

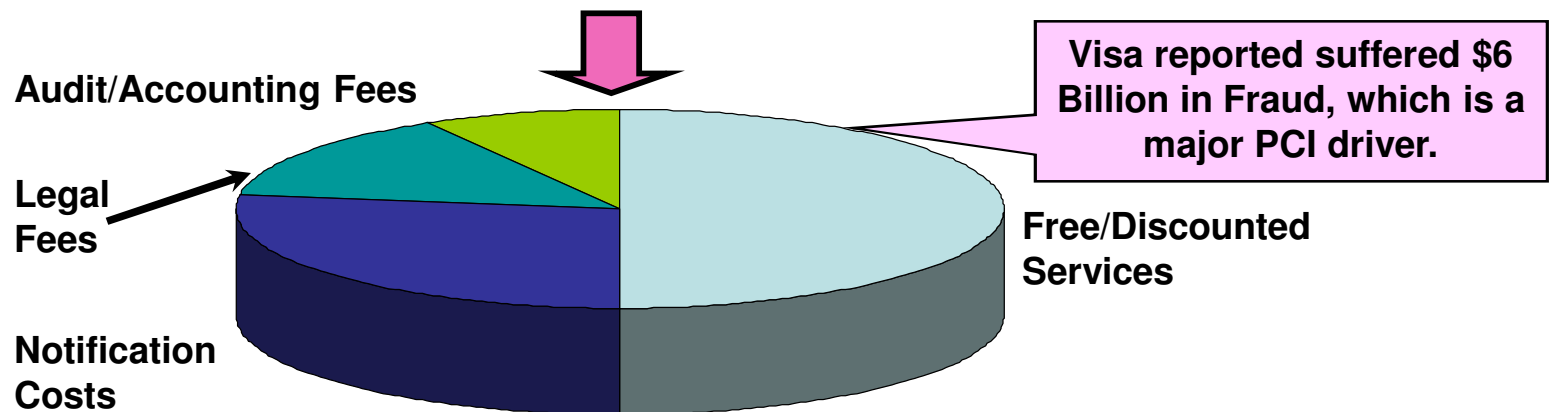
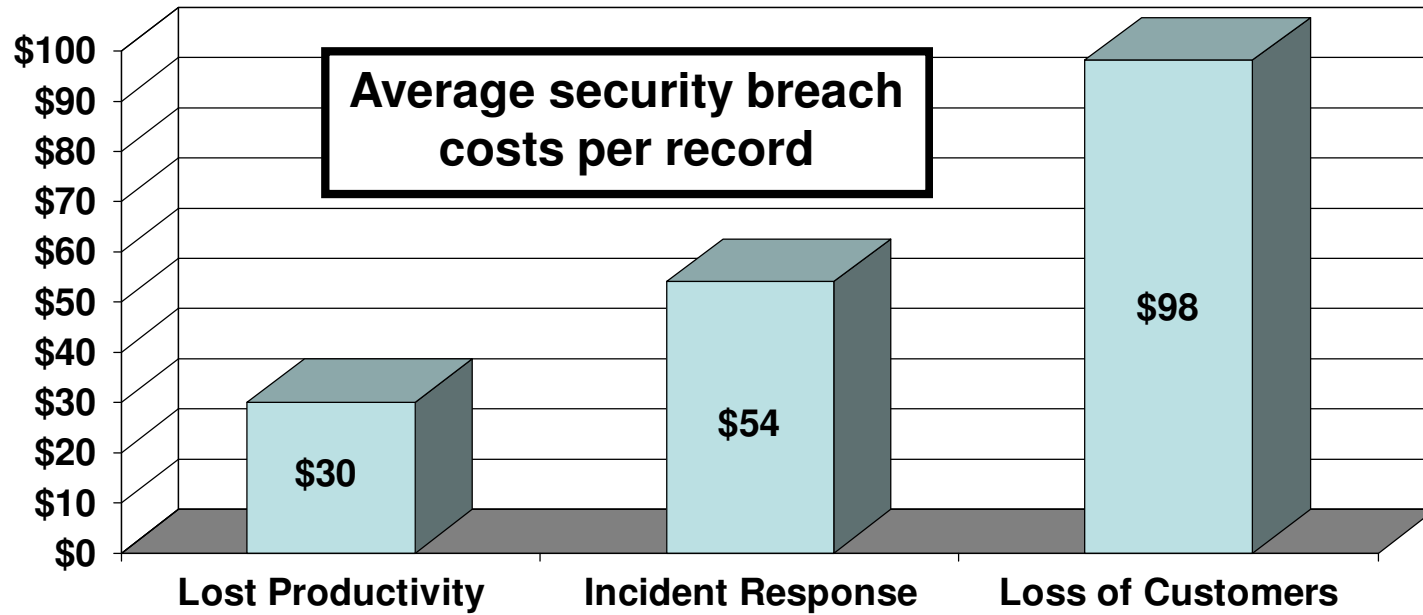


Are You Ready for PCI 1.2???
How about PA DSS???

The Latest Findings from the PCI Knowledge Base

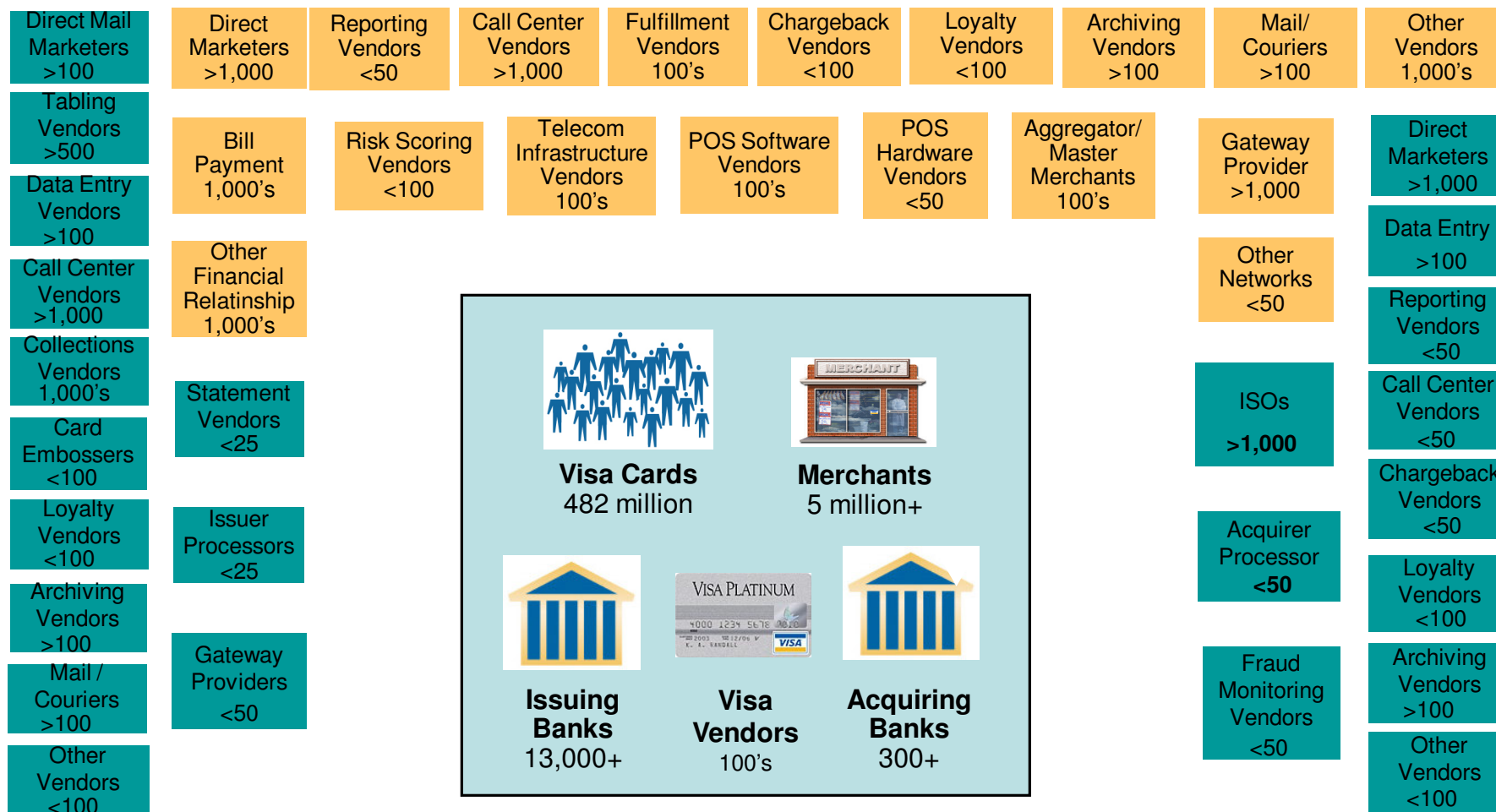
Presented by: Dr. David Taylor, CISSP
David.Taylor@KnowPCI.com

