Standards Today

A Journal of News, Ideas and Analysis

A publication of CONSORTIUM INFO.ORG

GesmerUpdegrove LLP

June–July 2009 Vol. VIII, No. 4

INTERVIEW:

Enabling an Ecosystem of Security: An Interview with PCI SSC's Bob Russo

Andrew Updegrove

As anyone who follows the news is aware, data breaches involving credit and debit card information have been very much in the public eye. In the cases that have received the most publicity, information relating to over 45 million cards was compromised by the breach of retailer TJ Maxx, and when malware was installed on a server of card transaction processor Heartland Payment Systems, the number of cards compromised may have exceeded 100 million. And indeed, with millions of retail outlets taking payments via credit and debit cards, the points of opportunity for hackers to access card data in batches large and small are inevitably great. The only way to prevent such breaches is for retailers, and those upstream from them (e.g., banks, processors and card issuers), to exercise great care and constant vigilance to guard against intrusion.

But what practices are most effective, and how much security is enough? These are difficult questions, given that the answer must address the vulnerabilities of a network that includes an almost infinite number of data entry devices, a global communications network administered by many different companies, processing and database software from multiple vendors, transaction processing service companies, card issuing banks throughout the world and multiple payment card brands. Achieving security in a manner that is consistent is also vital, so that merchants are not subject to radically different requirements imposed by each payment card brand with whom they do business. Clearly, then, there is a need for a central, collaborative organization that can set the bar for security for each primary area of vulnerability in the payment card ecosystem, define best practices, certify compliance efforts, and strive for consistency, all while remaining aware of

the realities of the marketplace, and costs of compliance. In other words, a standards organization.

In order to achieve such a consistent, effective security environment, five of the major payment brands (American Express, Discover Financial, JCB, MasterCard Worldwide and Visa) came together in 2006 to rationalize and standardize their evolving, individual programs and to collaborate to develop new standards as needed to address new cybersecurity threats. The organization they created is called the PCI (for payment card industry) Security Standards Council, or PCI SSC. Today, more than 500 stakeholders in the global payment card ecosystem (merchants, banks, government and others) have joined the effort as Participating Organizations.

Not long after its launch, PCI SSC hired Bob Russo as its first General Manager. Russo came to the job with 25 years of security industry experience, in the course of which he had been a founder or senior management member of many service, software development and compliance companies. As General Manager of the Council, Russo is responsible for executing the Council's policies and achieving its goals. More specifically, he oversees the Council's training, testing and certification programs, supports the certification process, coordinates research and analysis, solicits feedback from the vendor and merchant communities, and drives recruitment of stakeholders as Participating Organizations in the Council.

In this detailed interview, Bob Russo explains how PCI SSC came into existence, the industry challenges it was formed to address, the unique infrastructure that it has helped create, and how the Council is helping the payment card ecosystem to work together to safeguard payment card and personal information. What he has to share is useful to provide insight into the challenges of protecting such information from fraud. More broadly, though, the standards that the Council develops and the infrastructure that it supports provide an example of the type of comprehensive, global risk management regime that can be emulated in many other settings where equivalent amounts of personal information will become vulnerable to breach and misuse, from open government to electronic health records. Unless similar or equivalent organizations come into existence in these areas, the consequences may be regrettable.

Unless similar or equivalent organizations come into existence in these areas, the consequences may be regrettable

Disclosure: The author and his law firm, Gesmer Updegrove LLP, have represented PCI SSC since its formation.

Part I: Why, When and How

AU: *How did PCI SSC come into existence?*

BR: The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The Council was formed in September 2006 by the five major payment card brands, our founding members American Express, Discover, JCB, MasterCard, and Visa. These original members of the Council agreed to work together to develop and recognize one set of data security standards to protect their customers systems and the consumer's data that resides within them.

Prior to the formation of the Council, retailers and other merchants had expressed frustration at the challenges of securing card data in a way that was recognized universally by all the payment card brands they did business with. Organizations involved in the payment process also highlighted their desire for a mechanism to contribute to the card data security agenda and enable them to provide some input into the security standards they would be using. Hence, on the back of strong industry feedback, the Council was formed.

AU: *What are the special challenges that maintaining payment card security faces?*

BR: There will never be a silver bullet! Data, in one form or another, must always be stored and therefore must constantly be protected. Networks today are so complex, it is a constant job to make sure whatever little tweaks are made in one area by one group do not affect other areas. The only way to insure this is through constant testing, monitoring and vigilance.

