



PRESENTS:

“The PCI Leadership Report”

The Latest Findings from the PCI Knowledge Base

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

Today's Presenters



Chrisan Herrod
Executive Editor



Dr. Dave Taylor, CISSP
Founder PCI Knowledge Base



The Compliance Authority.com



The Compliance Authority.com is focused on Best Practices in IT Governance, Risk, and Compliance. Our web portal and digital magazine provide independent articles written by industry thought leaders and subject matter experts who are Compliance Authorities. We are an independent publication begun in 2006.

TCA sponsors a series of Thought Leadership Webinars focused on Corporate Governance, Risk, and Compliance (GRC).

WEBINARS are designed to be educational and informative with an emphasis on new information resulting from primary research.

Attendance at our WEBINARs provides CPE credit for your SOX, ISACA, and ISC2 certifications through the University of Fairfax.



<http://www.thecomplianceauthority.com/>

2008 GRC Thought Leadership Webinars

- **23 January**—available on our Website and on SOX Institute Website
 - IT Governance and The Board of Directors
- **12 March**—available on our Website and on UOF Website
 - Measuring the ROI for IT GRC Automation
- **26 August**
 - The Evolving Role of Risk Management—defining Enterprise Risk Management in the context of Corporate Governance
- **17 Sept**
 - New and Used—Frameworks and their role in Corporate GRC business processes
- **12 Nov**
 - The land of opportunity—how Green IT initiatives will affect your Corporate GRC programs

Today's Presenters



Chrisan Herrod
Executive Editor



Dr. Dave Taylor, CISSP
Founder PCI Knowledge Base



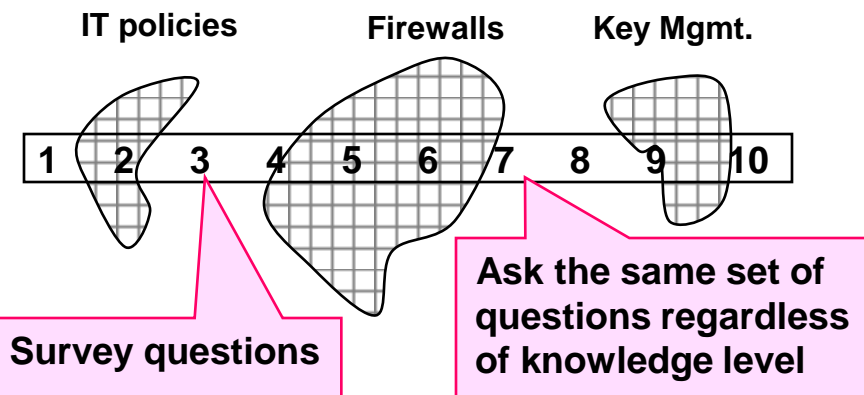
The PCI Knowledge Base Research Process

- **First, we assume you are already familiar with the PCI standards.**
- **If not, visit www.PCIStandards.org and download them.**
- **This presentation is based on over 100 hours of 1-on-1 interviews.**
- *We conduct 1-on-1, anonymous interviews with people who know all different areas of PCI: merchants, PCI assessors, acquiring banks, security technologists, PCI consultants & service providers – our “Panel of Experts.”*
- *Each interview is unique. We do not do surveys. There are no sample sizes. Our statistics are simply estimations, based on the trends which we see in the data, and supported by the trends that are identified by our panel of PCI experts.*
- **The purpose of statistics is simply to illustrate general trends, and we support them with direct commentary from the interviews.**
- **All of the anonymous interview results are available to review at www.KnowPCI.com. Access is free, but you must register.**
- **All data are coded post hoc, which enables us to create the charts.**
- **Our goal is to share our knowledge, and hope you will share yours.**