PCI Standards Exist to Reduce the Risk and Cost of Security Breaches



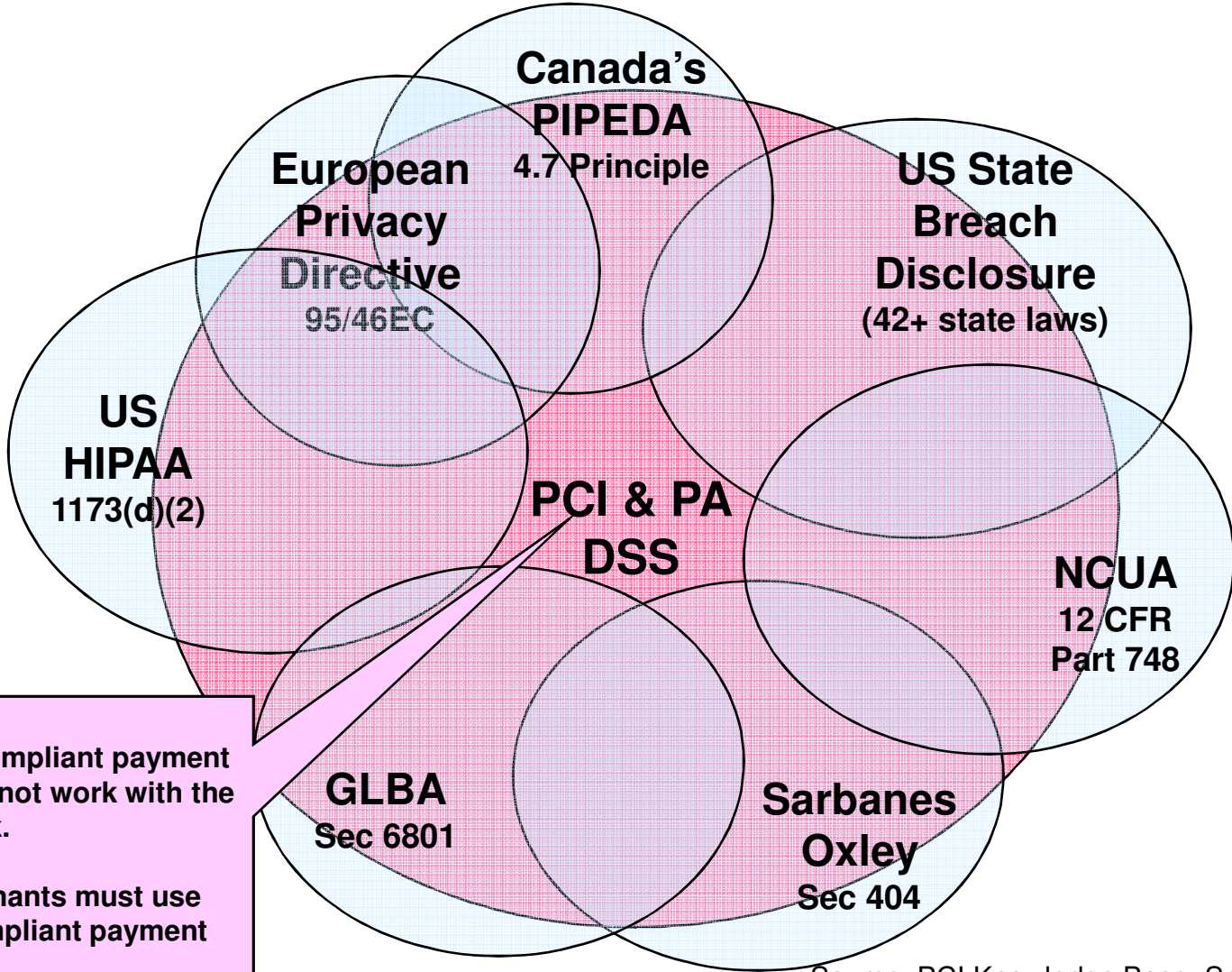
Source: Ponemon Institute, 2007

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



Source: Numbers are taken from Visa, April 2007

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

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

No Changes Are Expected in 1.2 to the 4 PCI Compliance Levels

Merchant Level	Qualification of Level	Validation Action	Validated By
1	Any merchant-regardless of acceptance channel-processing over 6,000,000 ecommerce transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise.	Annual On-site PCI Data Security Assessment	QSA Company or Internal Audit if signed by Officer
		Quarterly Network Scan	Qualified Scan Vendor
2	Any merchant processing 150,000 to 6,000,000 e-commerce transactions per year.	Annual Self-Assessment	Merchant
		Quarterly Network Scan	Qualified Scan Vendor
3	Any merchant processing 20,000 to 150,000 e-commerce transactions per year. <div style="border: 1px solid black; background-color: #FFDAB9; padding: 5px; display: inline-block; margin-top: 10px;">The impact of SAQ changes will be felt by many at YE 2008</div>	Annual Self-Assessment Questionnaire	Merchant
		Quarterly Network Scan	Qualified Independent Scan Vendor
4	Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants processing up to 6M Visa transactions per year.	Annual Self-Assessment Questionnaire	Merchant
		Network Scan	Qualified 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.

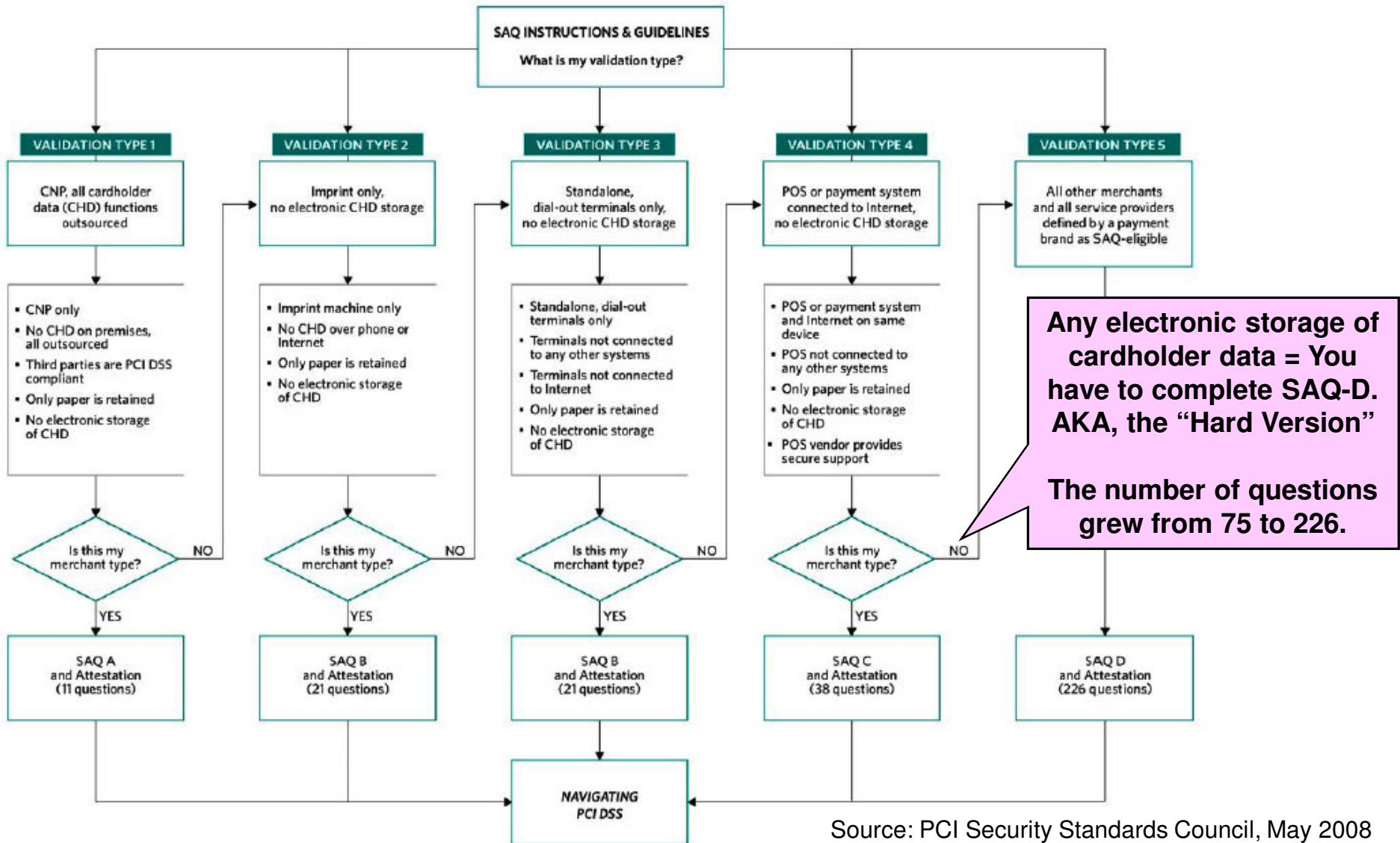
SAQ - D

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.

