

4TH ANNUAL 2008 VERIFONE RETAIL PAYMENTS CONFERENCE



ARTS PCI Best Practices Initiative

Cy Young
Chair
ARTS Board of Directors



- Association for Retail Technology Standards (ARTS)
 - The Standards Division of NRF
 - Members (204) are Retailers and Vendors
 - International, over 40% of members
- Mission
 - To enable the low cost, rapid deployment of technology in retail by reducing integration efforts through platform independent, vendor neutral standards.

WWW.NRF-ARTS.ORG

ARTS is one Division of NRF



ARTS Membership



- **Members**

- 207 Total
- 125 Vendors
- 82 Retailers

- 46% International

- **New in 2008**

- Nordstrom
- Reliance Retail(India)
- Publix
- Neiman Marcus
- Teradata
- Torex
- IKEA
- Staples

ARTS Evolution Highlights



- Jan 1993 - ARTS organized**
- May 1994 - ARTS Expands Internationally**
- Jan 1996 - Data Model Published**
- Oct 1998 - UnifiedPOS organized**
- Jan 1999 - ARTS is acquired by NRF**
- May 1999 - ARTS XML begins**
- Sep 2003 - Conformance Testing**
- Jan 2004 - ARTS publishes first RFP/ITT**
- Jan 2005 - IP Policy to protect implementers**
- May 2006 - SOA Support project**

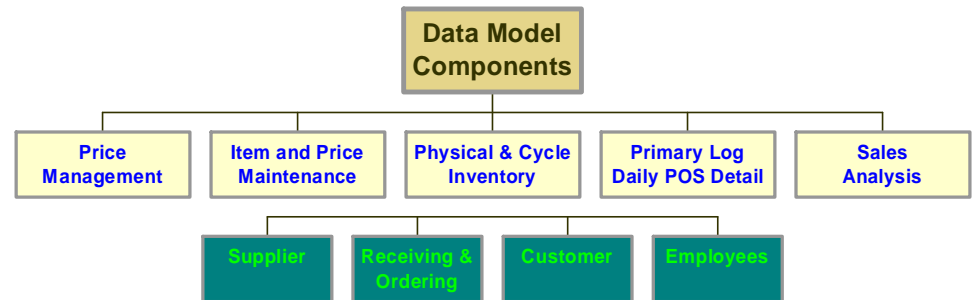
ARTS is Unique



- Retailers and Vendors working Together
- Strong Retail leadership
- Focus on “Inside the Store” but connect the enterprise
- Truly International
- Continually Strive for Cooperation
- One Mission for 14+ Years
- Conformance to Protect Investment

ARTS Standards

2008 VeriFone
Retail Payments
Conference



- Data Model
- UnifiedPOS Standard Device Interface
- ARTS-XML Standard XML Messages
- Standard Requests for Proposal (RFP's) (ITT's)

ARTS Latest Initiative



- **PCI** is the a major diversion of focus for the retail community
- **PCI Standards** are complex and the enforcement of them is seemingly arbitrary
- Most retailers are reluctant to share publically their PCI efforts
- ARTS and PCI Knowledge Base are creating a growing list of **PCI Best Practices**
- What you don't know **CAN** hurt you!

PCI Knowledge Base



- The PCI Knowledge Base is an independent community of persons who *Know PCI* and how to achieve compliance with the PCI security standards from the ground up. The Knowledge Base includes merchants, assessors, banks, payment processors, consultants and vendors of payment systems and security technology.
- The PCI Knowledge Base (www.KnowPCI.com) is dedicated to facilitating the exchange of experience and advice relative to the Payment Card Industry security standards and other related data security and privacy laws. Our members include merchants of all levels, as well as security assessors or auditors, and developers of payment processing systems, security products and many different types of service providers.

PCI Standards vs. Best Practices



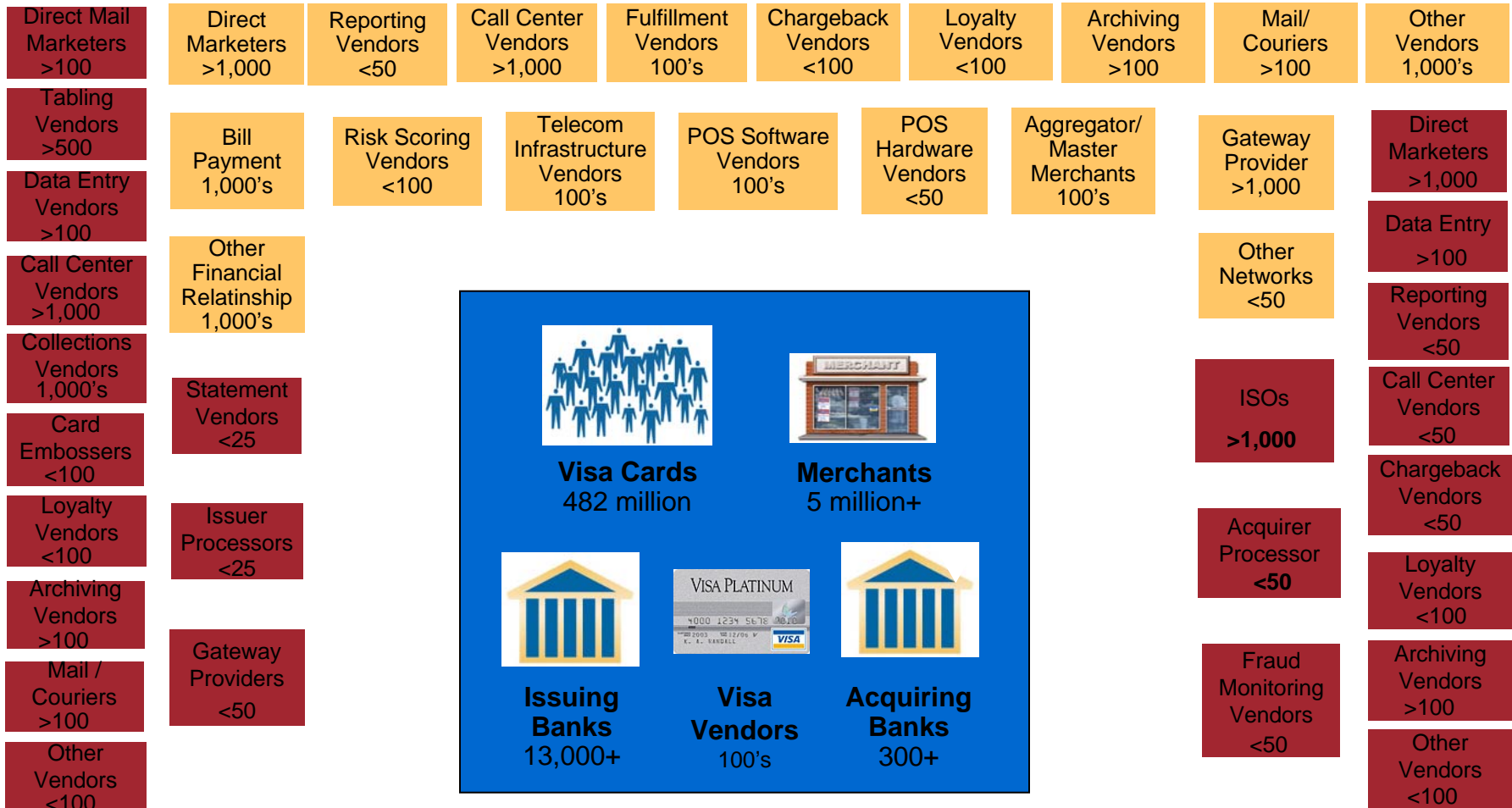
The PCI Standards: Tell merchants WHAT to do to secure credit card data.

PCI Best Practices: Tell merchants HOW leading firms do this.

These Best Practices are based on the experiences of leading merchants, and advice from PCI Assessors & other experts.

Source: PCI Knowledge Base, September 2008

PCI is Required for Millions of Merchants and Service Providers, Globally



Source: Numbers are taken from Visa, April 2007

“Digital Dozen” PCI Standards: Not a “Safe Harbor” Against Breaches



Build and maintain a secure network.	<ol style="list-style-type: none"> 1. Install and maintain a firewall to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data.	<ol style="list-style-type: none"> 3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a vulnerability management program.	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement strong access control measures.	<ol style="list-style-type: none"> 7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks.	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy.	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security

Source: PCI Security Standards.org, September, 2007

Who Has to Comply? PCI Levels for Service Providers



Service Provider Level	Qualification of Level	Validation Action	Validated By
1	All VisaNet processors (member and Nonmember) and all payment gateways	Annual On-Site PCI Data Security Assessment	Qualified Data Security Company
		Quarterly Network Scan	Qualified Scan Vendor
2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually.	Annual On-Site PCI Data Security Assessment	Qualified Data Security Company
		Quarterly Network Scan	Qualified Independent Scan Vendor
3	Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 Visa accounts/transactions annually.	Annual Self-Assessment Questionnaire	Service Provider
		Quarterly Network Scan	Qualified Independent Scan Vendor

Source: PCI Security Standards.org, September, 2007

Most Merchants, Banks & SPs Have to Use SAQ – D as They Store CCD



PCI becomes much easier for merchants with NO cardholder data. This is driving more merchants to consider payment outsourcing. However, this is not cheap.

SAQ - A

CNP (Ecommerce/MOTO) Merchants, with all outsourced cardholder data storage, processing and transmission. (No face-to-face merchants)

SAQ - B

Merchants who process cardholder data via imprint machines or standalone dial-up terminals only.

SAQ - C

Merchants whose payment applications systems are not connected to other systems internally or on the Internet.

SAQ - D

Merchants who do not fall under the types addressed by SAQ A, B or C, and all service providers defined by a payment brand as eligible to complete an SAQ.

New versions of the SAQs are expected before YE 2008, which will be based on the PCI 1.2 standard.

What Data Has to be Protected?

PCI 1.2, Oct 08 Will Not Change This



You have to protect Cardholder name, service code & expiration date if the PAN is stored.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

Applies to: “Any network component, server, or application that is included in, or connected to the cardholder data environment.” That’s broader than many think.

The PCI Top Five Reasons Merchants Fail PCI Compliance



- 1. Storage of Track Data (and other sensitive data)
- 2. Missing or Outdated Security Patches
- 3. Vendor-Supplied Default Settings and Passwords
- 4. Web Application Vulnerabilities -- SQL Injection
- 5. Unnecessary and Vulnerable Services on Servers

You have to score “100%” on the PCI DSS assessment (or self-assessment). Every requirement must be satisfied.

If you “cheat” and your acquirer finds out, or if you are breached (which is one way they find out), then you automatically become a “Level 1” for the next year, and need to hire an Qualified Security Assessor (QSA) to review you.

Source: Visa, April 2007

Best Practice: Avoid Taking the Checklist Approach to PCI



Tactical Products

- Firewalls
- Encryption
- Anti-virus
- Access controls
- App. Firewalls
- Intrusion Detection
- Vulnerability Scans
- Password Mgmt
- File Config. Mgmt
- Security Policies

Strategic Products

- Data Loss Prevention
- Enterprise Key Mgmt
- Endpoint Security
- ID & Access Mgmt
- Application Security
- Intrusion Prevention
- Threat Modeling
- Single Sign-on
- Event Correlation
- SIM / SEM

Source: PCI Knowledge Base, May 2008

PCI Standards: Cover Dozens of Different Security Technologies, But...