There will never be a silver bullet! Data, in one form or another, must always be stored and therefore must constantly be protected

AU: *The payment card ecosystem has many stakeholders besides payment card brands and payment card users. Who are the other players in the payment card chain, and what role do they play in ensuring security?*

BR: Along with input from the five founding members, the Council is able to enjoy a wide range of contributions and insight from our Participating Organization membership which is comprised of over 500 leading global players in retail, hospitality, financial services, technology, government and academia.

These represent some of the key players in the payment card chain, from card accepting retailers, their acquiring banks or processor service providers, through to consumers' card issuing banks, technology solution providers that service various parts of the payment chain, and associations that represent various constituents within these broad groups.

This Participating Organization group, along with the Council's approved Qualified Security Assessor community, numbering 168 people/companies, is able to provide the Council with real world insight and experience of deploying security standards in the field and the challenges and threat vectors security standards must combat. This Participating Organization group represents the people who are responsible for securely handling and defending consumer's data against attack and therefore are a valuable resource in feeding front line threat information into the Council.

From this participating organization group a smaller group of 21 representatives are seated as the Board of Advisors every two years through an open election and appointment process. Two thirds of the Board of Advisors are elected, with a further third appointed to ensure adequate geographical and industry representation. These organizations are the mouthpiece of their respective industries and ensure that the Council is able to partner with industry at a very detailed and actionable level in the standards setting process. This Board of Advisors is a critical enabler in our mission to secure businesses payment processes and consumers cardholder data globally.

Our current Board of Advisors is comprised of leaders in their respective industries such as Wal-mart, Microsoft, McDonalds, British Airways and APACS. The Board has worked tirelessly with the Council over the past two years to highlight areas of need in the market and devise educational resources such as the recently launched "Prioritized Approach" to the PCI DSS *[Ed: This is the Council's core standard, the PCI Data Security Standard]*, a resource that helps organizations starting out on their card data security journey to work with a risk based approach to compliance and start their process at the point that will reduce the impact on consumers and their business should a compromise occur. The Board of Advisors nomination and election process is underway this spring to seat the next Board and we welcome the Committees involvement in this process.

PCI Security Standards Council's QSA qualification requirements are exacting and detailed, involving both the security companies and their individual employees

AU: *Who else plays an important role in the payment card security ecosystem?*

BR: The Council's various certified security assessors and scanning vendors are organizations focused on security services and provide valuable consultancy, assessment services and technology solutions to organizations of all shapes and sizes that are focused on securing their payment card data. This is an important group at the front line of helping their customers secure payment card data.

- ***Qualified Security Assessor (QSA) companies:*** Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI DSS. The Council has qualified over 100 companies and trained and certified over 1500 assessors.

- ***Payment Application Qualified Security Assessor (PA-QSA):*** These are organizations that have been qualified by the Council. Payment Application Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI PA-DSS.

- ***Approved Scanning Vendors (ASVs)***: These are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers. The Council has approved over 130 ASVs.

Because the quality of PCI DSS validation assessments can have a tremendous impact on the consistent and proper application of security measures and controls, the PCI Security Standards Council's QSA qualification requirements are exacting and detailed, involving both the security companies and their individual employees.

As an aspect of the Council's auspices that interacts with stakeholders frequently, these organizations come under great public scrutiny. In order to maintain the highest level of standards in assessment following QSA training, the Council has launched a quality assurance program for QSAs and ASVs. The program was designed to provide QSAs and ASVs with a set of requirements that helps ensure they provide consistent, quality validation and assessment services to merchants and service providers.

The PCI SSC developed the quality assurance program as a direct result of feedback from the Council's Participating Organizations and assessment community and is intended to promote consistent interpretation of the PCI standards and ensure quality is maintained among all vendors. Participation in the program is required for the Council's registered QSAs and ASVs, in order for them to retain the ability to conduct PCI assessments.

[The] information that may be contained in the magnetic strip on the back of the payment card… [is] is the information that cyber criminals want to steal to create counterfeit cards. The proverbial keys to the kingdom

In addition, these key stakeholders share the redacted data of their assessments and provide a unique window for the Council to observe current challenges and trends within specific aspects of the DSS, and allow a feedback opportunity to understand the real world challenges of PCI implementation.

AU: *How are these other types of stakeholders represented in PCI SSC?*

BR: For those others not specifically included in our Participating Organization, QSA and ASV communities, the Council offers an education program that includes printed materials, online resources, webinars and face to face training sessions.