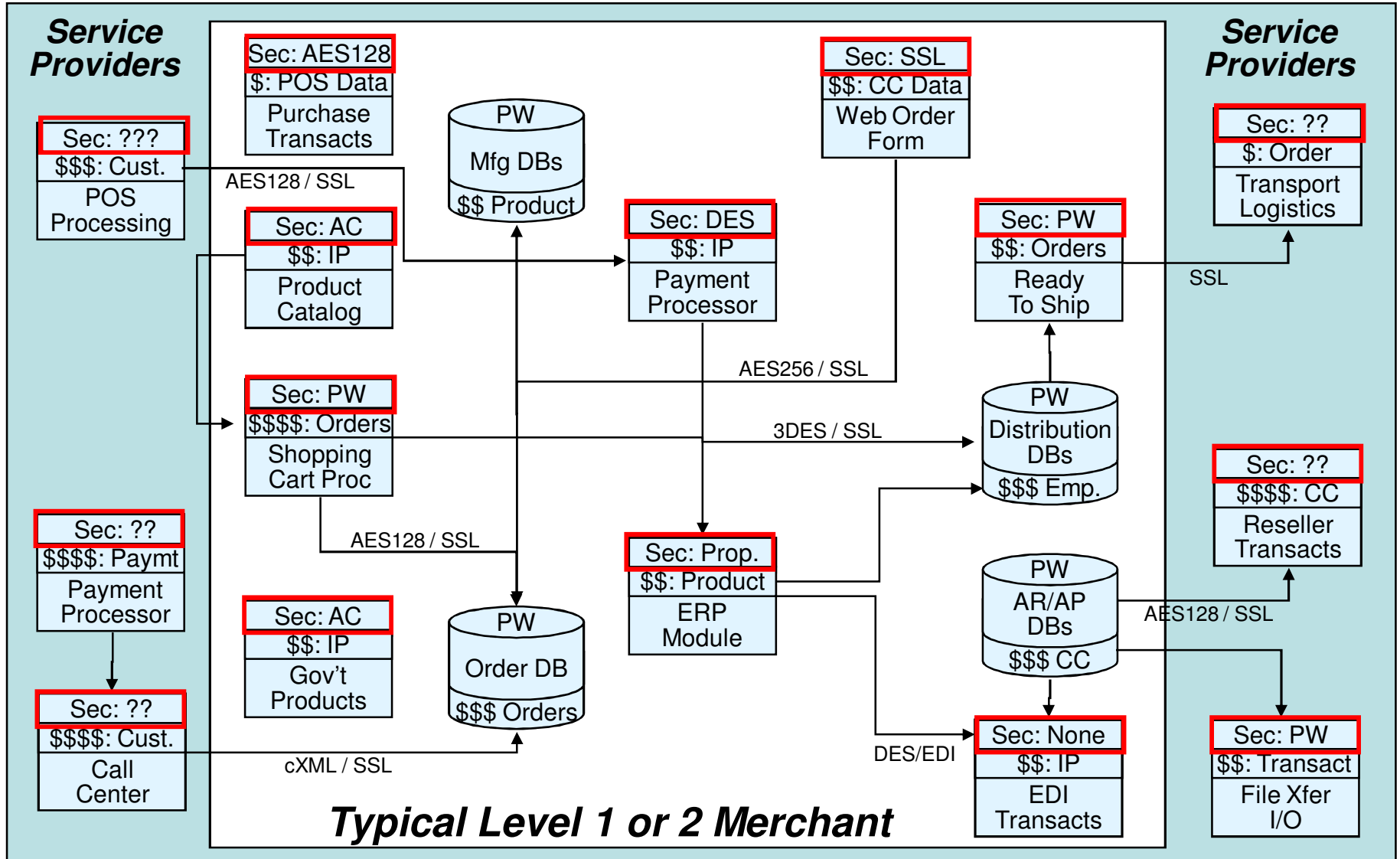
New versions of the SAQs are expected before YE 2008, which will be based on the PCI 1.2 standard.

Source: PCI Security Standards Council, May 2008

Self-Assessment Got Much Harder This Year, For Most Merchants & SPs



SAQ – D Adds Key Management Requirements for Levels 2 - 4



Summary of Expected Changes in PCI 1.2

REQ #	PCI REQUIREMENT CHANGES
1.	CONFIGURATION REQUIREMENTS APPLY TO BOTH ROUTERS & FIREWALLS. ADDED FLEXIBILITY ON TIMING FOR REVIEW OF FIREWALL ACL
2.	WEP NO LONGER ACCEPTABLE-ALL WIRELESS MUST BE WPA2 SSID's MAY NOW BE BROADCAST
3.	<i>NO MAJOR NEW CHANGES</i>
4.	DISCONTINUE WEP AFTER JUNE 30 TH , 2010
5.	ANTI-VIRUS REQUIRED ON <u>ALL</u> OPERATING SYSTEMS
6.	PATCH REQUIREMENT IS MORE FLEXIBLE REQUIREMENT 6.6 IS NOW MANDATORY
7.	<i>NO NEW CHANGES</i>
8.	<i>NO NEW CHANGES</i>
9.	OFFSITE STORAGE LOCATION MUST BE VISITED ANNUALLY MORE FLEXIBILITY RELATED TO SECURITY CAMERA AND ACCESS CONTROLS
10.	INTERNAL LOG SERVER FOR EXTERNAL , MORE FLEXIBILITY AND CLARIFICATION TO O... AND ARCHIVED AUDIT HISTORY
11.	MORE GUIDANCE ON WIRELESS ANALYZER AND WIRELESS INTRUSTION DETECTION SYSTEMS. PEN TEST REQUIREMENT - <u>BOTH INTERNAL AND EXTERNAL REQUIRED</u>
12.	EMPLOYEES MUST ACKNOWLEDGE COMPANY SECURITY POLICIES AND PROCEDURES "AT LEAST ANNUALLY." UPDATES "TO CONTRACT" & "CONNECTED ENTITIES" LANGUAGE

AV now required on "all" platforms

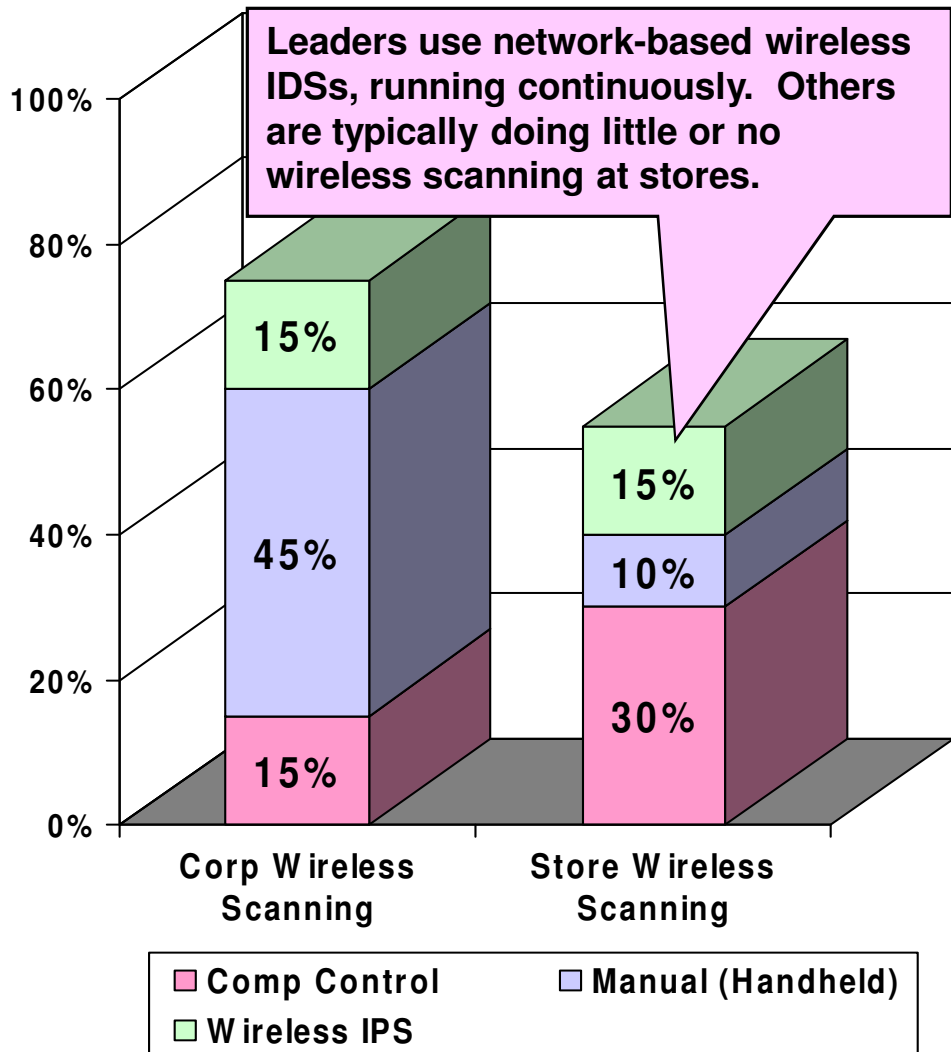
In some respects, for certain standards, PCI is becoming more "flexible" and even adds more focus on letting the firm be driven by "risk management"

SP Visitation????

Wireless IDS mentioned for the 1st time

Source: Digital Resources Group, September 2008

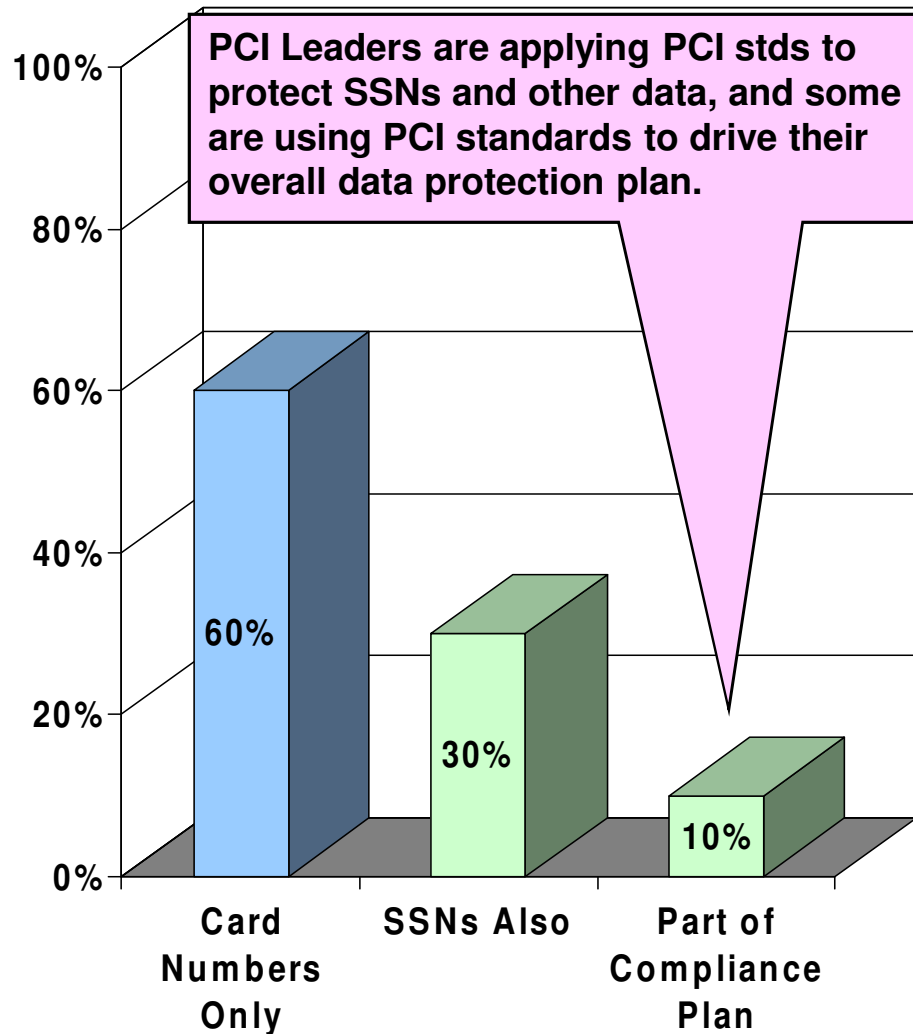
Wireless IDSs are Covered Explicitly in PCI 1.2 For the First Time



