

IBM Infrastructure Solutions—PCI and Compliance in SMBs Risking Customer Information Security

Host: Michele Ogalwitz, IBM Infrastructure Solutions

**Speaker: David <Monahan>, Senior Security Consultant, IBM Internet Security
Systems, X-Force Professional Security Services**

Hello, this is Michele <Ogalwitz>, IBM Infrastructure Solutions, and welcome to this segment of our Pod cast series for SMBs, PCI Compliance in SMBs--Risking Customer Information Security.

While the emergence of the internet helped shift the balance between small and medium businesses for SMBs and the large businesses enterprises in the area of customer reach and specialized markets, there's still a gap between the two in the area of internet security. Large enterprises have the budget and resources to draw potential and existing security drafts keeping their IT shops enabled to handle security matters.

SMBs don't have the same luxury and are essentially for hackers easy targets. Visa says that more than 80% of all credit card hacks were through companies that performed fewer than 20,000 transactions per year. So while large enterprises are for hackers the big payday, it is the ease with which they can attack the smaller businesses that motivate them. Because of that stricter security measures have been driven into the marketplace to help enforce better protection for customer information.

The Payment Card Industry Data Security Standard (PCIDSS) is the main set of requirements to protect cardholder information through maintaining secure electronic commerce. These requirements called, the Digital Dozen, apply to every company, large, medium and small, and while large enterprises are aggressively driving toward needing and maintaining compliance, many SMBs are still struggling for how to effectively get down the PCI compliance path.

Joining us today is David <Monahan>, Senior Security Consultant for IBM Internet Security Systems, X-Force Professional Security Services. As a 20 year veteran in Information Technology and Security, we'll be speaking with David on the key topics for PCI Compliance.

Hi David, how are you today and thank you so much for joining us. You've been in Security Sales for quite some time. I imagine you've seen a lot in the past couple of years.

David:

Hi Michele and thanks for having me. Yes, I have been doing this for some time. I've actually been a Professional IT Consultant for 20 years now. The last 15 years I have specialized solely in Information Security. In addition, I have been involved with PCI for

5 years now, three on the information security administration and mitigating control side for PCI and the last 2 as a PCI Qualified Security Assessor.

Michele:

David, that's a lot of experience and I'd like to take advantage of that if you don't mind, and talk to you today about some key topics that would really resonate with the SMB customers that are listening. I want to stop for a minute and just focus on education. For some of our listeners who are not familiar with PCI Data Security Standards, could you give them some background?

David:

The question is: What is PCIDSS? The PCIDSS or Payment Card Data Security Standard is a global security program that was created to increase confidence in the payment card industry and reduce risk to PCI members, merchants, service providers and consumers. PCI stands for the Payment Card Industry and is generally referring to guidelines associated with the PCI Standards Council. This Council is essentially an independent body formed to drive security standards for payment card account security. The founding members include American Express, Discover, JCB, MasterCard and Visa. The primary function of the group is managing the ongoing evolution of the payment Card Industry Data Security Standard.

Let's talk a little bit about the history of the PCIDSS, if you will. A few years back, essentially all of the various card members had their own version or their own Data Security Standard. The great thing that I like to say about standards is that there is usually more than one to salute. This created confusion in the marketplace. In addition, it created some issues with respect to payment card transactions and security compliance for merchants and service providers who actually processed more than one card brand.

Visa first developed the Cardholder Information Security Program (CISP) in 2001. MasterCard and other card providers started developing separate criteria as well. In 2004, Visa and MasterCard formally agreed to combine their efforts and they created the PCIDSS. The most recent version of this standard is PCIDSS V1.1. That is the one that is currently being enforced. In addition, in October of this year, a new version of that standard will be released to the public and that will be V1.2.

Let's talk a little bit about the players or those parties who are involved in payment card transaction processes. If we go to the next slide, what we'll see the various entities who are involved. First we have the Card Companies, or the Card Member brands if you will. Those members can include entities like: Visa, MasterCard and American Express. Then we have the merchants. The merchants are those that we're all familiar with and those are the ones who actually accept payment cards for point of sale transactions and e-commerce. Then we have the acquiring banks and those are the entities that actually acquire or gather up those transactions and provide processing services for the merchants, and they usually do so for a fee. In between we have Service Providers who also help to

<sell gas> with respect to actually providing the conduits and gateways for processing payments and they also assist with the settlement process on the back end.