The Council's newly launched Standards Training program is designed to help merchants and service providers improve preparation for on site assessment, understand what is involved in creating their own internal assessment capability, and establish an internal program to help sustain PCI DSS security practices and compliance. This new course was introduced directly as a result of stakeholder feedback to the Council.

AU: *What are the principle standards that PCI SSC has developed to date?*

BR: The Council's standards – the tools it makes available for use by public and private sector entities to secure payment card data – are designed to protect specific parts of the payments process. The Council is constantly looking for new standards to secure, and maintains a dialogue with its Board of Advisors and other industry stakeholders to bring new resources to the market to increase the security

of consumers payment card data. I'd like to give a brief overview of some of these tools.

PCI Data Security Standard (PCI DSS): The PCI Data Security Standard is a set of 12 requirements that cover 6 principles to secure payment card data. At the heart of this standard is the requirement that organizations do not store sensitive information that may be contained in the magnetic strip on the back of the payment card. This is the information that cyber criminals want to steal to create counterfeit cards. The proverbial keys to the kingdom. The fundamental principle of the PCI DSS is that organizations must not store sensitive data from the back of the card. Where information on the front of the card is stored, it must be rendered unreadable. This means that it must be truncated, hashed or rendered in some way unreadable.

Along with these fundamentals, the requirements range from securing networks and perimeters, maintaining up to date security patches and anti virus software, down to things like developing and maintaining an incident response plan and processes for your organization to follow in the event of a breach.

Forrester estimates that the TJX breach will cost TJX $1.35 billion in breach related costs including legal fees, call center costs, regulatory fines, etc.

The Payment Application Data Security Standard (PA-DSS): The Council developed this standard after feedback from our membership indicated that software applications represented a point of weakness in the payment chain. Payment applications might, for example, be touch screen applications you see used in a restaurant or convenience stores. Some of these payment applications may be unknowingly storing sensitive payment card data therefore undermining an organizations effort to comply with the PCI DSS. The Council introduced a process where payment applications are tested in Council approved laboratories to check that they are secure, not storing payment data, and will help, not hinder, an organizations efforts to comply with PA-DSS. The Council maintains a list of approved payment applications that have been tested in and approved by Council laboratories, on our website for merchants to cross reference the status of their own applications and to make informed purchasing decisions.

The PIN Entry Device Security Requirements: The PIN Entry Device security requirements have the same underlying principle as PA-DSS. They are designed to enable organizations to protect consumers' cardholder data and ensure that PED devices are not unwittingly storing payment card information, or jeopardizing organizations PCI DSS compliance efforts. As a PIN Entry device is a physical object, these requirements cover not just ensuring that a device does not store sensitive data, but also that it is tamperproof and should it be compromised, any contents of the device will self destruct.

The Council maintains a list of approved devices that have been tested in and approved by Council laboratories, on our website for merchants to cross reference the status of their own devices and to make informed purchasing decisions. The Council is currently working to expand the scope of this program to include different

device types including unattended payment terminals such as ticket kiosks and self service machines.

Lifecycle of the Standards: Development and review of the PCI DSS is a continuous process that follows the Council's published PCI DSS Lifecycle process. This document (Exhibit A to the PCI DSS) outlines the PCI DSS development and evolution process. Because compliance with the PCI DSS is required of millions of merchants, banks and other stakeholders around the world by PCI SSC's members, changes to the PCI DSS must be carefully considered, and those affected must be given advance notice of any new requirements that will be imposed upon them. The upgrading of the PCI DSS therefore operates on a two-year lifecycle process that incorporates five phases:

- Stage 1 market implementation of previous version/revisions
- Stage 2 feedback begins
- Stage 3 feedback review and decision-making
- Stage 4 new version/revision and final review
- Stage 5 discuss new version/ revision

The Council is currently in the implementation phase of PCI DSS 1.2. The next formal feedback period will start in July 2009, with the goal of launching the next version/revision of the PCI DSS in October 2010.

The last open review period culminated in the discussion of the new standard -- PCI DSS 1.2 -- at our annual community meetings in Orlando, Florida in September 2008 and in Brussels, Belgium, in October 2008. In addition to this formal lifecycle process, part of the ongoing work of the Technical Working Group (TWG) is to regularly discuss and examine existing and new security technologies, issues and best practices with the goal of ensuring that the PCI DSS provides strong levels of security and effectiveness to stakeholders in the payment process without unfairly burdening the global marketplace.

