerabilities or a potential compromise. Several of the forensic investigators that we've invited to speak at our Community Meetings over the years tell the same story. They find that the company suffering the compromise was unaware that cardholder data was present on the compromised systems and often have a better idea about how and where cardholder data flowed throughout the organization's network than the organization itself did.

Meet regularly with those able to create cardholder data pathways

People. We always say that security is compromised of the **People, Process and Technology** but it seems the more interconnected our technology becomes, the more disconnected our professional relationships with other people becomes.

To help stay current with process and dataflow, we encourage you to meet regularly with those in your company (or third-party relationships) who have the ability to create payment pathways. Are their processes up to date? What remote connections are there to third-parties? If you are responsible for maintaining the dataflow diagrams (and somebody in your organization should be) have a formalized process, place it on your calendar to meet regularly, even if it is simply check-in to confirm nothing has changed. According to the Ponemon Institute, those organizations that were doing more regular audits of the environment actually saved 55% overall on their annual cost to comply with PCI DSS. This simple step may save your organization significant expense.

Consider a data discovery and data loss methodology

At the Council, we view Data Loss Prevention as a *method* (not necessarily a product) to identify, monitor, and protect **data in use** (e.g. endpoint actions), **data in motion** (e.g. network actions), and **data at rest** (e.g. data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination and so on) and with a centralized management framework. Data loss prevention is not required by PCI DSS; however, it may be a valuable addition to your security strategy as part of your risk management program.

If you don't need it, don't store it

Lastly, but most importantly, remove legacy cardholder data that is no longer needed. I'm often surprised by the stories of compromises where data was stored with no business or financial reason to do so. However, you can only permanently eradicate the storage of cardholder data if you know first where your data is and then evaluate the business need for each location and flow of cardholder data.

Keep these considerations in mind when looking at ways to reduce your cardholder data footprint. When planned for and implemented properly, both point-to-point encryption and tokenization can minimize PCI DSS complexity and improve security of sensitive data but don't limit their capabilities by not properly identifying the cardholder data environment to begin with.

Small-to-Medium Business Focus

Passwords for Payments (P4P) Initiative

We both know that small businesses are increasingly under threat by hackers looking to steal their valuable credit and debit card information - and that awareness among this population globally is dangerously low.

Which is why at the PCI Council we've launched Passwords for Payments (P4P), an awareness initiative to educate the small business on password protections for payments.

As an organization that recognizes payment security is a shared responsibility, and that knows the first step to change is education, **we need your help**.

Join us in becoming an official P4P ambassador to educate small businesses on making smart and secure choices when it comes to using and changing passwords on computers and payment systems to protect their customer's confidential payment card information - and reduce their chances of being breached.

For more information and to join the P4P initiative, check out our small-medium business focused website.

Questions? Email us at P4P@pcisecuritystandards.org.

New PCI 101 Security Videos – EMV Chip, P2PE and Mobile Made Simple

Trying to get your head around what point-to-point encryption is and how it works to help protect payment card data? Looking to understand how to securely accept payments using a mobile device?

Maybe you've got customers who are asking you about why they need to do PCI if EMV chip is coming to the U.S.? Check out these new quick animated videos from the PCI Council that take a crack at explaining each of these technologies and their implications for payment security. They're fun, entertaining and informative and easy to share resources. Check them out on our SMB microsite or on the PCI SSC YouTube channel.