- A good majority of companies cannot effectively secure their wireless networks. They just put additional filtering between their wired and wireless networks as a compensating control (Source; PCI Consultant).
- 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).

Source: PCI Knowledge Base, May 2008

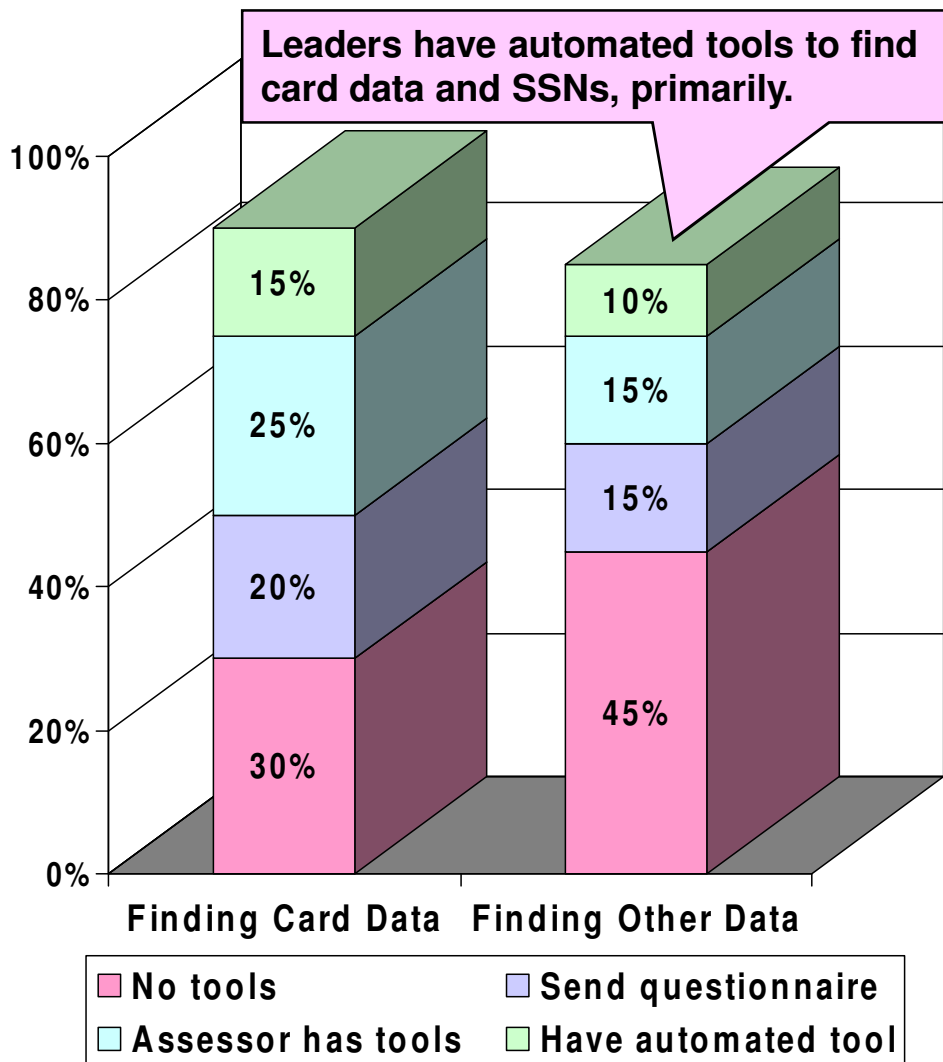
Leaders are Applying PCI Standards to Protect Other Sensitive Data



- We have a substantial loyalty program. We store an account number and a card number for the loyalty program. Some properties also collect a SSN or Drivers License number as customer IDs. These numbers are not encrypted or masked yet. Our compliance project only applies to card numbers (Source: Level 1 Hospitality Co).
- **LEADER'S VIEW:** 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, May 2008

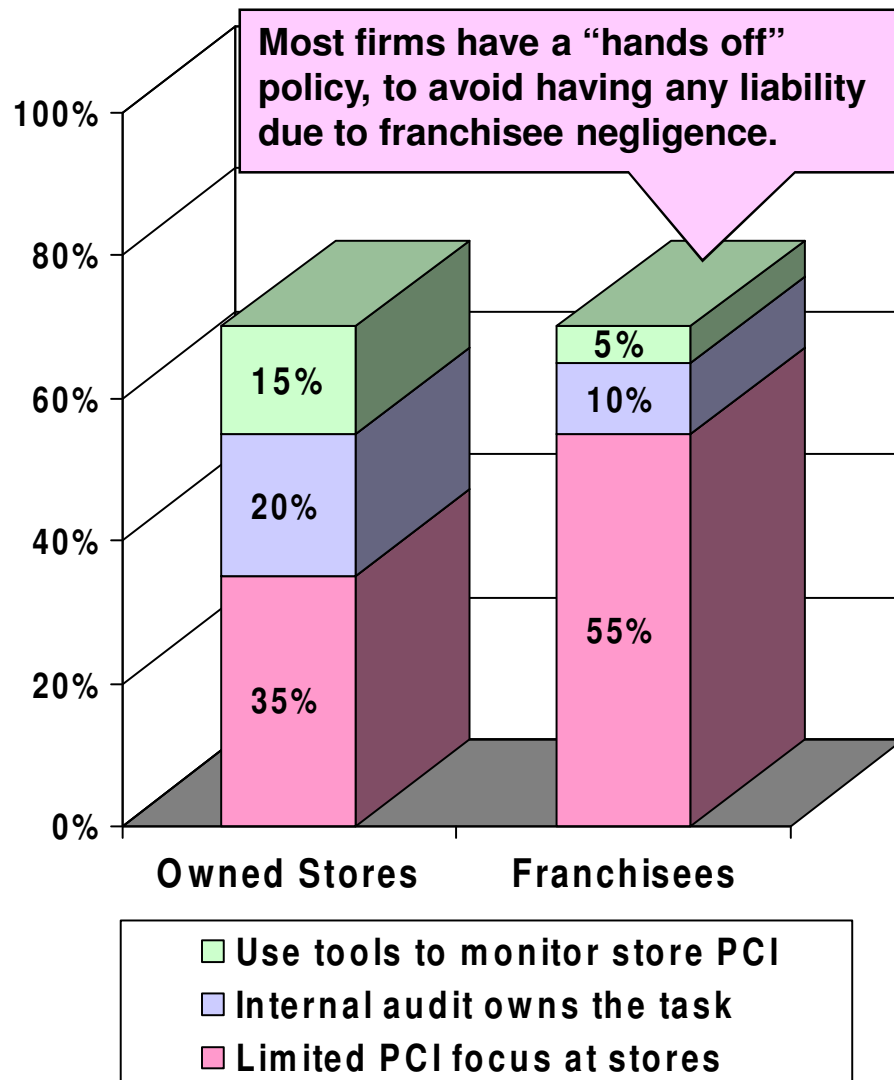
Leaders Have Tools to Find their Confidential Data to Secure it



- 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).
- **LEADER'S VIEW:** 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).