The number and variety of potential deployments for enabling and processing credit card transaction is huge, depending on IT infrastructure, hardware and the scope of the enterprise

While a planned lifecycle process is important, it is equally important that the Council be responsive to emerging threats. As a result, we have several mechanisms for ongoing communications with Assessors, Merchants and other stakeholders to provide guidance as new threats emerge. These include:

- Errata to the DSS itself;
- Flash bulletins on emerging threats;
- A monthly newsletter to the Assessor community with the latest threat information & corresponding changes required to the assessment process;
- Regular updates to the ASV test scanning environment to reflect new threats emerging "in the wild";
- Monthly Webinars with both assessors and merchants;

- Updates to the Council's online searchable FAQ and training materials to ensure they include the latest information on the threat landscape.

AU: *Most individual standards tend to address very discrete needs. The DSS is very different in that it seeks to describe a very broad security environment in many different ways. What are these ways?*

BR: The number and variety of potential deployments for enabling and processing credit card transaction is huge, depending on IT infrastructure, hardware and the scope of the enterprise. A multinational chain retailer in Boston will have a significantly different network map than a mom and pop shop in Buenos Aires, or from a financial institution that processes transactions from millions of merchants in Hong Kong. The DSS needs to take into consideration the variety of possible deployments and provide a solid foundation of security that enables these transactions to be completed in a safe manner. So, every facet of the Standards needs to be vetted to ensure that it works in multiple payment environments, and allows for the seamless integration of payment security into the transaction process. As such, a lot of the focus is not just on securing the payment information, but separating, or removing from scope the non-payment elements of the network

AU: *How does PCI SSC relate to other domestic and international standards organizations and their work?*

BR: As a global, open industry standards body providing management of the Payment Card Industry Data Security Standard, the Council must address all the payment landscape variances in around the world. As such, we openly solicit feedback and information from national and international interests. However, security solutions or guidelines mandated by regional interests may not be effective, or implementable in other areas of the world. As such, the Council regularly examines the work of other standards organizations to address whether they can function within the scope of the Council's global purview, as part of the ongoing lifecycle of the Data Security Standards. That said, the Council must remain relevant globally to service the needs of our Participating Organizations and founding members, so we will continue to resist alignment with any geographically specific norms.

A multinational chain retailer in Boston will have a significantly different network map than a mom and pop shop in Buenos Aires,… The DSS needs to take into consideration the variety of possible deployments and provide a solid foundation of security that enables these transactions to be completed in a safe manner

Part II: The Challenges Ahead

AU: *Over the past year there have been several high-profile break-ins, resulting in the compromise of cardholder data. What types of standards-related weaknesses were exploited by hackers in gaining access to this data?*

BR: From the information we have available, the PCI Standards remain sound. We have yet to see a data breach from an organization that was in compliance with the DSS. If anything, the recent breaches have underscored a necessity for more vigilant monitoring of systems, as compliance and subsequent risk for a data breach may be only one small network change away. Compliance is a snapshot in time. The Council continues to emphasize sound security practices as a business necessity, not simply a checklist approach to achieve compliance.

AU: *Security is expensive, and the economy is poor. How does PCI SSC balance costs with the need to ensure security for those that have the burden of implementing PCI SSC standards?*

BR: I think a more important question is how can an organization afford NOT to do this. Compare the cost of achieving PCI compliance to the potential cost of a data breach to an organization. For example, a recent survey by the Ponemon Institute found that the cost of a data breach rose to $202 for each compromised record last year, an increase of 2.5% over 2007, with an average expense to an organization of $6.6 million.

Forrester estimates that the TJX breach will:

- cost TJX $1.35 billion in breach related costs including legal fees, call center costs, regulatory fines, etc.
- the cost *per breached record* was anywhere from $90 to $305 *each*
- Fines from the payment brands can be as much as $500,000 per incident

Nonetheless, the Council recognizes the challenges merchants and other entities face in this economic climate. As a result of stakeholder feedback, earlier this year we introduced a new tool for helping merchants prioritize where to focus their compliance efforts, and therefore dollars. We want to show them where they might be able to reduce the most risk, the quickest. We called this tool the Prioritized Approach to PCI DSS.