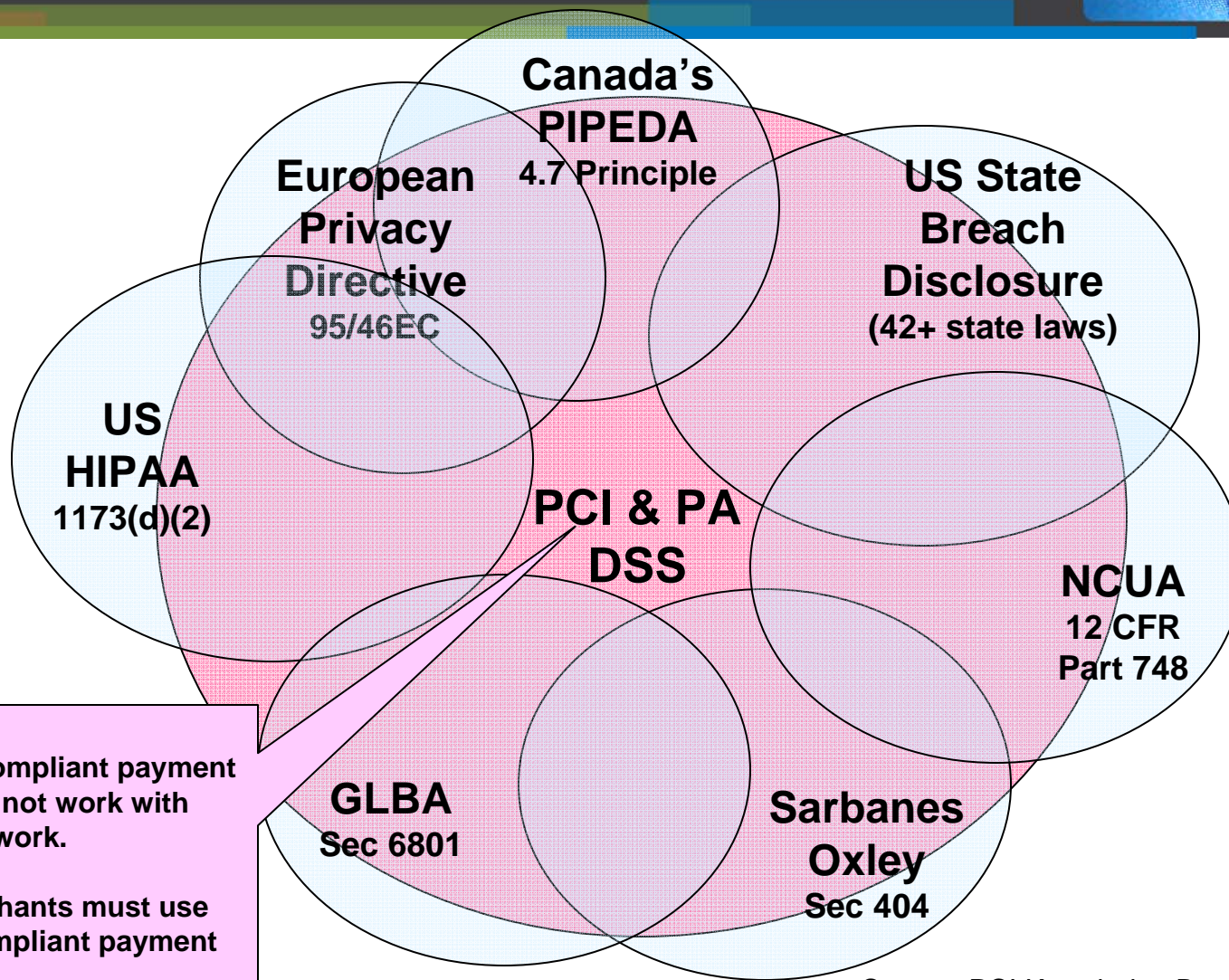


- **Req 1: VPNs, file transfer, network firewalls, personal firewalls**
- **Req 2: Wireless security, network access controls, infrastructure security**
- **Req 3: Encryption, key management, data masking, DB monitoring, data privacy, secure storage, data backup**
- **Req 4: Wireless, WIFI, PKI, secure email**
- **Req 5: Anti-virus, anti-spyware**
- **Req 6: Application development tools, patch management, application firewalls**
- **Req 7: Access controls, authentication, AAA software**
- **Req 8: Password vaulting, Identity and access management (IAM), two-factor authentication**
- **Req 9: Video monitors, smart cards, media destruction, shredders**
- **Req 10: Security event management, security log analytics**
- **Req 11: Vulnerability management, Intrusion detection/prevention**
- **Req 12: Security Info. Mgmt (SIM), disaster recovery, security training**

PCI does not address Virtualization, SaaS, Tokenization and other “emerging” technologies. PCI 1.2 does add “Wireless IDS” to the list.

Source: PCI Knowledge Base, May 2008

Best Practice: Use PCI as an Enterprise Security Control Template



PA DSS Dates:
10/1/09 – Non-compliant payment applications will not work with the payment network.
7/1/10 – All merchants must use only PA DSS compliant payment applications.

Source: PCI Knowledge Base, September 2008

The Scope of PA DSS includes ALL Merchants & SPs down to Level 4



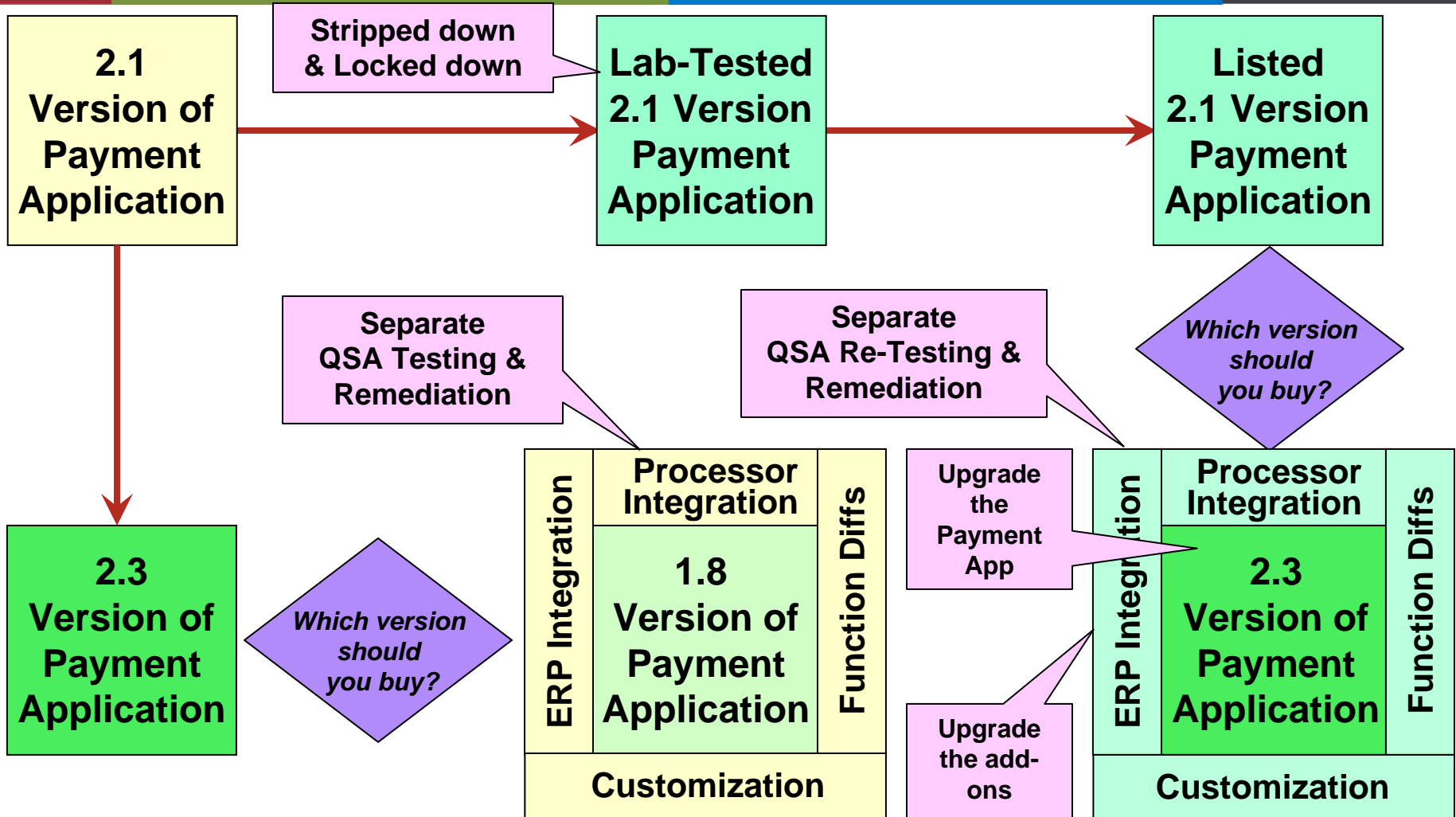
<i>Phase</i>	<i>Compliance Mandates</i>	<i>Effective Date</i>
I.	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (“VNPs”) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/08
II.	VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PABP-compliant applications	10/1/08
IV.	VNPs and agents must decertify all vulnerable payment applications	10/1/09
V.	Acquirers must ensure their merchants, VNPs and agents use only PABP-compliant applications	7/1/10

Until this year, PABP was a “best practice” and now it more broadly applicable than PCI DSS and has less built-in flexibility than PCI DSS.