The Payment Card Industry Data Services Standard or PCIDSS for short is essentially made up of 12 different sections. This next slide that we're looking at refers to the PCIDSS requirement; aka, the Digital Dozen. As you can see, there are 12 individual sections that are also broken up into higher level concepts. The first concept is basically the direction to build and maintain the secured network. The next concept involves protecting cardholder data; the third is maintaining the vulnerability management program; the fourth is to implement strong access control measures; the next one is to regularly monitor and test networks; and the following one is to maintain an information security policy within the organization.

Michele:

You know those standards seem to be pretty comprehensive, David. We've heard a lot about the digital Dozen and, in particular, most recently in the first half of this year we've heard a lot about Section 6.6 which really speaks specifically to the Web application security? There was a deadline of June 30/08 to become compliant. What should our SMB clients who are listening to this need to know about that section and the June 30th deadline?

David:

Yes, Michele, that is correct. Essentially what that is referring to is Section 6.6 of the PCI Auto Criteria or what is also known as a Report on Compliance Auto Criteria, sometimes known as the ROC. There are still a large number of Web applications that contain common vulnerabilities that are allowing hackers to gain access to company confidential information as well as an organization's confidential customer information. Section 6.6 is really a direct response to the broader security challenges and it gives an attempt to better protect credit card information from being compromised by insecure Web applications, or point of sale applications.

Beyond the obvious security implications, Organizations that do not address Section 6.6 by June 30th of this year, which has come and gone by the way, can be immediately found to be non-compliant. In addition, they can face large fines and will lose their ability to process credit card transactions.

Michele;

That really clarifies quite a bit. We know that particular deadline has gone past and there's been a lot of focus around becoming PCI compliant. It doesn't seem like everyone it affects knows it affects them for some reason. Can you just show us and really clarify, who does PCIDSS requirements apply to?

David:

The question is: Who does PCIDSS really apply to? The short answer is that it applies to everyone who processes credit card transactions. The formal answer is that all merchants and service providers that store, process, or transmit cardholder data must be compliant

with the PCIDSS. Some of the Industry Verticals that are commonly found within this category include retail businesses, the hospitality industry, transportation and, of course, financial services, healthcare, education and government. One little known fact is that the US and State Governments are actually some of the biggest users of credit cards. Let's talk, once again, about some of the players who are involved here.

Essentially, what we're mostly concerned with, at least with respect to compliance, are the merchants and service providers. PCIDSS and PCI Security Standards Council in conjunction with the Card Brand Members are actually making some determinations about how to classify who or what level they may fall into with respect to credit card processing and transaction processing.

The Merchant PCI level will be dependent upon the number of transactions that take place annually and the levels are defined as follows.

- The Level 1 merchant is considered to be processing more than 6M transactions per year.
- Level 2 can process between anywhere from 1M to 6M transactions per year
- Level 3 can process between 20,000-1M per year
- Level 4 processes less than 20,000 transactions per year

Service providers actually play an interesting role and are a little bit different than merchants. They are, however, still required to be compliant with PCIDSS and they must validate that compliance. The formal definition for the PCI glossary of terms for a service provider is:

- Any business entity that is not a Card Payment Brand Member or merchant who is directly involved in the processing, storing, transmission or switching of transaction data and cardholder information.

As you might expect, Service Providers have various levels as well. Level 1 Service Providers are all Processors and Payment Gateways. Level 2 is any Service Provider not in Level 1, but Level 3 is any Service Provider not in Level 1 who stores or processes less than 1M accounts or transactions annually.

On the next slide we see the Compliance Validation Requirements that have been imposed by Visa. This is a fairly complicated slide but the (inaudible) is that it can be very straightforward once we've been pointed out. Essentially, all merchants and service providers are required to perform an annual assessment that assesses and helps to validate whether or not they are compliant with PCIDSS. There are some differences though.