We have yet to see a data breach from an organization that was in compliance with the PCI DSS standard. If anything, the recent breaches have underscored a necessity for more vigilant monitoring of systems

The Prioritized Approach framework helps merchants identify highest risk targets, create a common language around PCI DSS implementation efforts and demonstrate progress on the compliance process to key stakeholders.

The Prioritized Approach framework was created to help merchants who are not yet fully compliant with the PCI DSS understand and reduce risk while on the road to compliance.

Comprised of six security milestones, the tool focuses on best practices for protecting against the highest risk factors and escalating threats facing cardholder data security.

We compiled the tool after considering actual data compromise events, feedback from Qualified Security Assessors (QSAs) and forensic investigators and input from the PCI SSC Board of Advisors. The framework gives practical suggestions on how to approach compliance with PCI DSS to create the most immediate impact on card data security in a merchant's environment.

In addition, the Council offers training, and additional resources designed to help organizations adopt securely protect their credit card data in a cost effective manner.

AU: *In a similar vein, how do you balance the need to react to new threats as they emerge with the need for so many banks, merchants and others to give input on standards and then implement them?*

BR: The DSS is a living document with a built in lifecycle process designed to assess the current threat landscape and incorporate any changes into future editions of the standards. This feedback loop provides a critical framework for assessing future revision, and is absolutely necessary to reflect and address emerging threats to the security of payment data.

One of the ways the Council stays current with threats and challenges in the payment landscape is through our Special Interest Groups (SIG).

SIGs are independently formed task forces that tackle specific areas of interest to their members. Each SIG is led by a member of the Council's Board of Advisors who help the groups examine the impact of different technologies and industry specific challenges on the implementation of PCI Security Standards.

The DSS is a living document with a built in lifecycle process designed to assess the current threat landscape and incorporate any changes into future editions of the standards.

SIGs are independently formed task forces that tackle specific areas of interest to their members. Each SIG is led by a member of the Council's Board of Advisors, who helps the group examine the impact of different technologies and industry specific challenges on the implementation of PCI Security Standards.

SIGs help clarify elements of the DSS that might be considered challenging, or open to interpretation for those in the payment chain seeking to secure their credit card data. SIGs will create actionable support documentation, specific instructions or recommendations in an effort to clarify how a specific technology, and the manner in which it is implemented, can affect an organization's compliance with specific requirements of the DSS. To date, four SIGs have been formed focusing on wireless, scoping, virtualization and pre-authorization. It's worth noting that these are independent groups that are formed and led by voluntary members of our Participating Organizations.

The PCI SSC Board of Advisors suggested the formation of the first series of SIGS, based on market awareness, threat mitigation and the input of our Participating

Organizations (POs). In the future, POs may also suggest or propose additional groups to focus on specific requirements of the DSS.

There is no Council staff input to the groups and they are free to make whatever recommendations they deem necessary. We've just published the first deliverable by the Wireless SIG led by Doug Manchester of VeriFone. That group came up with a Wireless Guideline document to help merchants understand how to securely implement wireless within or outside of their cardholder data environment. Through resources like SIGs we are able to ensure a variety of voices from around the payment chain are heard, and are inputting into valuable educational materials for our constituents.

In addition to work with our Board of Advisors and SIGs, the PCI SSC has commissioned PricewaterhouseCoopers PwC to review technologies such as end-to-end encryption, chip and PIN and tokenization to see what impact these technologies have on PCI compliance and whether these technologies should be made part of PCI requirements in the future. The feedback process, the SIGs and BoA structure and the PwC review, are efforts by the PCI SSC to make the standards setting process inclusive, transparent and relevant. I think we're doing a good job in this regard.

The greatest threat to payment chain security is complacency. Organizations must build in security practices into their ongoing business plans. As recent data breaches have illustrated, a checklist approach to security simply does not work

AU: *What are the greatest security threats that you see ahead?*

BR: The greatest threat to payment chain security is complacency. Organizations must build in security practices into their ongoing business plans. As recent data breaches have illustrated, a checklist approach to security simply does not work. Data security is not all about prevention; it also requires detection and monitoring.

Recent post-breach reviews by Verizon Business resulted in the discovery that:

- *Breached organizations only had 11% compliance level for Req 3 (Protect card holder data).*
- *only 5% compliance level for Req 10 (track & monitor all access to network resources and cardholder data)*

Data security is not all about prevention; it also requires detection and monitoring. If your networks are compromised, it doesn't have to follow that the data within them will be.