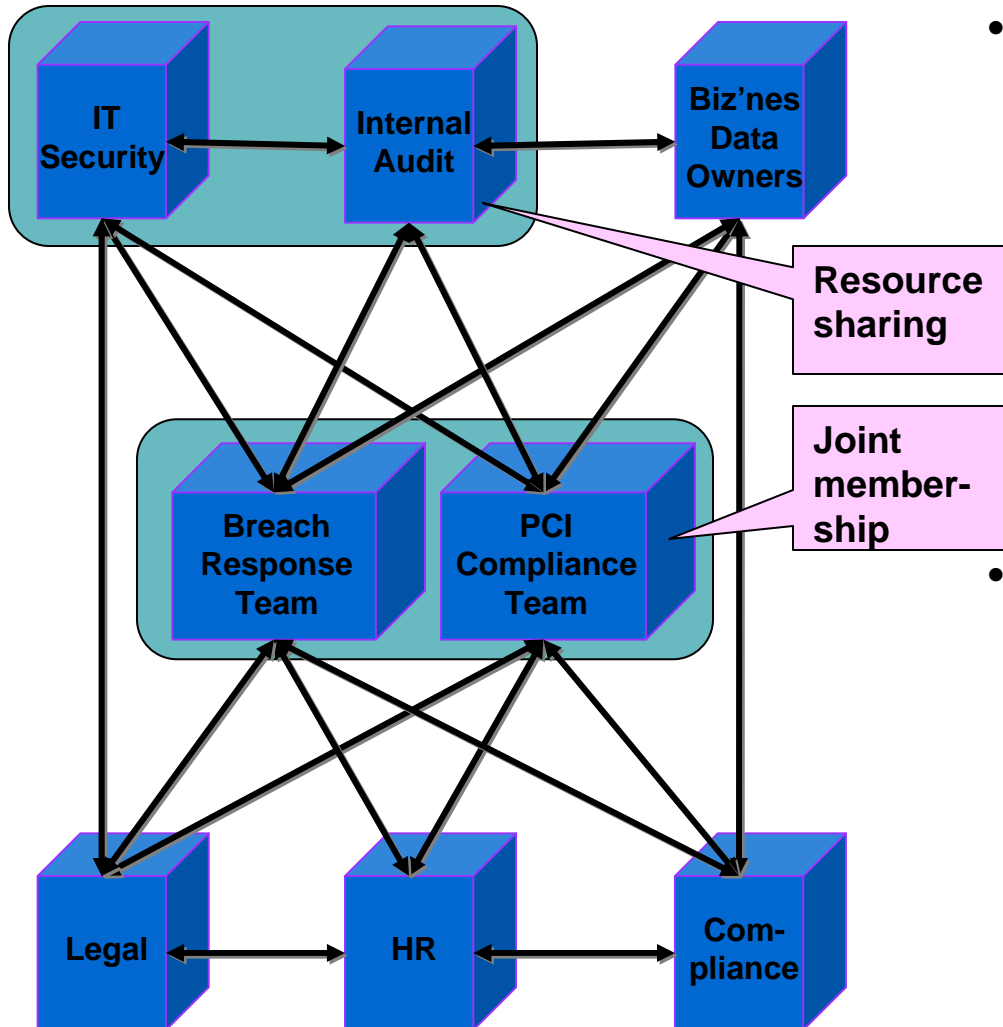
Few merchants, banks or service providers are ready to switch out all packaged apps that handle card data, and many still remain to be tested.

Source: PCI Security Standards Council, May 2008

Best Practice: Look Beyond the PA DSS “List” of Compliant Applications

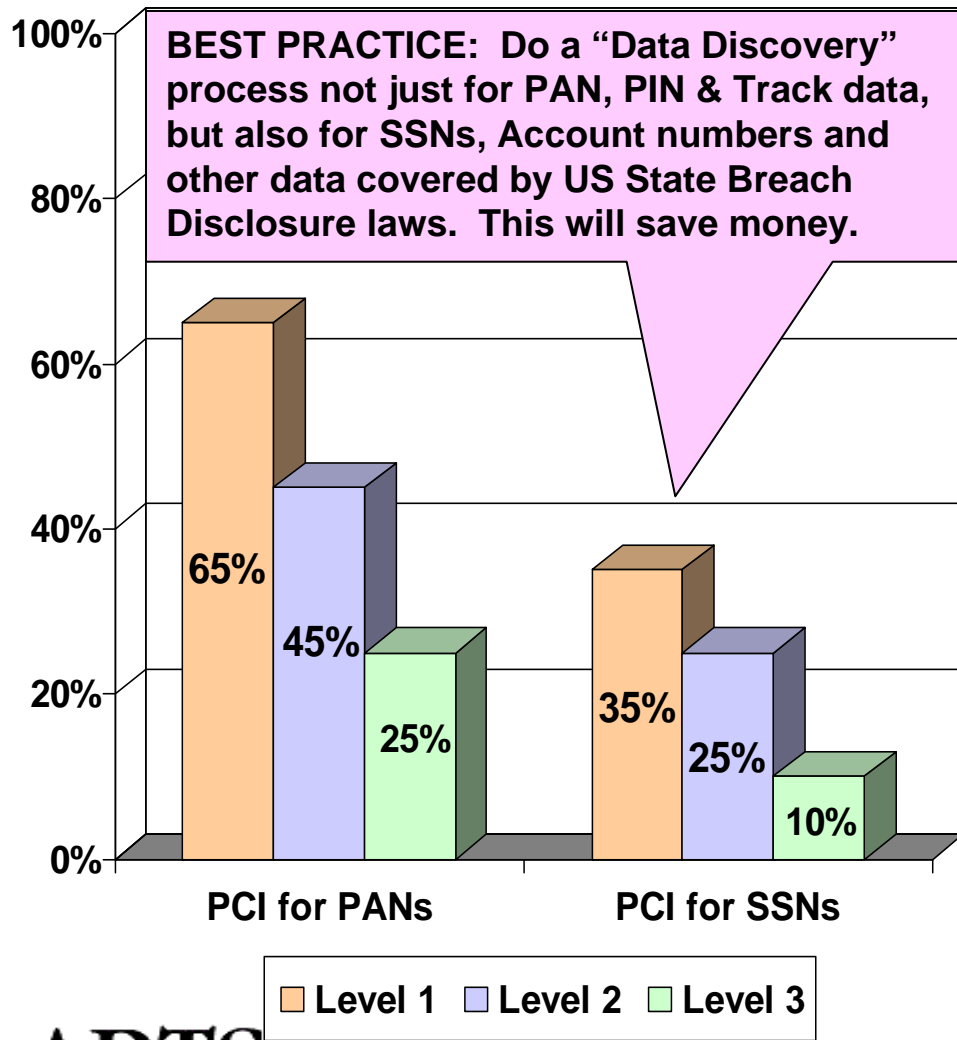


Best Practice: Internal Audit and Business Owners on the PCI Team



- **BEST PRACTICE:** Now that the payment side of our business is PCI compliant, we're scheduling quarterly reviews internally of PCI compliance. This is how we will "operationalize" PCI compliance, through our internal audit group, because they are technical enough to do it (Source: Level 1 merchant).
- PCI compliance monitoring is an add on function for public accounting, which does our internal audits. They are supposed to be looking at whether or not the controls we have can support our financial statements. However, these people don't have the skills to do PCI auditing (Source: Level 2 merchant).

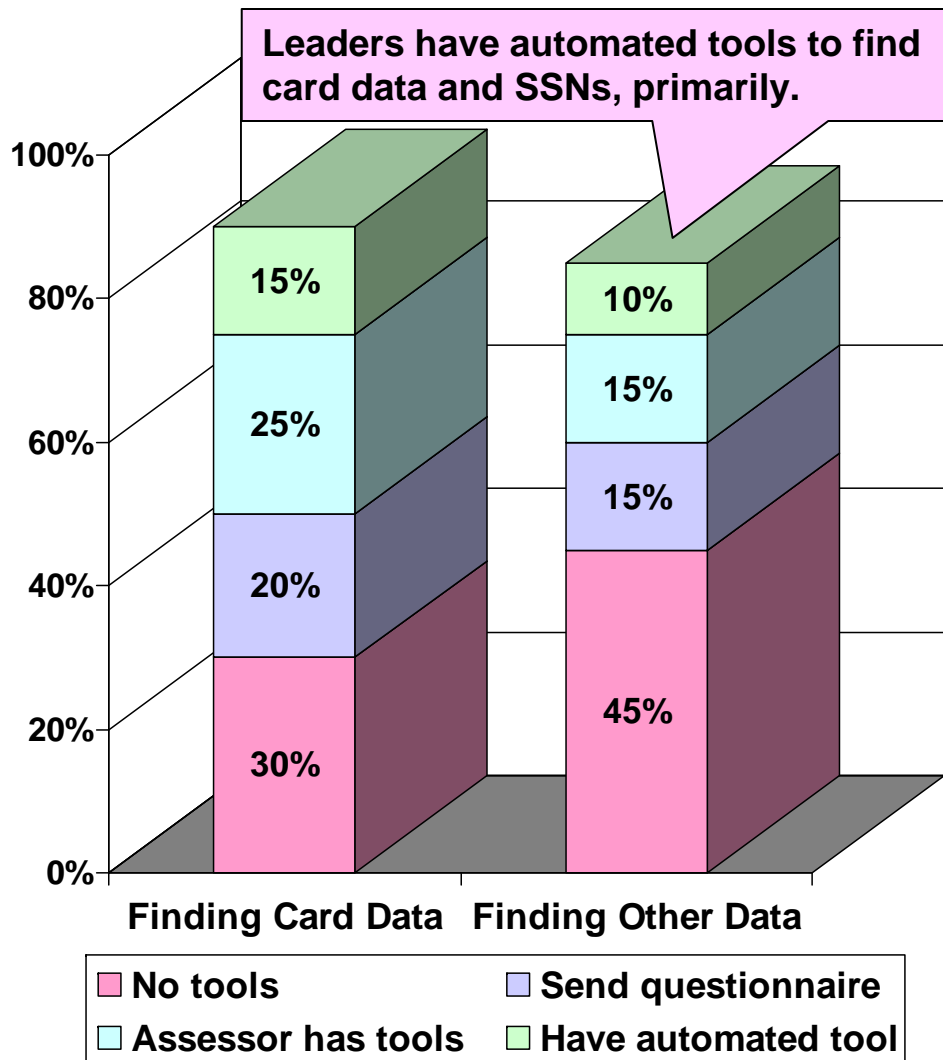
Best Practice: Apply PCI Standards to Protect SSNs and Other PII



- **BEST PRACTICE:** Apply many of the PCI standards (e.g., 1, 3, 4, 5, 6, 7, 8, 10, 11, 12) to the protection of SSNs, other customer and employee PII, and trade secrets. Do so early, to avoid doing tasks like network segmentation and encryption multiple times.
- **COMMENTARY:** In addition to protecting card data, we used PCI compliance as a starting point, and then spent a lot of time evaluating security of our employee DBs, which include SSNs, which we encrypted and masked on the screens (Source: Level 1 Service Provider).

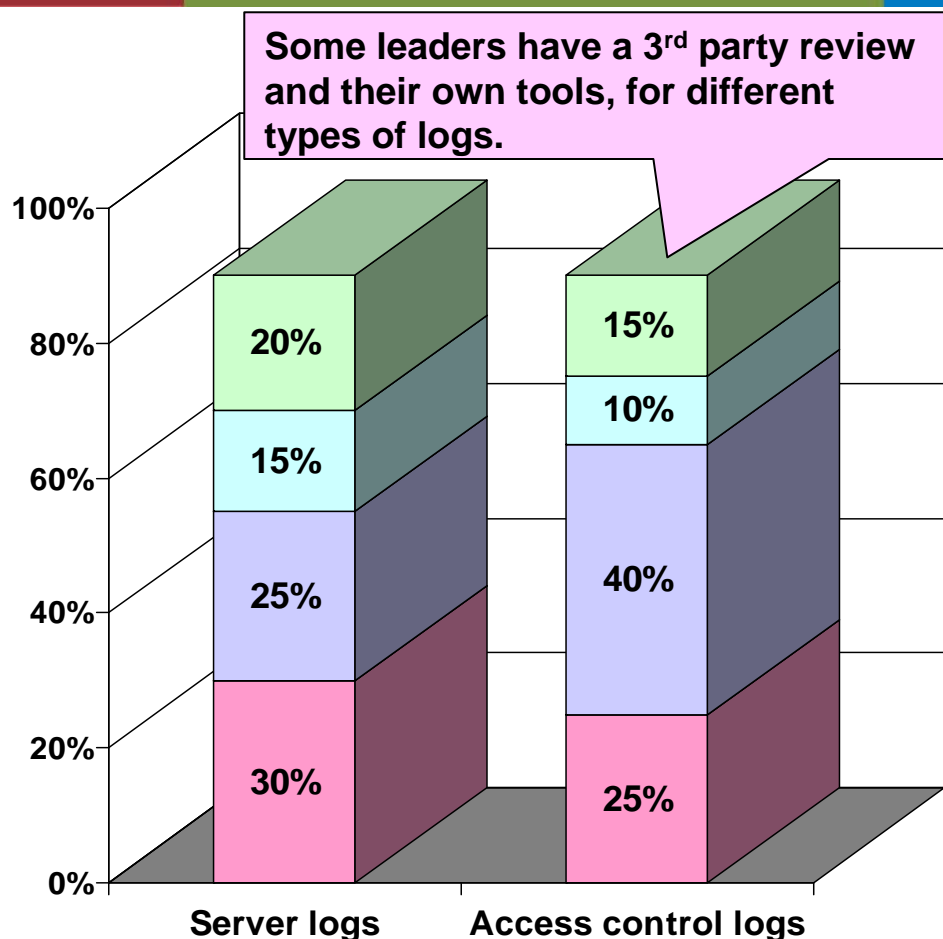
Source: PCI Knowledge Base, September 2008