For example, a Level 1 merchant and a Level 1 service provider or a Level 2 service provider are required to have an annual assessment performed by an outside entity or a qualified security company that specializes in doing independent assessment for PCI compliance. A Level 2, 3, or 4 merchant or a Level 3 service provider is also required to be on-compliant annually and they must also do an assessment. They can, however, fill

out what is known as the Self-Assessment Questionnaire. Essentially, though, they are still required to be compliant with all aspects of the PCIDSS and to validate that compliance in accordance with the PCI Report on Compliance Auto criteria.

There are some additional requirements as well. For example, all entities are required to have a Quarterly Vulnerability Scan performed with their internet-facing architecture and, in addition, have an Annual Penetration Test of that architecture.

Michele:

David, that seems like quite a bit of work and activity that needs to be done and maintained and that's just for Visa. I believe that there are separate validation requirements that narrow this but are slightly different for both MasterCard and American Express. Is that correct?

David:

That is indeed correct. I'm glad that you pointed that out.

Michele:

This doesn't seem to be very straightforward. I would expect, though for larger enterprises, this is a little bit easier based on the resources that they have, but for some of the SMBs this could be a bit challenging. It's not a one size fits all kind of thing; it's not that simple and straightforward as people would like it to be.

David:

That is indeed correct. In addition small, medium sized businesses usually do not have the same level of resources or technology available to them or the subject matter or expertise that the large companies or organizations may have.

Michele;

That brings me to a thought about facts and fiction. There is a lot of fact running around out there, but there is a lot of fiction as well about PCI compliance. One that always gets me is that it's going to go away if people just wait it out. The other is that a third party is actually doing the card processing and that all the SMB or the client or the SMB business is doing is accounting and the reconciliation and they don't need to be compliant. These kinds of false beliefs can really be detrimental to an SMB business if an audit comes around or a security breach happens. What are the myths about PCI out there that we should be looking at?

David:

Michele you make some very good points there and have drawn some very good conclusions as well. There are a lot of myths, if you will, with respect to being PCI compliant. You'd be surprised. They actually cut across all aspects of the marketplace for both large organizations and small organizations. The top five that I like to refer to as the myths of PCI compliance can be seen on this slide.

- PCI compliance is hard and no one is doing it. That's a good one but, essentially, it is completely untrue. PCI compliance is not a straight forward endeavor and is not as complex as it is very comprehensive and the requirements are highly granular; however, you must be compliant with the PCIDSS and everyone is doing it, or at least pursuing compliance.
- The myth that PCI compliance will the company secure. There have been very well known data breaches that have occurred over the last few months and years that have involved companies that actually have been PCI compliant; however, they have suffered a compromise from an unfortunate incident. The interesting thing is that the more due diligence that you provide and the more that you salute PCIDSS compliance actually reduces your liability and risk if and when a compromise occurs.
- This bullet is one of my favorites as well. It is the concept that inscription is scary and very difficult. The underlying technologies involved with inscription are very complicated and involve some advanced mathematics. However, they have implemented some very interesting twists, if you will, or some graphical user interfaces or other things that can make it fairly straightforward to implement.
- The fourth myth that I would like to address is that I don't process enough credit cards to worry about PCI. The facts are that even if you process one card a year, you must still be compliant with all the requirements.
- The last myth and this is one I see a lot, is that there is a tool or a single point solution out there that will make me compliant. Nothing can be further from the truth. If you hear vendors telling you this, you need to be suspicious. PCI compliance involves more than just technology; it also involves industry best practices, information security policies, processes and procedures and a commitment by upper level management to actually become PCI compliant.

Michele:

Those myths can get a lot of people in trouble. I'm sure that you are now going to start ignoring anybody who says those types of things, but it becomes important for us to understand the myths and understand how important PCI compliance is because there are consequences to not being compliant. Let's talk enforcement for a minute. Many people don't know that the PCI council doesn't actually do the enforcement of PCIDSS requirements or do they? Help us understand the difference between the PCIDSS as a standard versus the enforcement of their requirements.

David:

That's actually an interesting concept; the standards versus enforcements. Essentially the PCI Security Council is an independent standards body that was formed by the various members in the industry. Essentially, they cannot impose upon merchants or service providers any fines or penalties or any other punitive actions. What they do is approach

and engage their acquiring banks and other processing entities and hold them accountable for the subsequent customers to be compliant with the PCI standard.