Pass them along via Twitter, LinkedIn and other social media platforms: Check out the new PCI 101 security videos #PCI4SMB http://bit.ly/1q7sLua

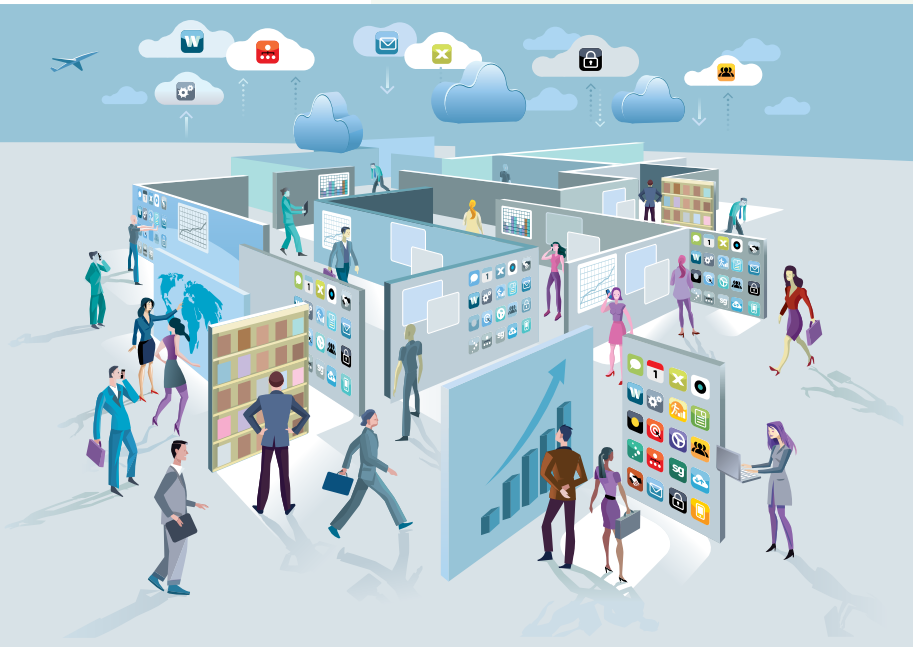
PCI RESOURCES FOR SMALL BUSINESSES

- Quick guide to the PCI Data Security Standard (PCI DSS)
- Listing of secure payment software for point-of-sale – Validated Payment Applications (eg: shopping carts)
- Listing of secure point-of-sale devices – Approved PIN Transaction Security Devices (eg: card readers)
- Listing of technology partners for proper and secure installation of point-of-sale systems – Qualified Integrators and Resellers
- Quick resources and infographics
- PCI Awareness and PCI Essentials training

To access these resources, go to the PCI SSC website.

Networking with Your Peers Before the 2014 Meetings!

- Learn more about the event and register here
- Use the #PCICM hashtag to share this event via Twitter
- Join our LinkedIn Networking Group



New Participating Organization Spotlight

Academy of Information Systems

Academy of Information Systems (AIS) was established in 1996 as a multi-disciplinary training center. It currently conducts training in the fields of information security, competitive intelligence, information technology and management systems. AIS also organizes conferences at national and international levels. AIS became a Participating Organization in order to stay abreast of the latest news in the field of PCI Standards and to share experience, especially in the area of training and awareness.

Crosskey Banking Solutions

Crosskey develops, delivers and maintains systems and solutions for the Nordic bank and capital markets. Our mission is crystal clear – make it easier and more profitable for our customers to operate a bank. Crosskey is one of the first PCI DSS compliant providers in the Nordics. We decided to join the PCI Security Standards Council in order to keep updated with what is going on with the PCI DSS and to learn, adapt and contribute to the ongoing efforts to secure cardholder data. When we develop banking solutions, we have the customers of the future in mind.

The CCV Group

The CCV Group is a European player in electronic payment solutions with 850 employees across offices in the Netherlands, Belgium, Luxembourg, Germany and Switzerland. We joined the PCI SSC to stay informed on developments surrounding PCI Standards with the intention of proactively using this knowledge in our development. For us, PCI data security is more than just a requirement – it helps us make sure that the products we create today are ready for the world tomorrow.

EDF Energy PLC

EDF Energy is one of the UK's largest energy companies and its largest producer of low-carbon electricity. A wholly-owned subsidiary of the EDF Group and one of Europe's largest energy groups, we generate around one fifth of the UK's electricity and employ more than 15,000 people. We supply electricity and gas to about 5.5 million residential and business customers, which makes us the biggest supplier of electricity by volume. EDF Energy has become a Participating Organization so that we can contribute to new standards, participate in Community Meetings, receive regular and focused communications from the PCI Security Standards Council and get great discounts on training.