Best Practice: Use Automated Tools to Find Confidential Data



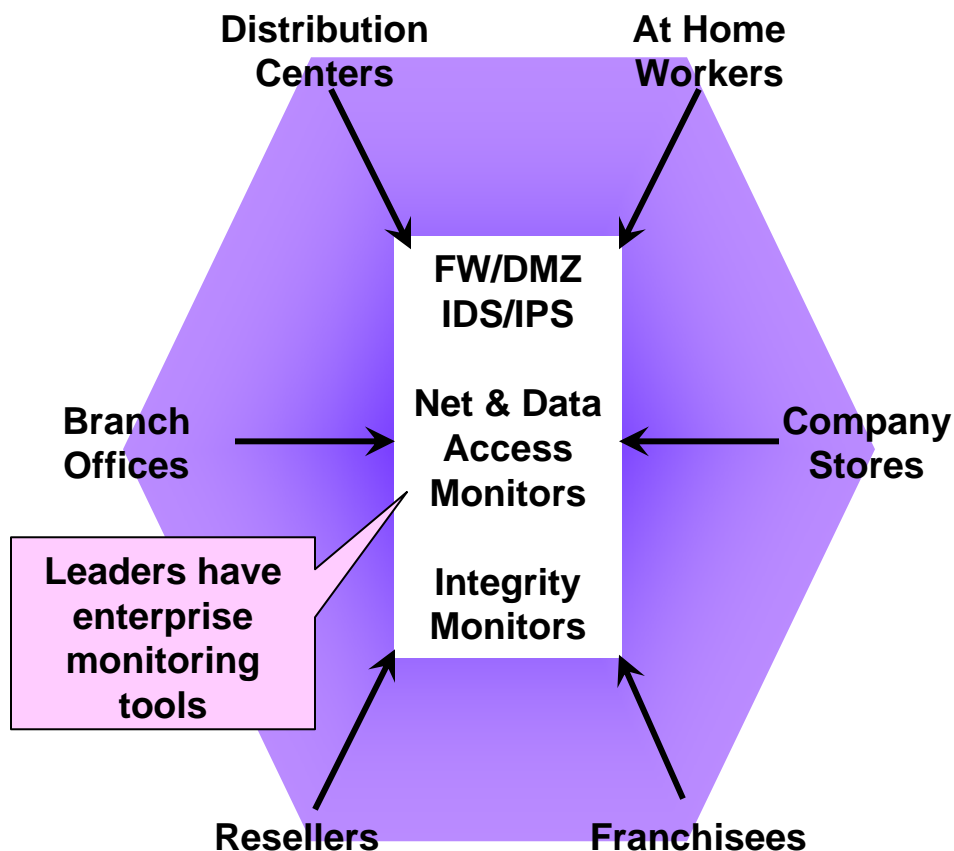
- The biggest problem we see with merchants is just finding the data at rest. Some companies send out a questionnaire asking depts if they have PCI data stored. If they get back a bunch of "No" answers they think they are done (Source: Vendor CTO).
- After 6 months with a PCI assessor, we are still finding card data in places we didn't expect to find it (Source: Level 1 Retailer).
- **BEST PRACTICE:** We have several tools we use to find confidential data in our systems. One is dbDataFinder, another is ISYS Search Software, and there is also Helix, from Cornell University (Source: Level 1 Merchant).

Best Practice: Automate the Analysis of Security Logs



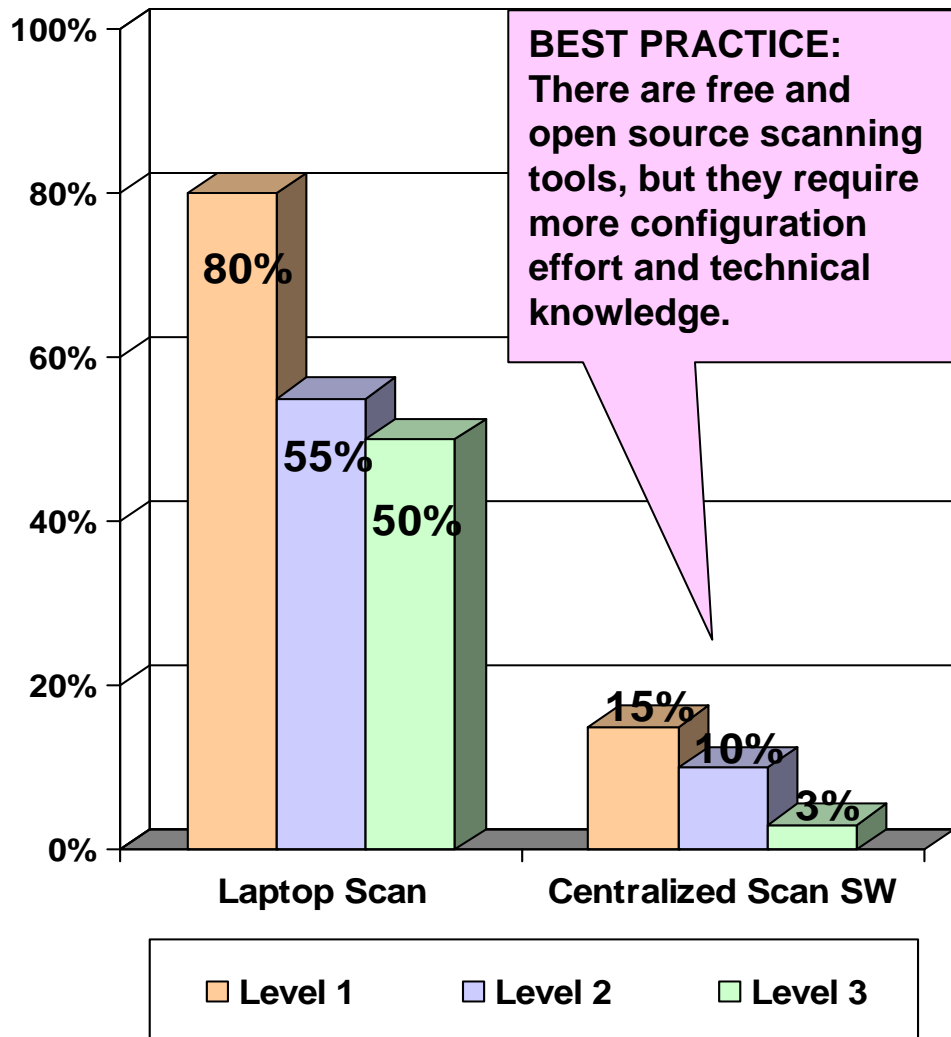
- **LEADER'S VIEW:** The native logging tools such as Cisco MARS are not comprehensive. We need a overall data logging and monitoring tool that is manageable (Source: Level 2 merchant)
- **LEADER'S VIEW:** Most merchants cite SYSLOG as their approach to server log management. While I know some assessors who will sign off on that as sufficient, we do not. There is much more to log management than what syslog does (Source: PCI Assessor)
- Because of the perceived intrusiveness of system audit and logging, merchants are looking for a rationale to do less, and some simply turn it off (Source: PCI Assessor).

Best Practice: Remote Compliance Management



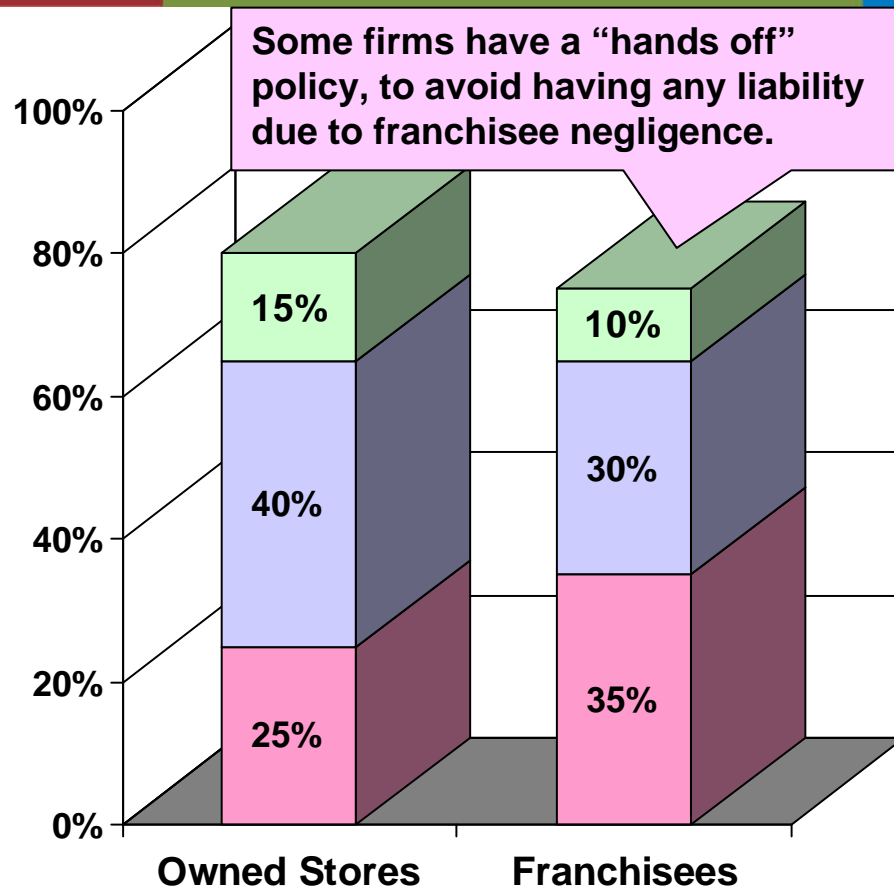
- **BEST PRACTICE:** Do not ignore store-level or other remote location vulnerabilities. Simple questionnaires to store management are OK, but automated network scanning and system monitoring tools are the best way to manage compliance long term.
- The biggest security challenge we have is small franchisees. They can open up ports and we won't know about it, because we're not scanning all the ports in all the store systems (Source: Level 1 Merchant).
- I've seen assessors tell clients to implement Tripwire out to the POS across all their stores. But then the client wasn't doing anything with the data (Source: PCI Consultant).