Source: PCI Knowledge Base, May 2008

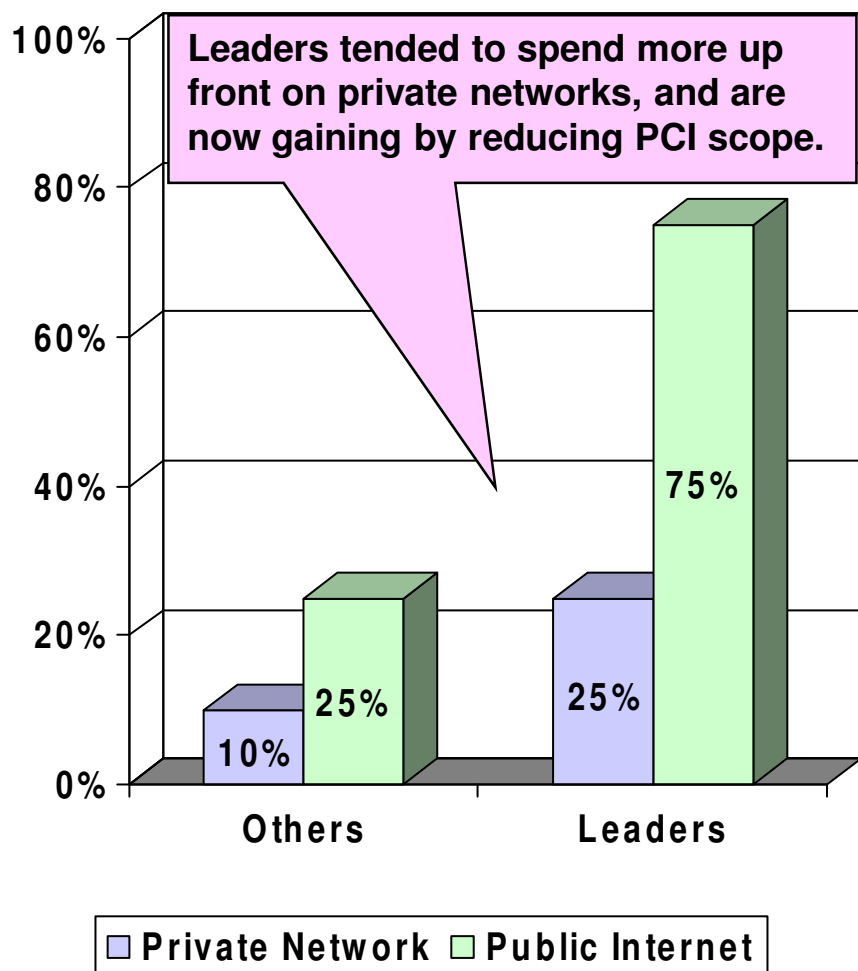
Leaders Have Tools to Monitor Security at Stores and Franchisees



- **LEADER’S VIEW:** 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).

Source: PCI Knowledge Base, July 2008

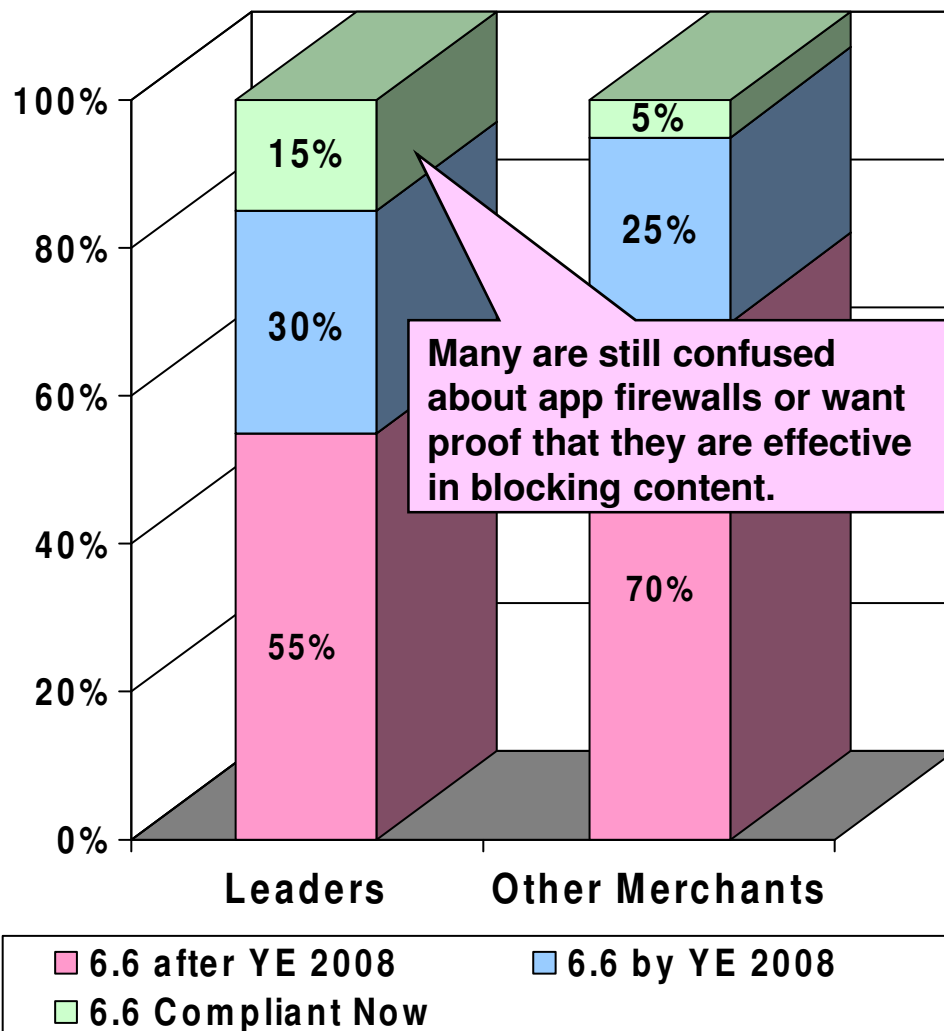
PCI 1.2: Unencrypted Data on Private Nets is OK, But Not Very Secure



- **LEADER'S VIEW:** We used Savvis to build us a private retail network within their ATM cloud. Our network was VPN encrypted within their private ATM cloud, and had private links into our stores (Source: Level 1 Retailer).
- **LEADER'S VIEW:** We have a fully private, segmented ATM network. We invested a lot several years ago to deploy the private network. I consider that one of our best practices (Source: Level 1 Merchant).
- We have a hub and spoke, private network to the stores. There is no public internet connectivity in the stores. Our QSA still said we had to encrypt data over the private network (Source: Level 1 Restaurant Chain).

Source: PCI Knowledge Base, May 2008

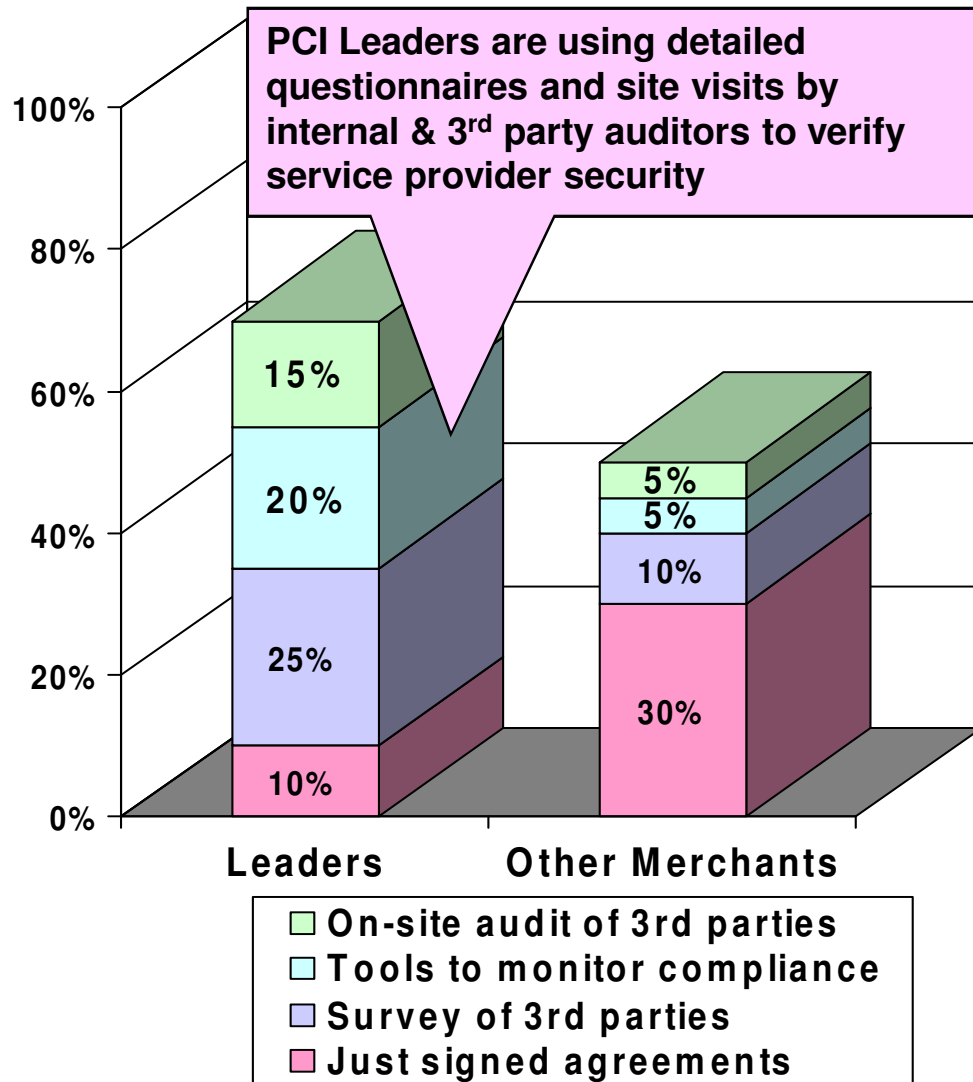
Only a Minority of Merchants, SPs and Banks Currently PCI 6.6 Compliant



- PCI has been baked into our security priorities for the past 3 years. We're starting our 2008 PCI project plan, which will be focused on meeting PCI 6.6 (Source: Level 2 Service Provider)
- We're looking at PCI 6.6 as a chunk of this year's budget. We'll probably get the FW appliance, rather than do the external code review. The appliance seems easier to implement and will cost less, based on the research I've done (Source: Level 2 merchant.)
- For requirement 6.6, we tell some companies they will need a compensating control by mid-year. Some firms have already written their CCs, because their applications will not pass (Source: PCI Technologist).