What happens is that the PCI Standards Council can actually levy direction and, in addition, punitive action against the Acquiring Banks and other entities and that essentially that rolls downhill to the merchants and service providers. Remember that the PCI Security Standards Council is an independent body to govern the Global Security Standards for the payment card industry.

Michele:

That's a very interesting distinction. Basically, they beat up on the service providers and that way they actually impose the fines for the (inaudible) so that's how they make sure that everybody plays the game the way they're supposed to.

David:

Actually, it's the Acquiring Banks, Michele. You had the right idea.

Michele:

Acquiring Banks--right idea! Now that we've qualified standards versus enforcement, let's talk about compliance versus validation because the earlier chart that you talked about with Visa about their validation process and what you have to do to validate, is different from actually being compliant. Help us through that thought process.

David:

There's quite a bit of confusion about what compliance entails and also validation. The way to keep these things separate and distinct in your mind is to think that compliance is required by all entities that process credit card transactions. Compliance is really spelled out by the Data Security Standard itself. How you validate that compliance is actually sort of the measuring stick. That is done by using the Report on Compliance Auto Criteria and as has been stated before, everyone who processes credit card transactions wants to validate or measure themselves against the PCI requirements for Auto Criteria Compliance.

Michele:

I did have a PCI fact that I believe is on your chart as well and what it talks about is most merchants, especially 1-3, are past the deadline for validation within the US and fines are actually being given out for that failure. This is an area that they need to know and understand the difference between the validation and actual compliance.

David:

For example, small to medium sized businesses may be able to assert their compliance or validate their compliance with respect to PCID assessments by simply filling out what's known as the Self-Assessment Questionnaire. Most large organizations are required to bring someone in from the outside who is an unbiased third party and a qualified security company and have that unbiased entity actually perform that assessment for them. Some of our small to medium business customers are actually having us come in to do this for

them. We work with them to through the entire 70-80 pages of the entire PCI Report on Compliance around the criteria.

Michele:

That's because we're a QSA, isn't it?

David:

That is correct. We're a Qualified Security Assessor and we're also a Qualified Security Company.

Michele:

That's great information to know, that you have to have a QSA in place because if you don't, something can happen like a security breach or an audit. Then the world turns upside down, and I don't know about you, but one of the scariest words in the English language is "audit". I have a chart here that talks a little bit about why customers fail PCI audits. It is really interesting to note that 7 out of the 12 PCIDSS requirements areas have the highest assessment failure rates. Yes, that's a bit scary for folks really to be able to take a step back and say: Am I even doing the right things in these areas? What are some of the trouble spots for SMBs that they need to look at when they're going down the PCI path so that they don't fail the audit and so that they're covering all of their bases as they move forward? What are the trouble spots or the sticking points?

David:

Essentially, you're correct. You can see the slide you're referring to: The Top Reasons Customers Fail PCI Audits. They're all valid and they all play an important role and they all have some level of involvement with respect to customers failing or not being compliant with PCIDSS.

Some of the PCI compliance sticking points or some of the issues that I've seen as I go from environment to environment really amount to be some of the same things and they are reflected in the previous slides and numbers, if you will, for failed assessments.

- The first is the lack of knowledge as to where all the sensitive PCI information is. Most of the customers we have seem to think they have a very good idea of where this information is stored or where it might be contained. Usually, though, after we've done some discovery and some investigation upon arrival, what we find is they don't know where all the data is and we even uncover a few surprises. In order to actually secure or meet the DSS requirements you have to understand where all this instant data is. In that way, you know how to manage it properly and put in the proper controls.
- Another area, or potential sticking point, is the storage of prohibitive cardholder data. PCI sensitive information is comprised of two forms: that which you can store and must be stored in a protected format by using such things as encryption and there are also data types that you can never store and hosts the transaction authorization process. A good example of that is the magnetic stripe data that is

contained within the credit card itself. In addition, I find that there are a lot of environments that have a lack of proper network segmentation. In most environments, historically, their IT system environments have actually evolved over time and they have PCI systems co-mingled with non-PCI systems. The important thing to note here is that if you have an environment where you have actually mixed PCI and non-PCI systems that all aspects of PCIDSS apply to all systems. This can actually be very cost prohibitive and overwhelming to try to assess or remediate.