Best Practice: Centralize Wireless Network Scanning



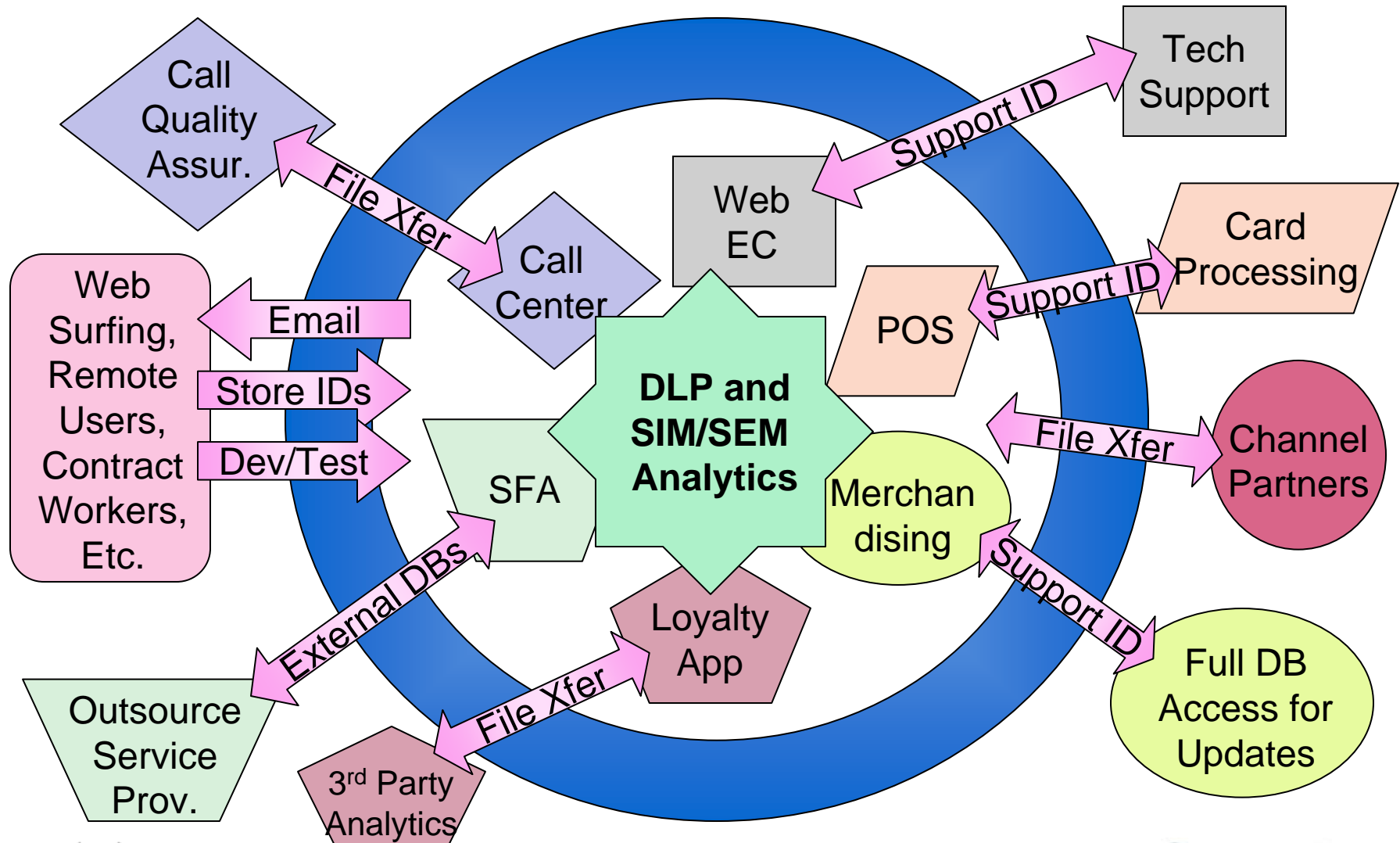
- **BEST PRACTICE:** PCI DSS requires quarterly wireless scans, often done by carrying a laptop with scanning software around HQ and stores. But installing the SW at all stores costs enough such that few merchants do it.
- Our wireless system is segmented from the store networks and we have it scanned regularly to be sure there to way to get from the wireless networks to a store POS system or corporate network (Source: Level 1 Retailer).
- Currently, we have a wireless analyzer which runs on a laptop. We run this quarterly. We will bring in a tool for wireless intrusion detection (Source: Level 2 Merchant).

Best Practice: Automate “Gold Load” Configuration & Change Mgmt

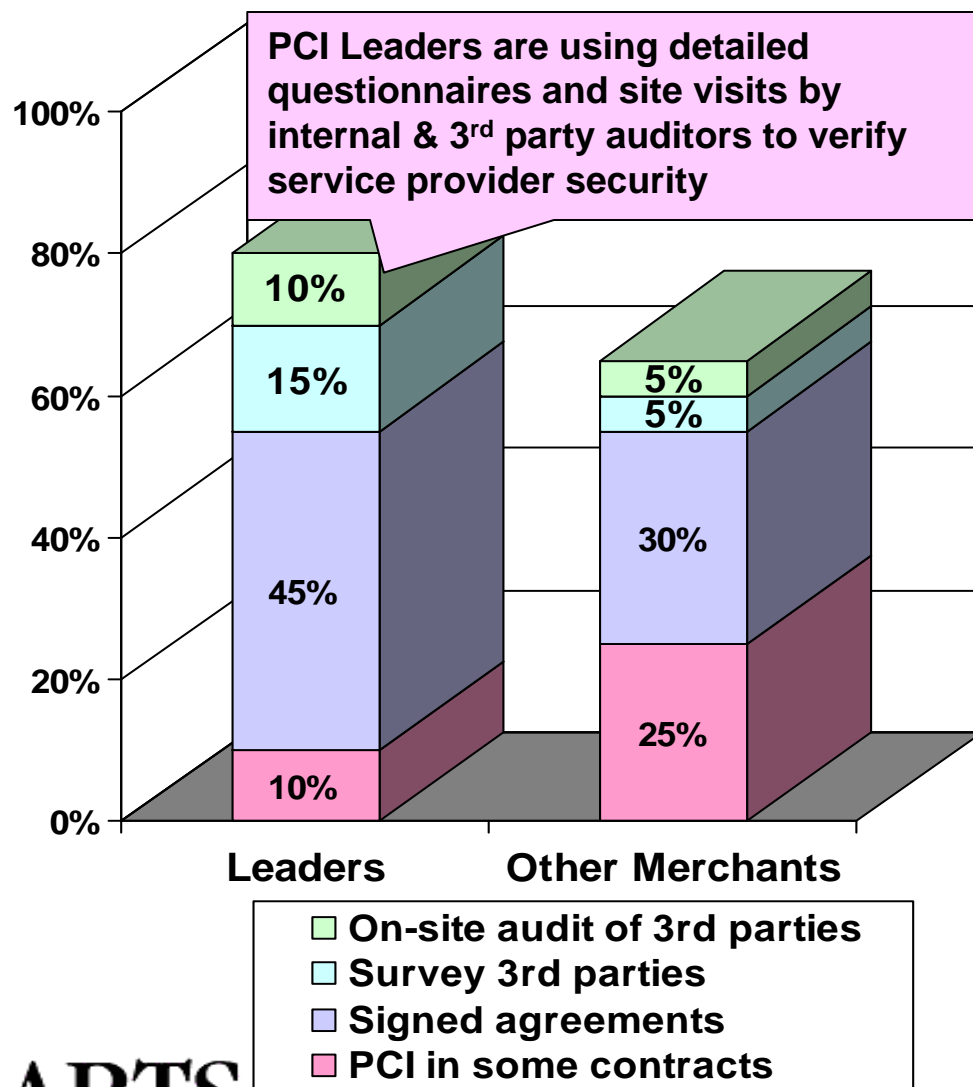


- **BEST PRACTICE:** We have several thousand stores in our chain, and the key issue for us is control of their POS systems. We mandate the same setup for both our owned and franchised stores (Source: Level 1 merchant).
- For our franchisees, we require a wide range of standardized operating procedures which relate to security. However, we cannot force them all to use the same property management system (Source: Level 1 Hotel Chain).
- We do not have a PCI mandate in our contracts with franchisees. There are a number of specific criteria that they have to meet, but PCI is not included (Level 1 Hotel Chain).

Best Practice: Reduce and Track External Data Access

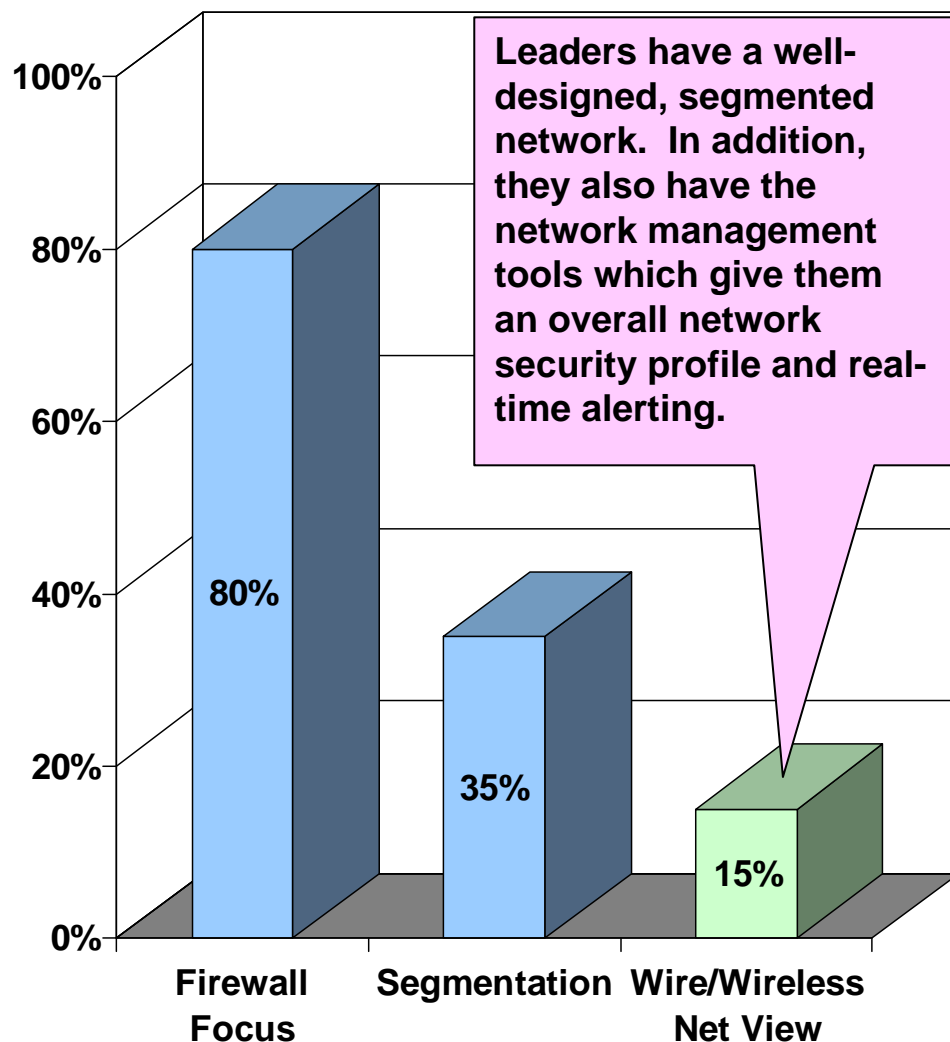


Best Practice: Due Diligence of Service Provider Security – Not a “Letter”