Source: PCI Knowledge Base, May 2008

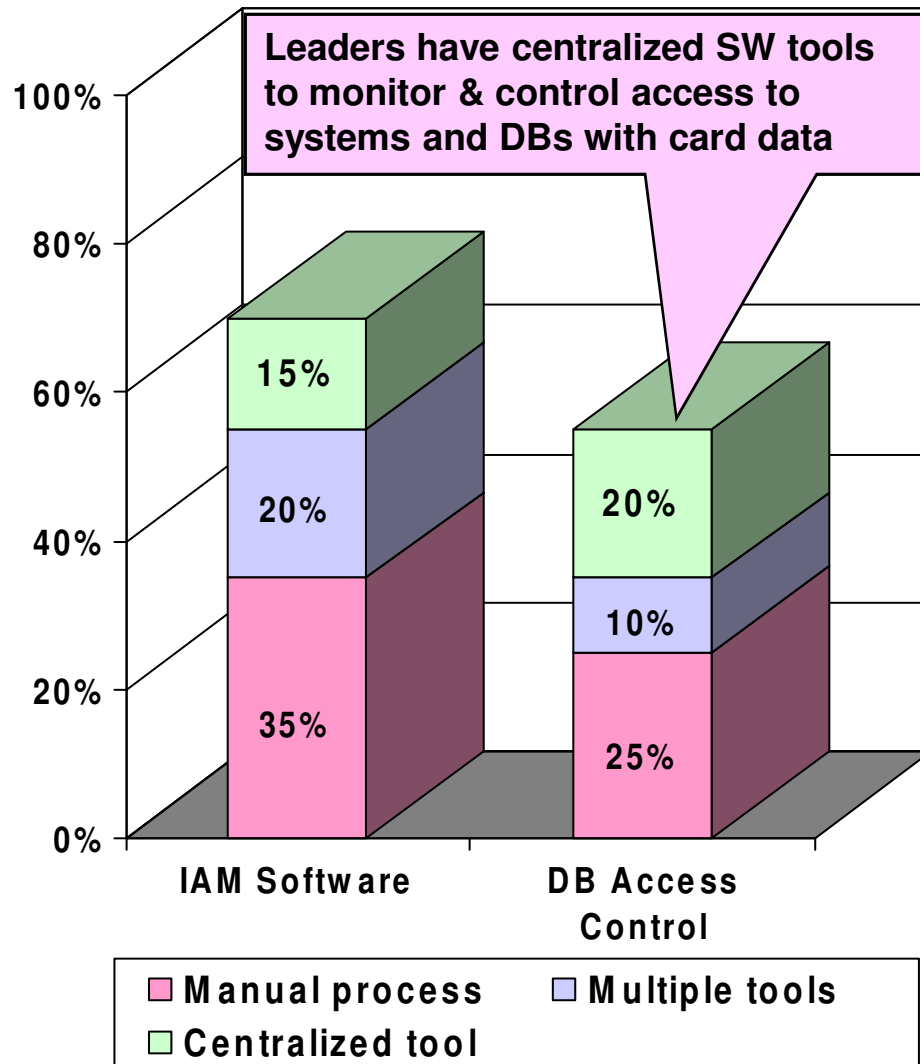
Leaders Use Tools for Due Diligence of Suppliers' & Partners' Security



- **LEADER'S VIEW:** 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).

Source: PCI Knowledge Base, May 2008

Leaders Have IAM & DB Access Tools to Track Individual Access to Data



- Our access control management is mostly manual. In addition to being required by PCI, this is also required by SOX and SAS 70. So, whenever anyone changes depts. or leaves the company, we have a person who makes all those changes. It's a labor-intensive task (Source: Level 1 Service Provider).
- We still handle ID management on a system by system basis. We have no centralized management. That means I wind up talking to each application or data owner and each system admin, to make sure who has access to each environment. I would not recommend this approach, but we can't justify the tools we need (Source: Level 4 merchant).

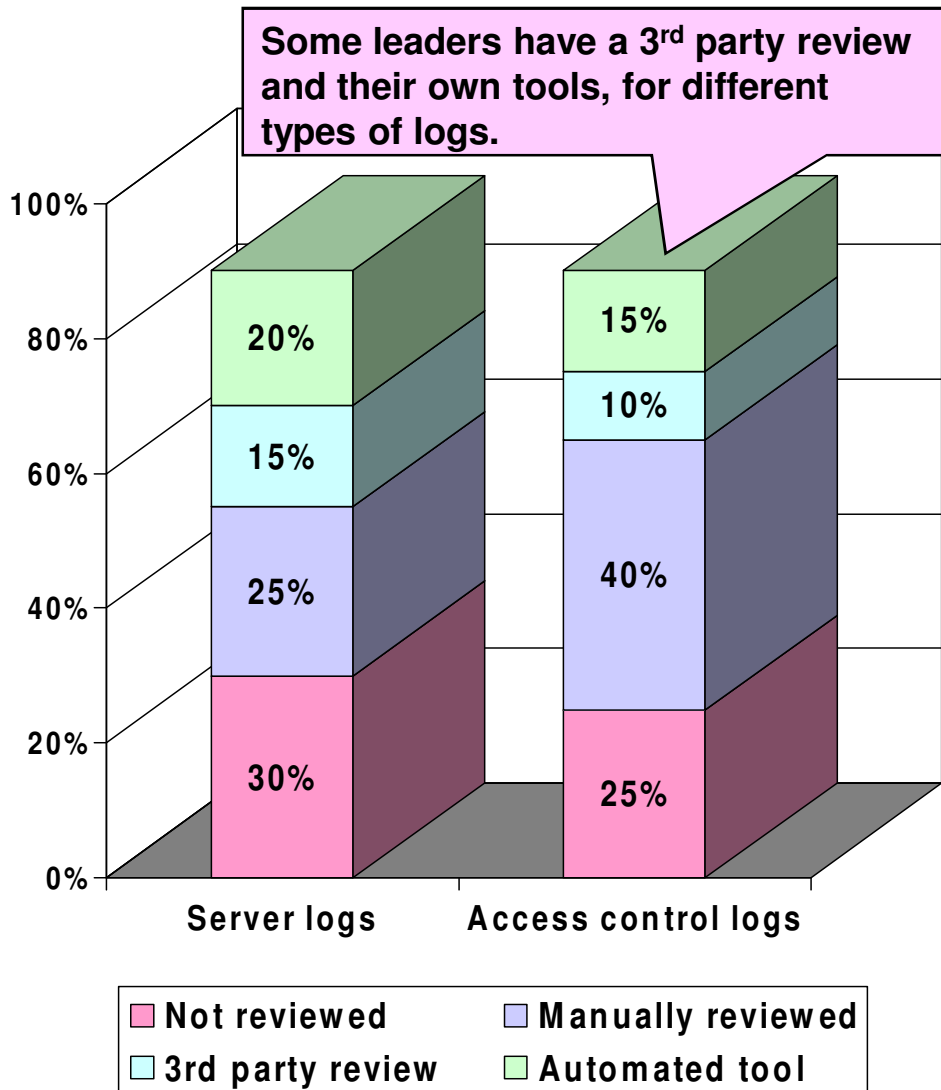
Source: PCI Knowledge Base, May 2008

Most Merchants and SPs Say They Cannot Keep Up with Log Monitoring

1. The volume of data generated by network access controls, intrusion detection systems, file integrity monitoring, database access controls, etc. is overwhelming all security managers, even those with the largest staffs.
2. PCI doesn't require that all this data be centralized and monitoring be automated, but if it isn't, there's very little value in collecting the data in the first place.
3. This is the major value of a strategic approach to achieving compliance.



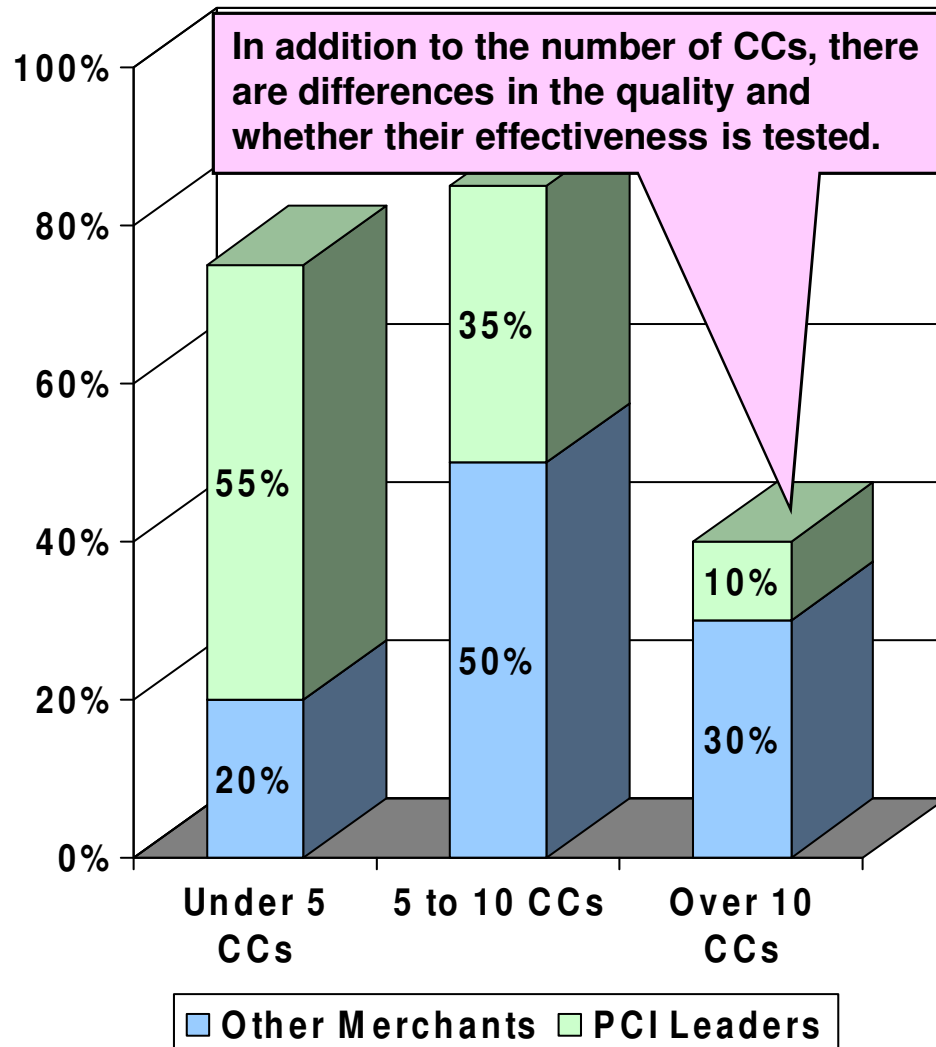
Leading Merchants Have Tools to Review & Analyze Security Logs



- **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).**

Source: PCI Knowledge Base, May 2008

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).