Groupement Interbancaire Monetique de L'uemoa (GIM-UEMOA)

GIM-UEMOA is the leading card payment system and service provider in the UEMOA (West African Economic and Monetary Union) region. Over 100 banks and financial institutions are connected to the GIM-UEMOA platform. By working with the PCI Security Standards Council, GIM-UEMOA is looking to become an active part of the payment standards process and to exchange best practices with others in the industry.

NEW PARTICIPATING ORGANIZATIONS

Welcome to these organizations that joined between January-June 2014.

- Academy of Information Systems
- Airlines Reporting Corporation
- Amazon.com
- AOL Inc.
- Canon USA, Inc.
- Carlson Wagonlit Travel
- CCV Holland B.V.
- COOP Israel
- Crosskey Banking Solutions
- Crutchfield Corporation
- Delhaize America Shared Services Group, LLC
- EDF Energy PLC
- Enterprise Holdings, Inc.
- General Motors Global Connected Consumer (OnStar) Subsidiary
- Global Cash Access
- GlobalCollect Services B.V.
- Groupement Interbancaire Monetique de L'uemoa (GIM-UEMOA)
- Interoute Communications Ltd.
- Liverpool Victoria Friendly Society
- Lumen21, Inc.
- Nacion Servicios S.A.
- National Australia Bank
- Patterson Companies, Inc.
- Paymark Limited
- Pet Supplies Plus
- Philips International B.V.
- Secure Retail
- Syzygy Risk Sciences
- T-Mobile USA, Inc.
- TransUnion LLC
- University of California
- University of Colorado

Lumen21, Inc.

Lumen21 is a consulting firm specializing in infrastructure optimization and custom application development, and we are a Managed Services Provider. Lumen21 has joined the PCI Security Standards Council in order to help customers comply with the PCI DSS and other regulatory security standards. We are enabling our retail customers to fully leverage the business benefits of cloud computing. These include lower capital and operating costs, increased business continuity, strengthened security and improved energy efficiencies, which can all be achieved while enforcing current compliance standards. With its sister companies, Lumen21 will make available PCI scanning services and auditing services for a comprehensive solution to retail clients' needs.

Philips International B.V.

Nancy Rodriguez, Global PCI Compliance Director at Philips (a leader in cardiac, acute, home healthcare, energy efficient lighting solutions and new lighting applications, as well as male shaving and grooming and oral healthcare), enrolled the company as a Participating Organization within two months of her hiring. "I felt it important for Philips' voice to be heard in providing input for the standards and guidelines documents, as well as receiving valuable updates on industry-specific topics, price-reduced training and two free seats at the Community Meetings. I have been involved with the PCI Security Standards Council almost 10 years and find that networking made life-long friends and colleagues."

Secure Retail

Secure Retail is a specialist provider of payments hardware and services for the retail, hospitality and unattended sectors. We provide solutions that minimize business exposure and complexity to meet the rigorous demands of the latest PCI Security Standards. Secure Retail is the preferred distributor of VeriFone payment terminals and a provider of Miura, Atos and Displaydata technology. We offer portable and fixed PIN entry devices, mobile POS, tablets, unattended terminals and electronic shelf edge labelling. We also provide various options of secure cradling and tethering solutions. We joined the PCI Security Standards Council because it fits well with our business ethos.

Syzygy Risk Sciences

Syzygy Risk Sciences has focused for many years on helping our partners and customers balance the growing number of cyber security risks. The PCI Security Standards Council and the developed standards are examples of well-crafted and balanced risk management programs to assist our customers in protecting cardholder data, and the PCI SSC is a leading industry example of how to properly develop security frameworks. Being active with the Council gives us a chance to help address new technology challenges as well as providing feedback to evolve the control frameworks.