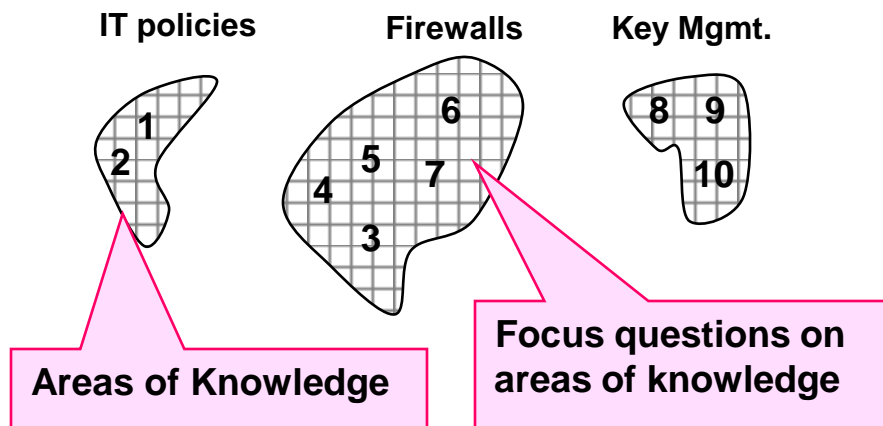
Source: PCI Knowledge Base, May 2008

Methodology: Survey Research vs. Knowledge-Based Research

Typical Survey Methodology



PCI Knowledge Base Methodology



- People's knowledge of complex subjects is not the same level across all areas of the subject. It is concentrated in specific areas
- PCI is a very complex subject, covering many different areas of security technology, as well as procedures, policies and business
- Surveys about complex subjects force a person to guess about some areas, while ignoring a person's in-depth knowledge in other areas
- The PCI Knowledge Base focuses its research process only on those areas where each person has in-depth knowledge, eliminating guessing and improving the accuracy of the results

Sources of the PCI Leadership Perspectives in This Report

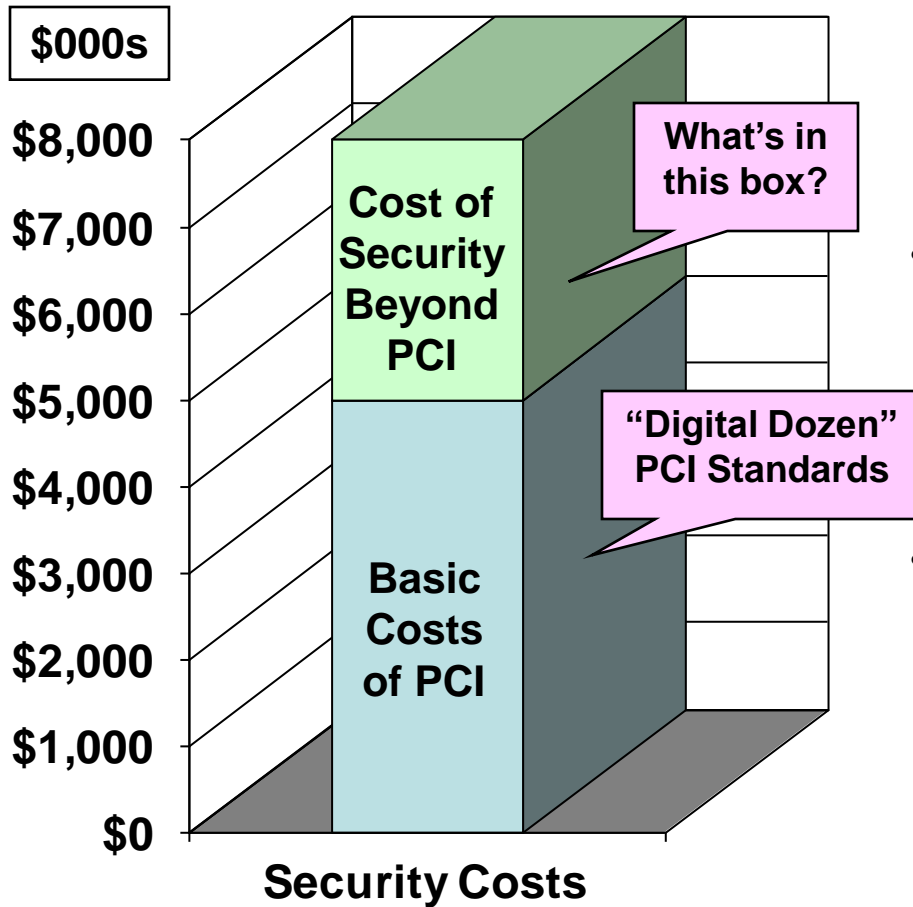
Knowledge Source	Defining PCI Leadership
Technology Managers	Implementing the management tools to alert me to potential problems in time to stop them
Internal Audit Managers	Automating monitoring and reporting to ensure continuous compliance
Banks / Card Processors	Protecting financial data to reduce risk of fraud
PCI Assessors	Ensuring policy enforcement and avoiding compensating controls
Vendor CTOs	Identifying and securing confidential data throughout the IT infrastructure
PCI Consultants	Integrating discrete controls and training staff to effectively utilize the data