- Another area is the lack of file integrity monitoring. What that means is that there are system files, encryption files and other sensitive information files that must be monitored for possible tampering or compromise. This is done by using Call Integrity Monitoring Technology. It is essentially a mathematical hash that's performed on the file and directory structures containing this information and then any change to those file and directory structures can be detected using File Integrity Monitoring.
- Another area where we see a lot of issues around involve the use of production or real customer data to test these systems when they're being developed. That is essentially very frowned upon with respect to PCIDSS.
- Some of the other issues we run across are lack of proper encryption, lack of proper logging, and log reviews via Security Administration practices, the lack of separation of duties between those who write applications and those who actually test them and, also, the failure to label cardholder media as confidential.

What are the compliance consequences or non-compliance consequences, if you will? We're actually getting to the heart of the matter here. If you are non-compliant and a breach occurs, merchants and service providers have a liability for the Acquirer's Bank's losses and card reinsurance costs. These can be staggering.

In addition, restrictions imposed by card companies can prohibit the future use of credit cards and credit card transaction processes. Additional costs can be levied due to the liabilities and cost associated with investigative and legal aspects and repayment of all total losses may actually exceed the ability to pay and cause total failure of the organization. Indeed, some of the organizations and businesses that have encountered or endured a compromise have actually filed bankruptcy.

Other potential consequences include a damaged brand reputation, negative publicity in the marketplace and, essentially, a loss of customers.

Michele:

David, that brings up a very good point when we look at some of these consequences. We've got a few fictions in that area as well, right? For instance, some business leaders believe that unless they actually have a security incidence, they won't be fined or that it's actually cheaper to pay the fines than to meet compliance. So, it's okay to be non-

compliant if you don't have a security breach and even if you do, the fines are enough for you to be able to handle. How true is that?

David:

Well, that's a good question as well. What are the real risks if companies don't comply with PCI? First, for your small to medium sized business you are facing unforeseen or unbudgeted fines and penalties. This can have a severe impact on your business. On this next slide we see description and penalty summaries for the various card brands. Keep in mind that if you are processing more than one card, these could actually be accumulative, if you will.

For example, for Visa, if you're a merchant and you are found to be non-compliant, the Acquiring Band can start to fine you for the first violation \$50,000. In addition, there can be monthly penalties and they can also raise your transaction fees. As you can see by this slide MasterCard, American Express all have plans and programs to deal with this issue. In addition, if you are breached and found to be non-compliant, you can subject to a half a million dollar fine right off the bat.

Michele:

Those seem like some pretty big risks. It doesn't sound like just paying the fine is going to help you out there at all. You could be out of business before you pay all your fines. Especially in the case of SMBs, who I would presume, those fines would really cut into their profit margins.

David:

You bet and most SMBs are very lean and run very lean and mean and don't essentially have the resources to deal with unforeseen budgeting requirements.

Michele:

One thing we've also been seeing is that they're not really seeing the benefits of this. They just don't see its potential, in addition to all the other myths, of the benefits of being PCI compliant. They don't see a return on the investment as they go down that road. Can you talk a bit about the benefit of being complaint and the return on the investments they're going to make in this area?

David:

It's really easy to lose your focus and be drawn in by the potential impact of all these proposed fines and penalties. One of the great things about becoming PCI compliant is essentially that you're addressing best practices for information security and there are actual benefits of doing that and you can actually measure considerable return on your investment.

The next slide is called: Benefits of Compliance. We will address five different categories of what potential return on investment could look like. For everyone, and that includes most of us who carry credit cards themselves, it essentially reduces the risk of

potential unauthorized exposure of sensitive information including your identity and your cardholder information. After awhile you see increased confidence in the payment card industry. No one likes to see headlines on a day to day basis about another data breach and issues that surround that.

Also, there's this concept that we referred to earlier called Safe Harbor Protection. Let's say you have gone through your PCI compliance effort and you've done all the due diligence and some unforeseen incident occurs, what you will find is that the penalties and risk in the organization are significantly reduced if you have actually become compliant and instituted the proper programs, technology and processes.

The next group is essentially members of the brand, if you will. Essentially, what the Card Brand members want to do is try to protect their reputation as a business.