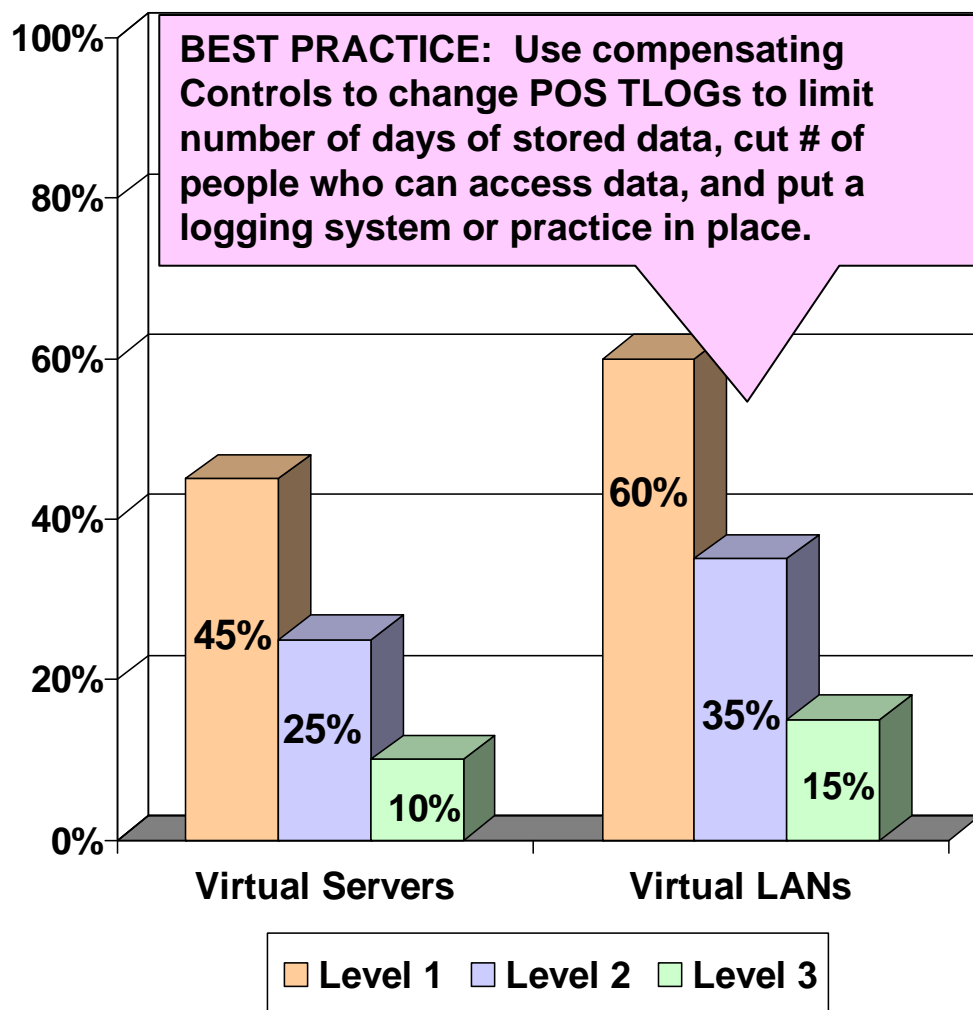
- **BEST PRACTICE:** We make sure that PCI compliance is mentioned in all our service provider contracts. We also do due diligence and measure our service providers' security effectiveness. We have our own form for that. Having an industry standard would be better, but we cannot wait for that (Source: Level 1 merchant).
- Third party security is the most overlooked area of security because companies assume that the third party owns the risk if they have a simple agreement addendum that mentions PCI. From 75% of all forensic exams we've done, the breach occurred at a third party, not the merchant (Source: PCI Assessor).

Best Practice: Segmented Networks and Integrated Management



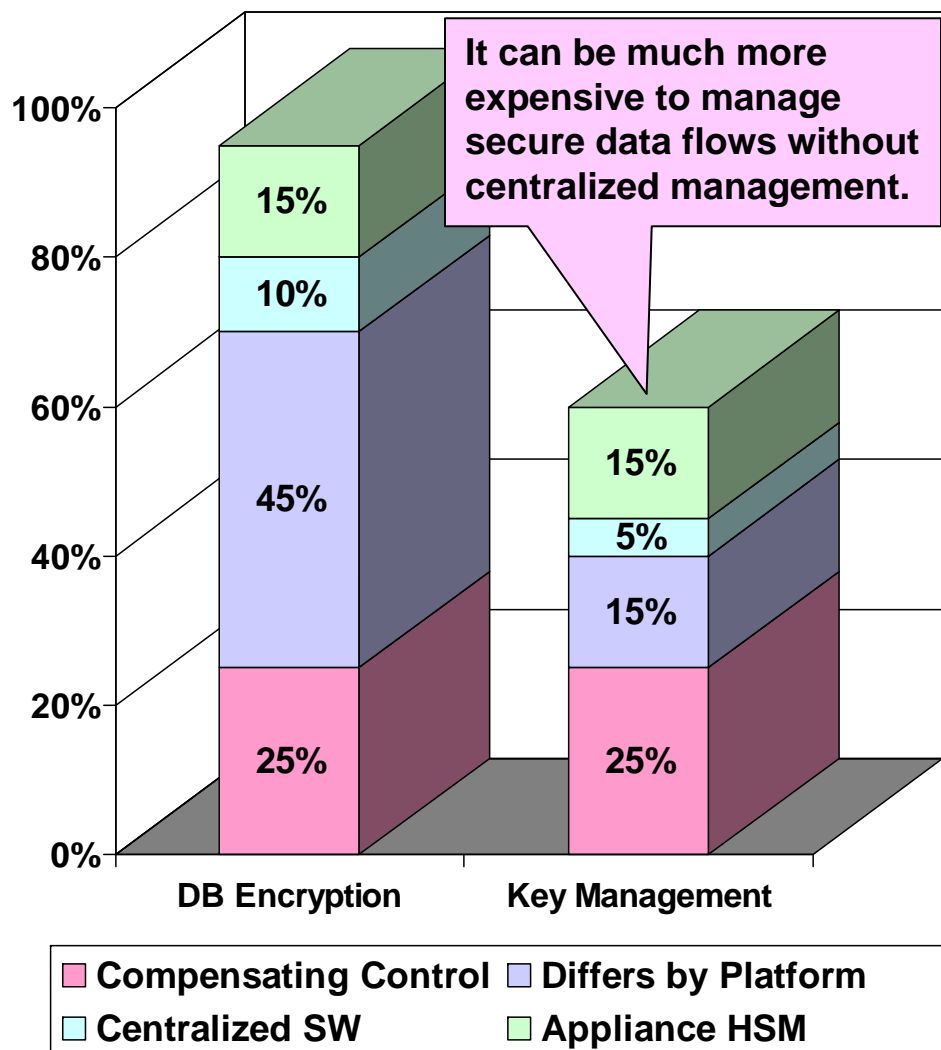
- We have a homegrown application software environment. It's legacy, but we cannot replace it all. And we don't have to for PCI as the systems don't have any cardholder data. We relied on network segmentation to get us PCI compliant (Source: Level 2 Merchant).
- Recommendation: The best way to reduce risk is to isolate systems, via network segmentation. The typical merchant struggles with the problem that cardholder data is intermingled on many different systems. So, if companies segment the network, they can reduce scope and reduce risk to card data (Source: PCI Technologist).

Best Practice: Deploy Virtualized Servers and VLANs to Segment Data



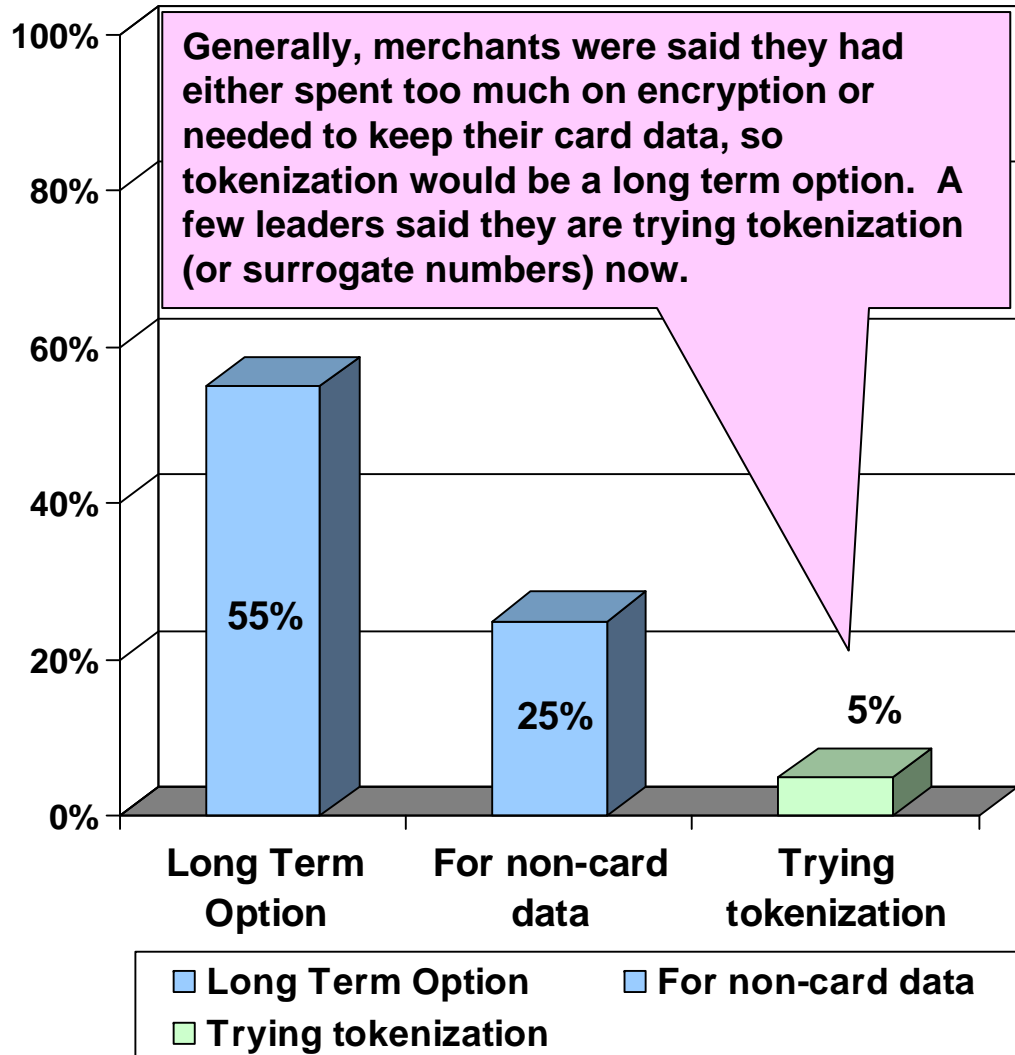
- **BEST PRACTICE:** Some leading retailers have begun to deploy server and network virtualization technology as part of their data segmentation process. This can save money for growing businesses.
- We are deploying more virtualized servers over 2008. We were told they are OK for PCI, as long as we keep apps with the same risk level on the same physical server (Source: Level 1 merchant).
- We got a ruling from our assessor that VLANs were “PCI compliant” as a way to segment our networks, though we are being cautious about deploying them (Source: Level 3 Merchant).