Source: PCI Knowledge Base, May 2008

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

4

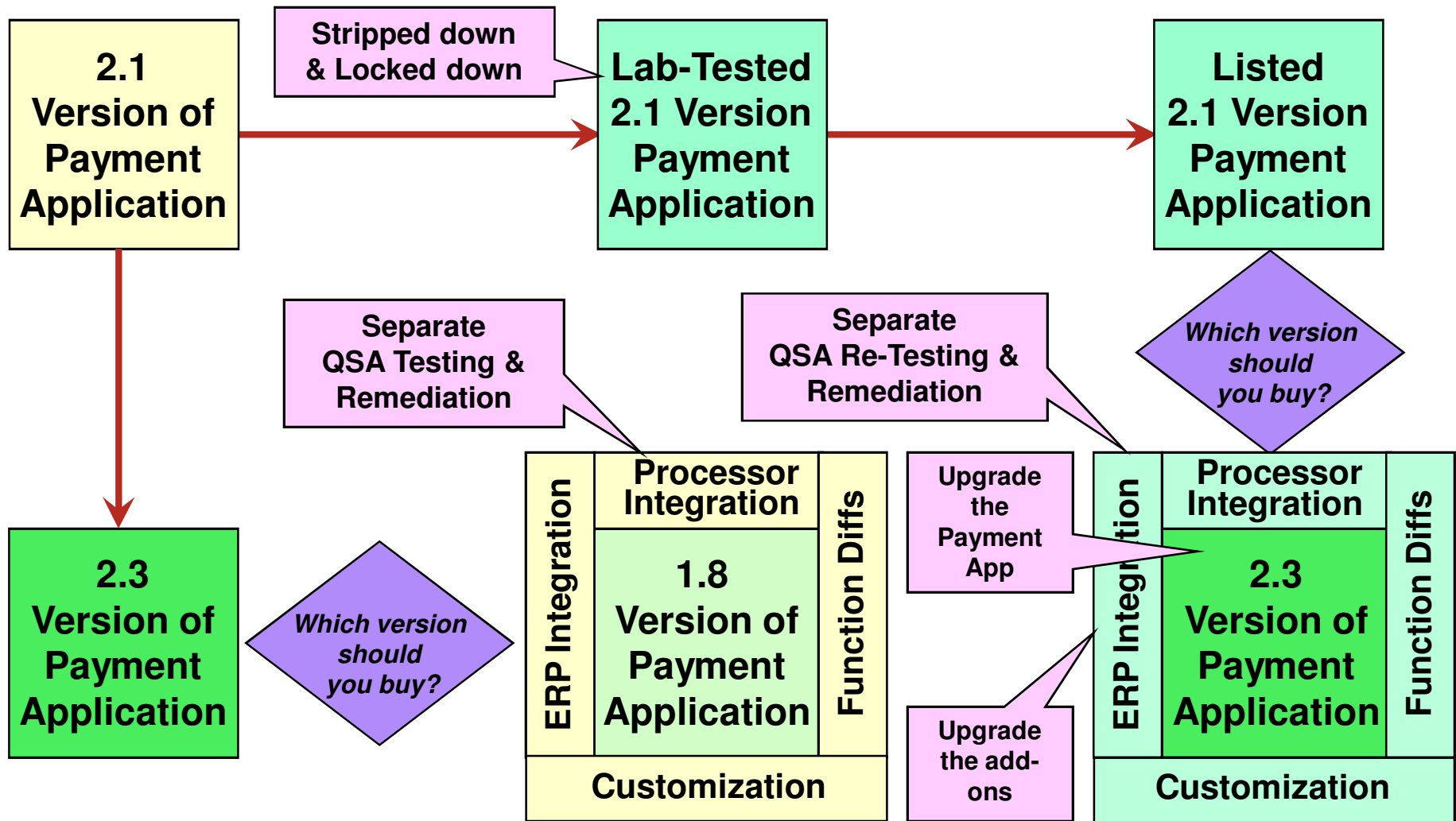
<i>Phase</i>	<i>Compliance Mandates</i>	<i>Effective Date</i>
I.	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (“VNPs”) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/08
II.	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.

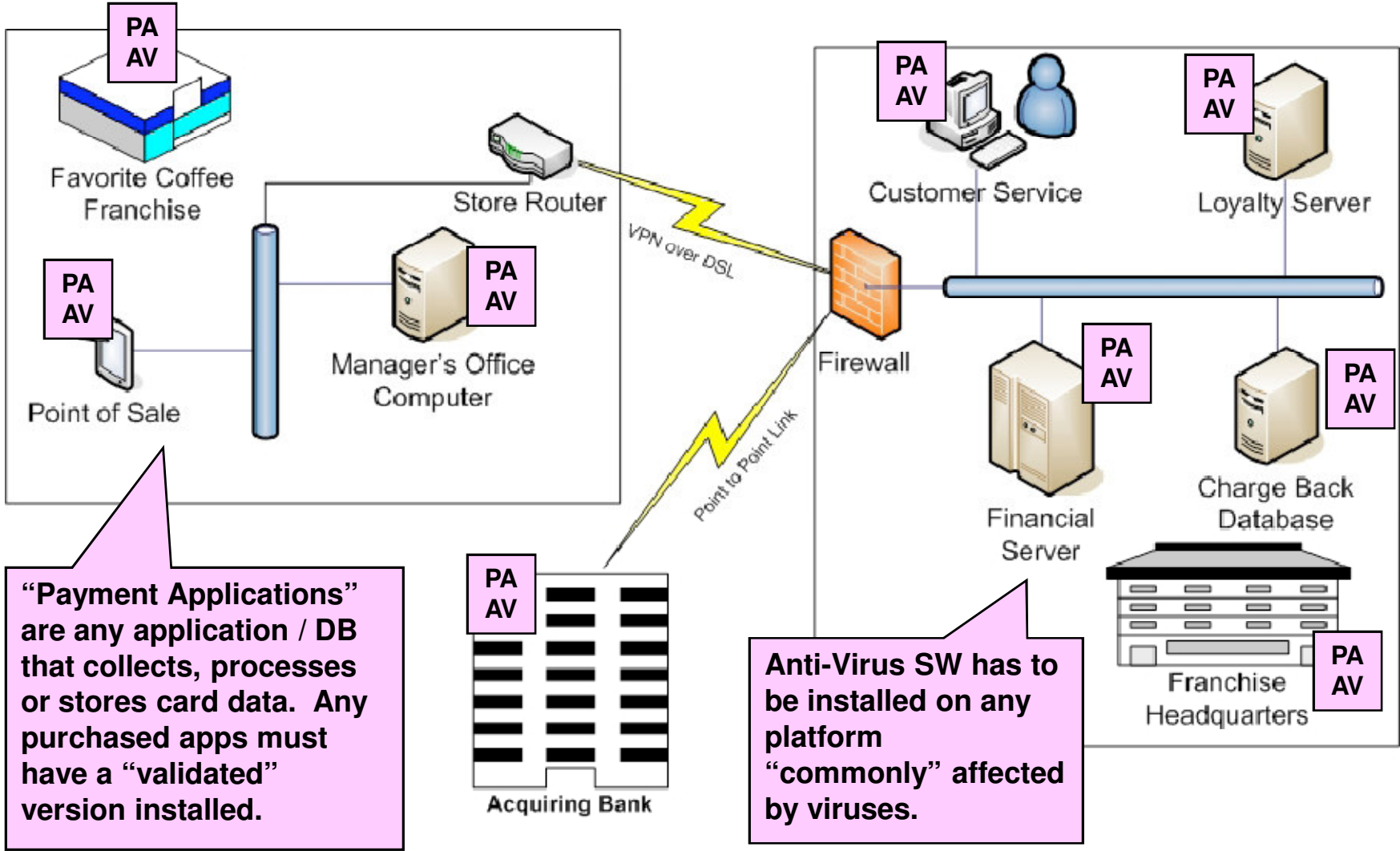
Source: PCI Security Standards Council, May 2008

You Should Look Beyond the PA DSS “List” of Compliant Applications



Source: PCI Knowledge Base, September 2008

Pervasive Impact of AV Change and PA DSS Validation Requirements



“Payment Applications” are any application / DB that collects, processes or stores card data. Any purchased apps must have a “validated” version installed.