Next, we have merchants and service providers and what they want to do is try to gain a competitive edge, increase revenue and approve bottom lines, maintain positive image and protect customers. If they are compliant, we can achieve these objectives as well. Across the industry we can encourage good security amongst our neighbors and we can also find that PCIDSS will actually help an organization apply with governmental privacy requirements. As a matter of fact, some State governments have actually lifted whole sections from the PCIDSS and included it in their Privacy Legislation.

Finally, last but not least, we are all consumers if we carry these credit cards around with us and use them. We want to make sure that we safeguard the information for consumers and help prevent identity theft.

Michele:

Those are some really key points and we want to talk a little bit now about the challenges of getting PCI compliance. Now that we understand the benefits, now that we understand the rest when it's not achieved, let's talk about how to get compliance when a company is out of compliance and they know that or they have actually failed an audit. What do they need to be thinking about for remediation?

David:

I like that term remediation, Michele, because it really gets to the heart of the matter of being able to move your organization or business into a posture or best practices that you need to be in. What I like refer to is that remediation is like "eating the elephant". What happens is when you actually perform, either yourself as an organization, is you bring in an outside entity and he will assess your organization and your processes and technology with respect to PCIDSS compliance. No one that I've heard of can actually be non-compliant immediately out of the gate. What happens is that you find gaps or areas where you are non-compliant. These gaps must simply be articulated and then a high level project plan is developed around filling in those gaps in trying to move that organization towards compliance. The analogy I like to use is that it is like "trying to eat an elephant". Well, how do you eat an elephant? An elephant is a pretty good size, it's pretty big and some of the projects and compliance gaps that we find across an

organization are numerous and they're not small. What you have to do is approach this like any other large scale problem, divvy it up into bite-size chunks and once you do that, you have to organize and formulate a program and a plan within the organization to try to become compliant by remediation of a gap, if you will. Some of the concepts that you must address in doing this is that the effort must be well planned. You must also have a dedicated staff to be successful and that staff needs to be dedicated to the entire practice or process of becoming compliant from the highest levels of management in the organization all the way down to the foot soldier at the bottom of the food chain, if you will.

Also, compliance or remediation must be done in phases and steps to allow for sanity checks for each task. In addition each task must be re-evaluated with respect to PCI compliance. Accountability must be assigned and enforced for doing that.

All remediation starts with behavior changes for the employees as well as across the organization. As we all know, change can be somewhat difficult and uncomfortable for people to embrace but the change must be well defined and must be well trained, must be implemented and deployed and it must be enforced on the back end. Having a very well defined structure for doing so can help to ensure the successful remediation of PCIDSS gaps and non-compliance. Once you have completed this entire effort, remediation can have a return on investment if it's well planned.

In essence to achieve compliance and sustain it, you must be willing to do several things but before I go into that, it's important for folks to understand that it's definitely and discreetly difficult at times to actually become compliant with PCIDSS. It can be a gargantuan step for an organization, but once you become compliant it's actually a little bit more straight forward of a process to maintain that compliance. In order to do that, there are some other points that we must discuss.

You must be willing to see this as a living activity, not a slice in time or a snapshot. It must become a part of the overall business process. One of the prime directives of businesses is to manage risk, and this is no different.

In addition, you must be capable of moving the business to a best practices model. If you have been following a best practices model, then PCIDSS can make a lot of sense to you just like any compliance with any other regulatory or industry requirement.

As well, catalyzing changes and behaviors so you can better achieve overall compliance across the organization is another point.

Finally the last point is allowing changes to be introduced into the environment that will help the organization grow in order to help the individuals within that organization to take ownership for them.

Michele:

David, as you were talking about what you needed to do to meet compliance and sustain it, it does sound like a it's a lot, but I think that what you're saying is that it's something you have to go through. Once you go through it, it's a lot easier to maintain it than it is to get there. You have to get through it first to get to the relatively easier side of things. Is that right?

David:

That's correct.

Michele:

As part of the remediation process, I'm presuming that you need to implement new policies and solutions. What should an SMB look for in a solution to help them to get down to PCI compliance habits? I'm assuming there's no silver bullet to this.