Source: PCI Knowledge Base, May 2008

PCI Standards In Context

Why is PCI Leadership Important? Protection Against Breaches

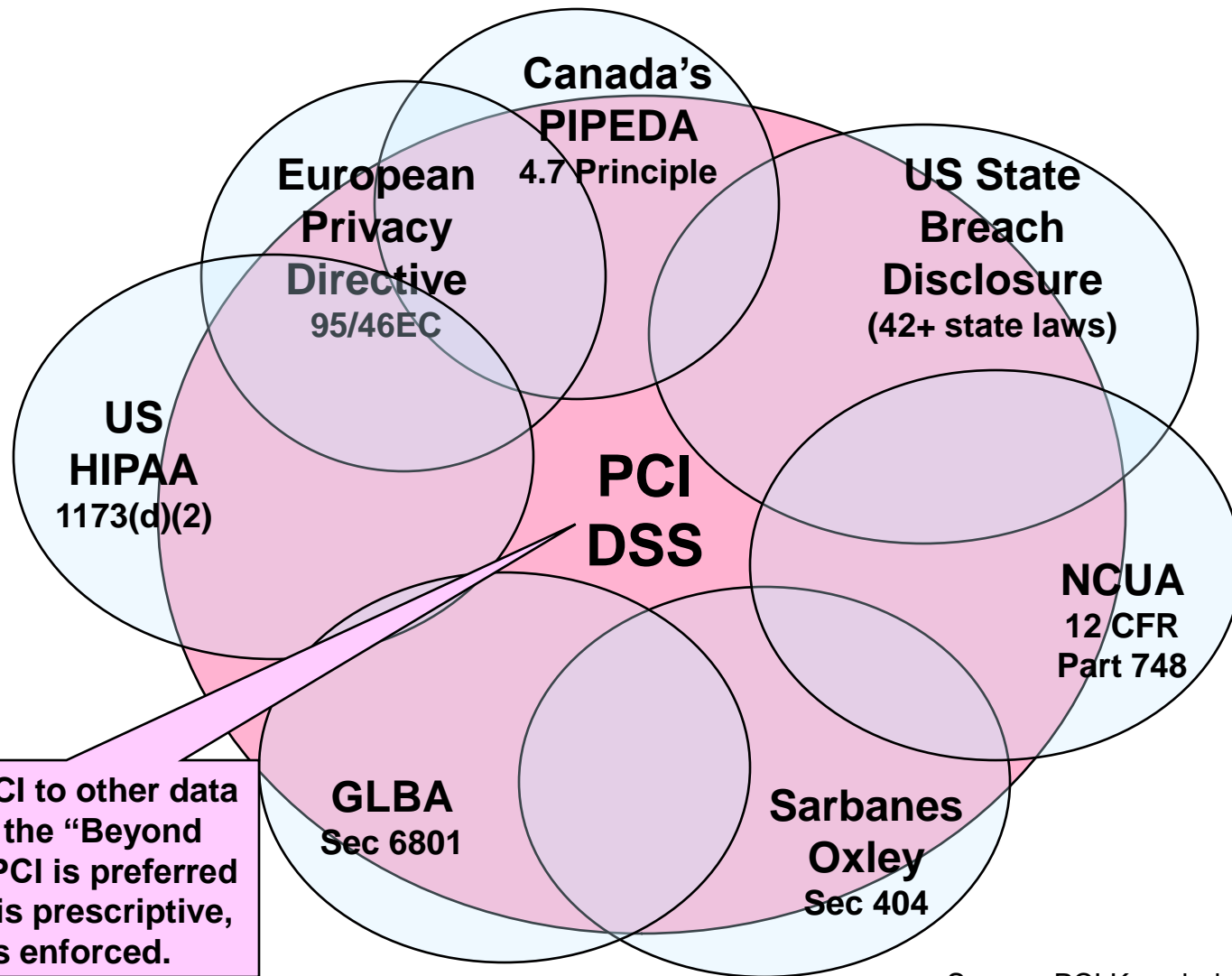
How Much Does it Cost to Secure Your Enterprise “Beyond PCI”?