Anti-Virus SW has to be installed on any platform “commonly” affected by viruses.

Source: PCI Knowledge Base, September 2008

What's in it For Level 4s to Get PCI Compliant? Competitive Edge

Level 4 Merchant Driver #1: Competitive Advantage

Case: A Level 4 Mortgage Services company – Processes credit cards for up front fees. Not required to be compliant, yet.

Motivator: When customers and prospects started asking if they were compliant, the first time they lost an account, upper management decided that we need to get compliant, then use compliance as a way to take business from other mortgage companies.

Cost: Because they only had card data in one system, the costs were under \$10K, using open source software and by purging all data not absolutely necessary.

Bottom Line: Achieved compliance in under 3 months, mainly by doing a self assessment and improving the documentation of their security procedures.

Source: PCI Knowledge Base, September 2008

What's in it For Level 4s to Get PCI Compliant? Brand Preservation

Level 4 Merchant Driver #2: Brand Preservation

Case: A Level 4 Consumer Package Goods Company – Launched an E-Commerce business unit that sells direct to consumers.

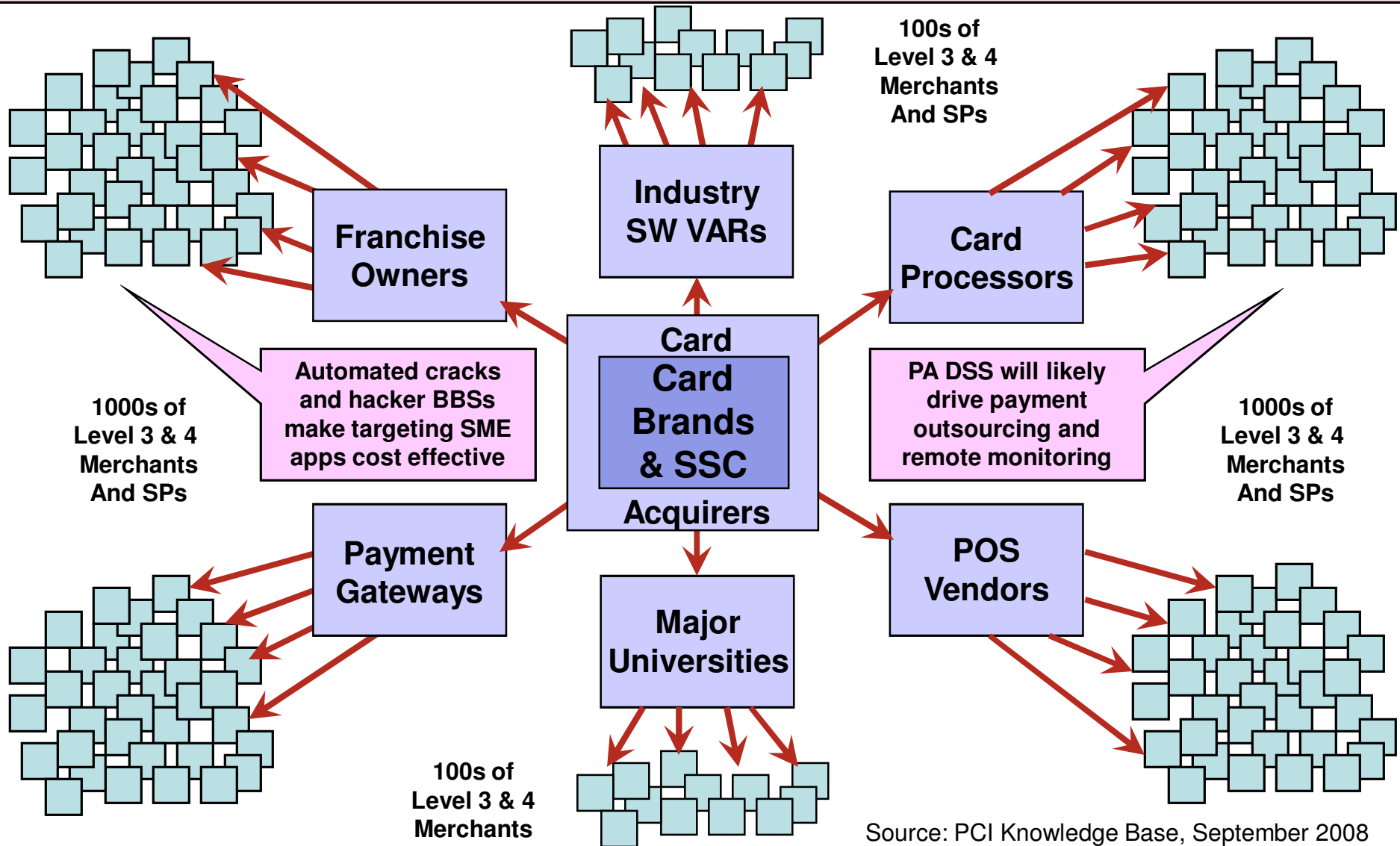
Motivator: Had a minor breach that served as a “wake up call,” to the importance of security, then went beyond minimal PCI compliance, driven by management’s belief that they could turn the negative (the breach) into a positive – an online store that promotes customer security.

Cost: The Web Commerce group outsourced their payment processing, costing under \$2K per month. Internal spending was focused on training of employees and marketing the more secure online store.

Bottom Line: Achieved compliance in under 6 months, with most of the effort related to documenting policies and procedures.

Source: PCI Knowledge Base, September 2008

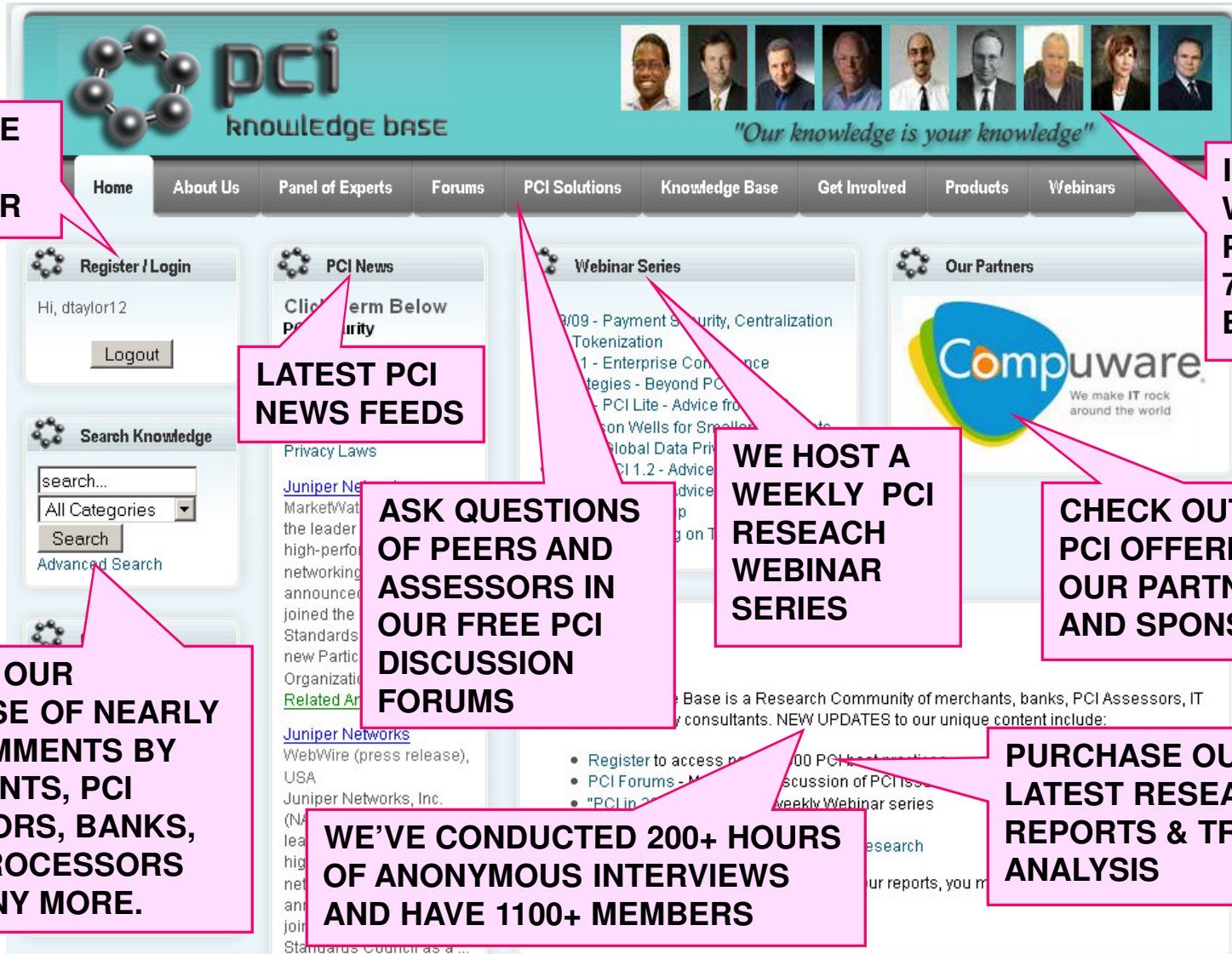
Level 4s: Driving and Monitoring Compliance of SME Merchants & SPs



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.

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 COMMENTS BY MERCHANTS, PCI ASSESSORS, BANKS, CARD PROCESSORS AND MANY MORE.

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



Share Your Knowledge

To join our knowledge sharing program, visit the PCI Knowledge Base.



Contact:

Dr. David Taylor, CISSP
Founder, PCI Knowledge Base
David.Taylor@KnowPCI.com
203-569-7951