Best Practice: Use Native Encryption and Centralized Key Management



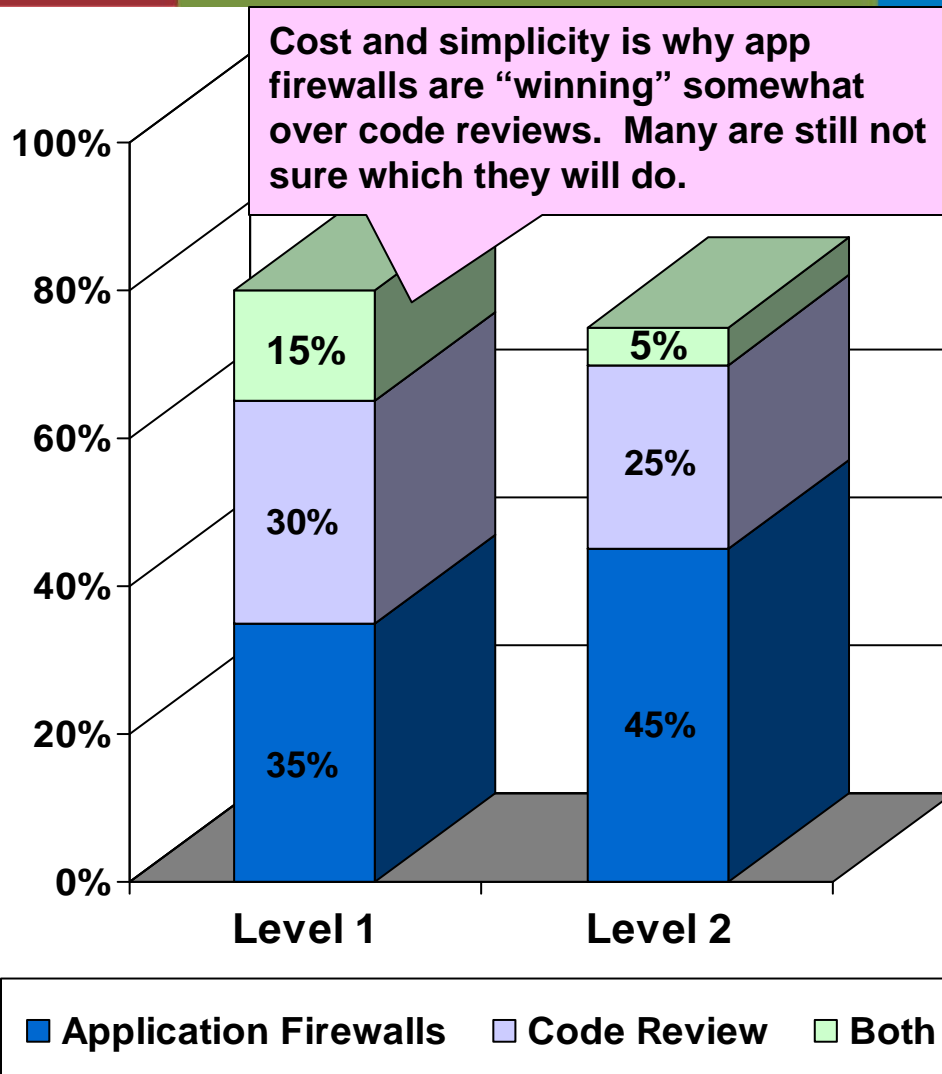
- **BEST PRACTICE:** The use of native encryption provides the best performance at the lowest cost. But encryption keys should be centrally managed. If not, the movement of data between systems results in risks due to decryption. The key management system should not be the enterprise directory system, as these are not sufficiently secure.
- We talked to several encryption and key management vendors - RSA, Ingrian, Protegrity - and got estimates - several hundred thousand for data at rest and in transit. The key to data encryption is in figuring out what data is confidential and what you need to share (Source: Level 1 merchant).

Best Practice: Use “Tokens” In Place of Card Data



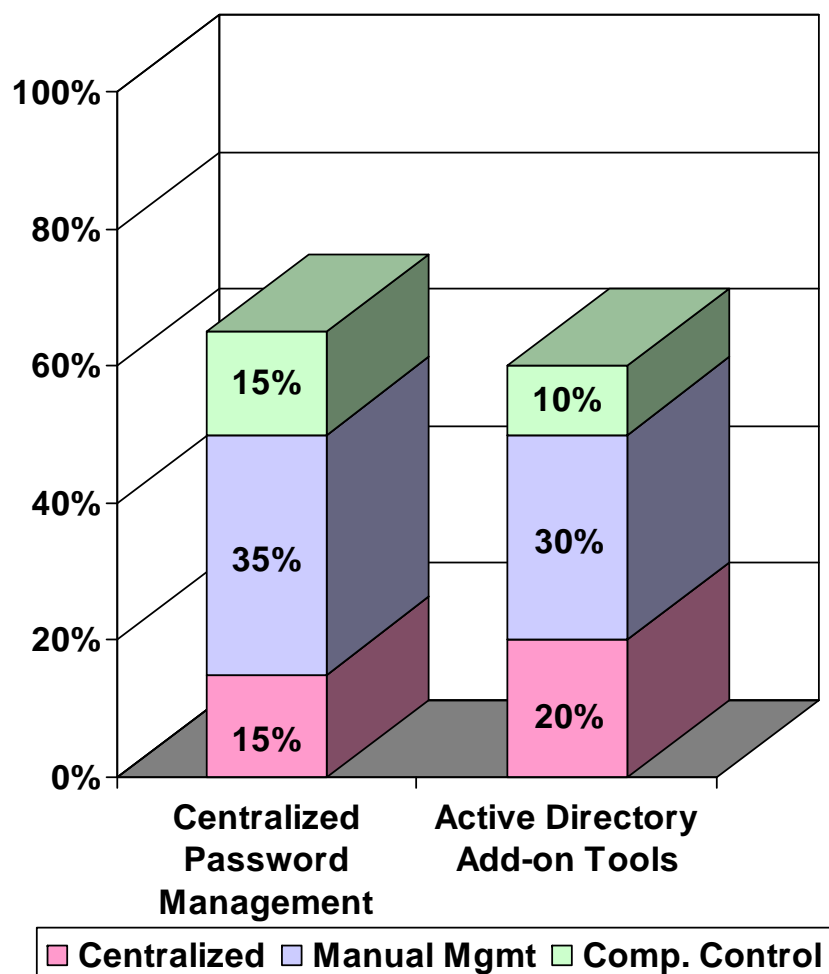
- There are several different ways to implement Tokenization (or surrogate numbers). There are a lot of homegrown systems that use Reference IDs - such as XREF - cross reference - creates encryption key at the reader (Source: PCI Assessor)
- **BEST PRACTICE:** We decided to eliminate, or at least minimize, the card data we have on our system. We implemented the tokenization or card number proxy system from Shift4. Basically, when the agent takes the card number, it goes directly from our system to Shift4, and a token number is returned and that is what is stored (Source: Level 1 Service Provider)

Best Practice: Use Both Application Firewalls and Code Reviews



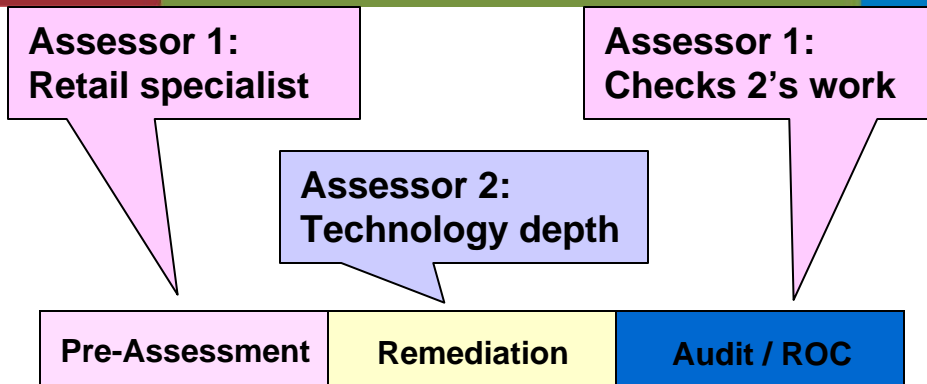
- For PCI 6.6, we don't treat an external code review as equivalent to having an application firewall. Right now, our code review is internal and ad hoc. We need to review it. We need to get the application firewall in place first, while we do the code reviews, which will take a while, months or maybe a years (Source: Level 2 Merchant)
- PCI 6.6 represents a false choice for merchants. Application Firewalls and Code Reviews do very different things. We did a detailed code review, and that was useful. But the PCI standard says you have to have an app firewall. But an application firewall gives management a false sense of security (Source: Level 3 Merchant.)

Best Practice: Privileged User Management to Cut Internal Breach Risk

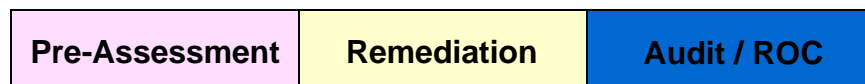


- We do centralized password admin now. But it's all manual. I want to have an automated way for people to reset their passwords (Source: Level 2 Retailer).
- Passwords are an IT resource killer. In terms of overall workload, password resets make up 25% of our user calls. We have Active Directory, but we need to use add-on's to enable password and ID management (Source: Level 1 Retailer).
- We need to upgrade password mgmt. Because of PCI, we found customer facing applications that don't have password aging. Also, our business customers may share their IDs on our system (Source: Level 2 Merchant).