AU: *What are the greatest practical challenges you see ahead for PCI SSC?*

BR: The aforementioned lack of vigilance is a big problem. And the misconceived perception that the DSS cannot prevent data breaches continues to be the greatest challenge to payment card security.

AU: *What role should government play? Is there a danger that we will end up with 51 different sets of security regulations in the US alone? How should industry and governments work together to avoid such a result?*

BR: Payment card fraud is something that concerns all of us, businesses and consumers; from the pizza shop down my street to the country's largest online and bricks and mortar retailers, from a housewife who manages the weekly shopping to the businessman who conducts trade globally. For the consumer, in spite of zero liability protection under these circumstances, having your card details stolen can be an inconvenient and stressful experience. It is also very costly for financial institutions who have to reissue cards, and for businesses that can lose customer confidence and suffer damage to their reputation.

We welcome the government's interest in the topic of payment card data protection, and the Council appreciates the government's ongoing commitment to understanding and exploring the initiatives underway to contain and reduce fraud for businesses and consumers globally. We have enjoyed input from several government related entities on our Participating Organizations and have attended and spoken at many security related government events, as well as enjoy government speakers at our own Community Meetings, so we welcome the opportunity to continue to work together to continue to reduce card data compromise.

That said, for years the United States has relied heavily on the private, rather than the public, sector to rapidly create thousands of new standards every year in virtually every branch of industry as new needs arise. The PCI Security Standards Council is just one of the hundreds of "consortia" that have been founded for such a purpose.

We welcome the government's interest in the topic of payment card data protection, and the Council appreciates the government's ongoing commitment to…contain and reduce fraud

The PCI Security Standards Council is not yet three years old. Yet we have come a long way in raising awareness of the issue of securing consumers payment card data among businesses globally, along with providing a forum for collaboration amongst those in the payment chain to create a robust set of universally recognized security standards for the industry. We believe, in partnership with our Participating Organizations, we are doing a good job.

AU: *Are there other standards-related goals that need to be addressed that lie outside PCI SSC's charter that need to be addressed, and if so, by whom?*

BR: Unfortunately we don't know what we don't know. I'm sure there are, but I am so laser focused on our mission (and in conjunction with our global partners…i.e. EPC and all of the other areas of the world) we are constantly evaluating other issues that come up in other parts of the globe.

Part III: Lessons Learned

AU: *PCI SSC is generating solutions that will be relevant to an increasing number of other national and global networks that must safeguard consumer data. Electronic Health Records provide one example of data that will need to be stored and accessible to many types of parties (hospitals, doctors, insurers, and so on). Implementing Open Government goals provides another. What aspects of the PCI SSC approach are likely to provide useful models in these other situations?*

BR: The PCI Data Security Standards are built from the strongest, most fundamental best practices available to secure a specific type of (payment) data. However, we have always maintained that the principles and practices inherent within the DSS can help organizations properly segment their networks and protect any type of sensitive data you may be required to handle.

In fact, in a recent report, titled, "PCI Unleashed: Embracing PCI As A Next-Generation Security Architecture," (May 22, 2009) Forrester Research senior analyst, John Kindervag suggest that PCI should be the foundation for organizational security. From the report:

[T]he principles and practices inherent within the DSS can help organizations properly segment their networks and protect any type of sensitive data you may be required to handle

PCI: Used by millions of companies, it:

- Has been vetted
- Has established support communities actually
- Has a highly trained workforce (more or less 20,000 QSAs)
- Is easy to hire expertise around
- Non-PCI companies are looking at PCI as a best practices framework.

The conclusion he draws in the report? "PCI incentivizes good security and makes an excellent baseline framework."

AU: *What have you learned at PCI SSC that consumers or others should know that they may not be aware of?*

BR: Many consumers erroneously equate credit card fraud with identity theft, and this is simply not the case. Having your credit card number stolen is not the same as having your identity stolen. In most credit card fraud circumstances, there is zero-liability on the consumers' part. They are significantly protected from financial implications of credit card fraud. However, we recognize the issue of credit card fraud is a serious matter to businesses and financial institutions, and we are leading the charge to reduce the scope of this fraud on a global basis.

AU: *What haven't I asked you that readers should know about PCI SSC and its work?*

BR: Through the participation and input of stakeholders all over the world, and an increase focus on payment security, we are now at a point where the levels of credit card fraud are at an all time low, when measured in basis points. With the ongoing support and assistance of all in the payment chain, we hope to continue to drive this reduction, and help protect the future of payment security.