David:

You are indeed correct. Once again, that's why I caution people against resisting vendor advertisements of being able to provide you with a single technology point to actually help you achieve compliance. Compliance is achieved with solutions, tools, processes and information security best practices. If you take away any one of those elements and it's going to be difficult for you to achieve your objective.

Solutions are also part of the overall effort to achieve and maintain compliance for the long haul. Once again, getting compliance can be a very gargantuan step. Once you are there, maintaining compliance can be very straight forward. The solutions can only come from a collaborative effort across your organization with discipline verticals, if you will, and also in partnership with, for example, other outside entities. Some of these entities can include your compliance area within the organization. Most companies or businesses actually have people that are dedicated to managing risk and focusing on compliance with regulatory and other industry standard requirements. You also have to involve your IT organization and since this has a significant impact on your ability to conduct business, you must also engage your business leadership as well.

You should also look to engage a Qualified Security Assessor or Company. These are entities that have been deemed and certified by the PCI Security Standards Council to actually provide this expertise and service.

Last but not least, you also have to engage all your Service providers who may be providing products and services that actually affect the overall security and safety of PCI and confidential information.

Michele:

You know, David, as you were talking about what we should be looking at from a solution perspective, a couple more of those faults came to mind especially around the vendor comment you made earlier. We have a lot of businesses that are under the impression that some vendors would not sell them a non-PCI compliant device or

application or if a vendor tells them that a device or application is PCI compliant that they can trust that. It doesn't sound like that's the case based on what you're saying here.

David:

That is indeed correct, Michele. There's some serious confusion about that entire subject. A lot of vendors are saying that if you buy our particular technology and implement it, you will become PCI compliant. Even if that particular vendor has certified their particular application or specific technology with respect to application security requirements; if it has been implemented in an insecure, non-recommended or non-supported configuration, you can immediately take your business or your organization out of compliance with PCIDSS.

Michele:

That's a very good point and I'm hoping that a lot of our folks listening to this call are going to walk away and realize that there is no silver bullet. It's bits and pieces and the solution is only part of the way to get down the compliance path.

IBM is a vendor that really does provide several of those pieces that you need from a services and a hardware and software perspective. We have some unique capabilities. Would you care to share with us some of IBM's capabilities to help our SMB customers down the PCI road?

David:

You bet. As you can see by this next slide, there are numerous IBM services, software and hardware which will help you address PCI compliance requirements in your environment. The important take away from this is to see that we actually provide technology in service solutions to cover all twelve of the PCIDSS Digital Dozen, if you will. In addition to that, IBM ISS is one of the three companies within the world that can provide PCI Consulting Services as a Global Company. In addition to that we also work with a wide variety of clients from small to medium size businesses all the way up to the largest companies that you can think of.

Michele:

David we have accomplished so much today. This has been a real education, a real enlightening and informative session, at least for me and I'm hoping for the folks that are listening. Any last bits of advice for our SMB customers who are listening to this and really looking at PCI differently now and compliance, in particular, for PCI?

David:

I know that pursuing compliance with any kind of regulatory process or requirement can be overwhelming and can actually create lots of anxiety. The important thing to know is that PCI compliance is something that is do able and that organizations are undergoing the process to actually address the gaps in their organization and in their business to try to become compliant.

There's an old saying that I like to refer to and it goes like this: "A rising tide floats all boats". What I've found as organizations launch into this process and head down the road towards future and compliance, it raises the awareness across the organization with respect to industry best practices for information security and protecting critical corporate assets and, certainly, PCI sensitive information that includes cardholder information for customers and other information of that type is a critical asset of the business and it requires the same level of protection that you would for any other asset as well. In addition to that, what I've found is as awareness spreads throughout the organization, people tend to take ownership and become more concerned about protecting the business and doing the right things.

Michele:

That's a very, very good piece of advice. Thank you so much, David, for lending us your vast amount of knowledge and expertise around PCIDSS and how to be compliant. This was a great session and thank you for joining us.

I'd like to thank all of you who are listening to this for joining us for this segment of the IBM Infrastructure Solutions Pod Cast Series for SMBs, PCI Compliance and SMB. For more information about PCIDSS and IBM Solutions to help you achieve and maintain compliance, you can go to one of the three Website addresses on the last chart of this presentation or you can go to www.ibm.com/expressadvantage/security. Thank you for joining us and have a wonderful day.