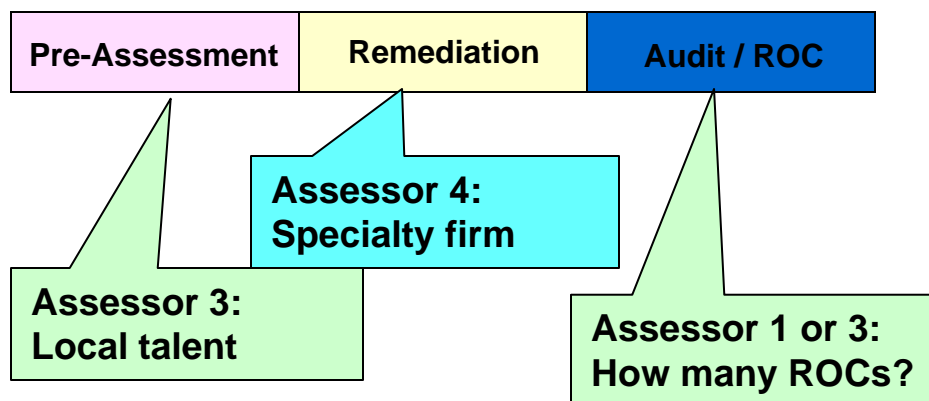
Best Practice: Use Different Assessors for Remediation and Audit



Consumer Products Division

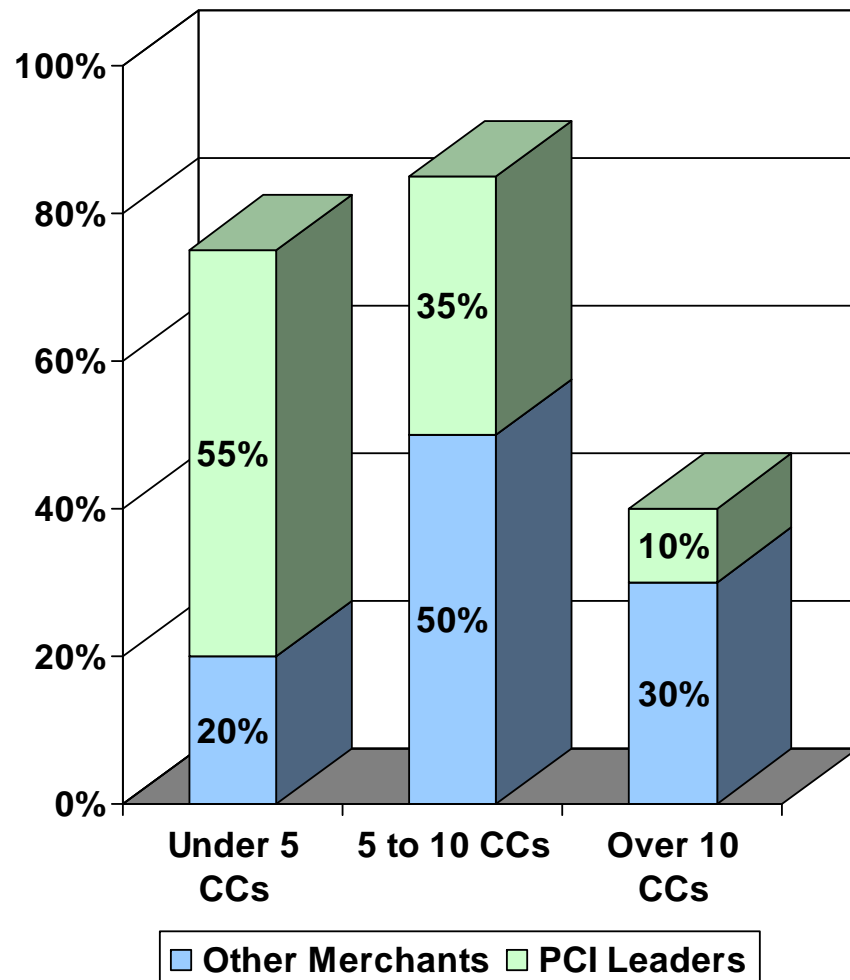


E-Commerce Channel



- **BEST PRACTICE:** We started out using VeriSign. They came in last year to do a pre-audit and gap analysis. We had originally planned to use them for remediation as well, but we decided to bring in Fishnet for the remediation (Source: Level 2 merchant).
- We had a different company, Aegenis, who does the QSA training, develop our compensating controls, and our assessor reviewed and accepted them (Source: Level 1 merchant).
- I'm not concerned about any ethics issues in terms of the assessor reselling product or reviewing their own remediation. I want to make sure we pass (Source: Level 1 merchant).

Leaders Use About 5 Compensating Controls Others Use About 10



- Typically I see a handful of compensating controls. Over 10 is a high number. Over 20 is excessive. I see most of them as a substitute for encryption of data at rest. I know a merchant who convinced their auditor that they had good access controls on their mainframe and didn't need encryption. I'd want to see proof of the effectiveness of those access controls before I would sign off (Source: PCI Assessor).
- Our bank, which is Bank of America, said nothing about our compensating controls, of which we had about a half dozen. I don't even think they reviewed them (Source: Level 1 Merchant).

Getting Ready for PCI 1.2 and PA DSS

Some Recommendations



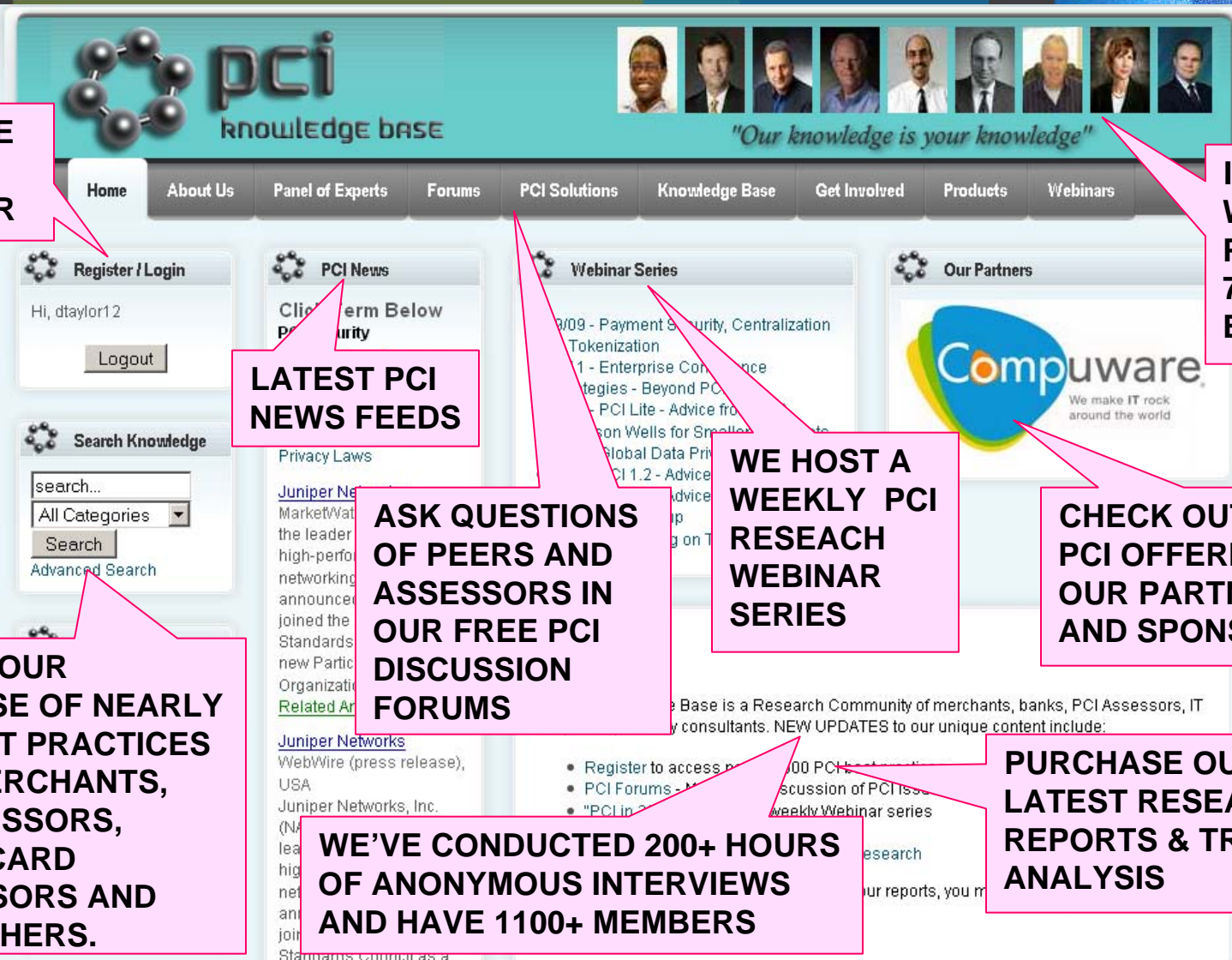
1. **Download 1.2 and PA DSS and review with IT, CISO, Internal Audit, etc.**
2. **Check with your assessor (if any) on interpretation of “payment app”.**
3. **Also get a ruling on “commonly” before buying new AV software.**
4. **Reduce PCI scope via network segmentation and data purging.**
5. **Turn on monitoring functions and fix any performance impacts.**
6. **Investigate Wireless IDS vs manually scanning all locations.**
7. **Ensure individual data access is tracked via ID management system.**
8. **Replace manual, non-scalable log review / analysis with usable tools.**
9. **Implement IP scans and pen testing more often than PCI requires**
10. **Apply PCI controls to SSNs and other confidential data if possible.**
11. **Implement tools to monitor PCI compliance by service providers.**
12. **Plan to replace all compensating controls over the next 1-2 years.**

Recommendations for SMEs – Start Now



1. **Stop collecting card data and other confidential data you don't use.**
2. **Talk to your acquirer and understand their demands & timeframes.**
3. **Bring in a consultant for a “gap analysis” but do the SAQ yourself.**
4. **Write / update security policies – and be sure you can meet them.**
5. **Reduce PCI scope via network segmentation and data purging.**
6. **Turn on monitoring functions and fix any performance impacts.**
7. **Make sure all systems are patched and “hardened.”**
8. **Ensure individual data access is tracked via ID management system.**
9. **Implement a monthly risk and vulnerability review process.**
10. **Extend PCI controls to SSNs and other confidential data.**
11. **Implement tools to monitor PCI compliance by service providers.**
12. **Plan to replace all compensating controls over the next 1-2 years.**

Why Join the PCI Knowledge Base (www.KnowPCI.com)?



IT IS FREE TO REGISTER

INTERACT WITH OUR PANEL OF 70+ PCI EXPERTS

LATEST PCI NEWS FEEDS

WE HOST A WEEKLY PCI RESEARCH WEBINAR SERIES

CHECK OUT THE PCI OFFERINGS OF OUR PARTNERS AND SPONSORS

SEARCH OUR DATABASE OF NEARLY 3000 BEST PRACTICES FROM MERCHANTS, PCI ASSESSORS, BANKS, CARD PROCESSORS AND MANY OTHERS.

ASK QUESTIONS OF PEERS AND ASSESSORS IN OUR FREE PCI DISCUSSION FORUMS

WE'VE CONDUCTED 200+ HOURS OF ANONYMOUS INTERVIEWS AND HAVE 1100+ MEMBERS

PURCHASE OUR LATEST RESEARCH REPORTS & TREND ANALYSIS

Participate in PCI Knowledge Base



- *Participating in the Knowledge Base*
 - **Review the Items -- You can comment on an item (agree, disagree, etc)**
 - **Recommend items -- You can email individual items to a colleague**
 - **Report a problem -- Let us know about broken links or any other problems with an item or the website**
 - **Favorite items -- You can create a list of "favorite" items which you can use to customize your experience in the Knowledge Base**
 - **Find items from a specific Expert -- Those items attributed to a specific member of our Panel of Experts can be identified**
 - **If you have experience, good or bad or confusion, with PCI, contact David Taylor at info@knowpci.com for an interview about your experiences**

Why Adopt ARTS Standards?



- **Retailers:**

- Protect investment
- Increase ROI
 - Faster implementation
 - Lower costs
- Learn the Business

- **Vendors**

- Increase sales
- Rapid response to enhancements
- Focus on innovations and mundane

How to Join



- WWW.NRF-ARTS.org
- Dues by annual revenue
- Vendors: \$2,500 to \$5,000
- Retailers: \$1,500 to \$3,000

Contact Information



Contact:
Cy Young
cy.young@coat.com

Visit ARTS
<http://www.nrf-arts.org/>

Visit PCI Knowledge Base
www.KnowPCI.com