- PCI Leadership is critical, because there can be a huge and meaningful difference between compliance with the PCI standards and the level of data security needed to protect an enterprise against security breaches.
- For example, the Hannaford grocery chain was PCI compliant and yet, **AT THE SAME TIME**, they had a security breach of 4.2 million credit card records.
- Hannaford’s CIO, Bill Homa, indicated that his company needs to go well beyond PCI to try and be secure. He predicted this effort would cost his department millions of dollars, “but not tens of millions.” The chart at left is an illustration of his point.

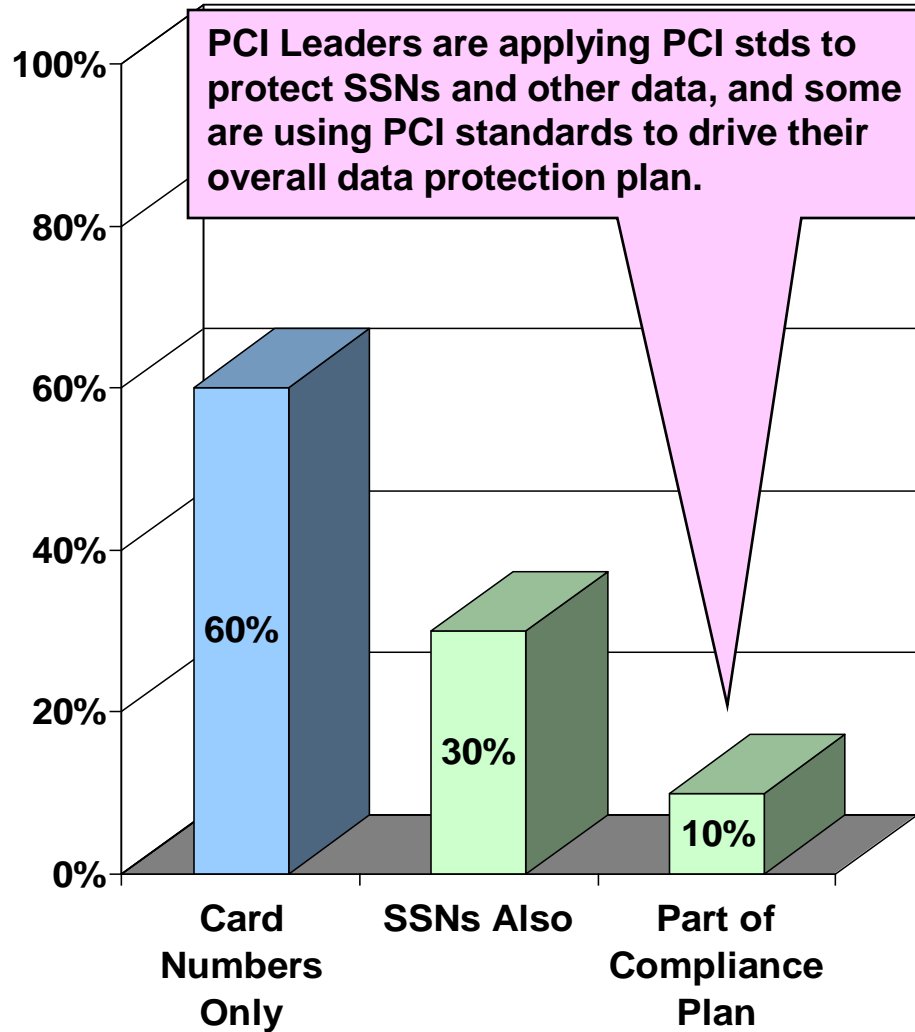
Source: PCI Knowledge Base and Storefront Backtalk, April 2008

Leaders are Leveraging PCI to Achieve Compliance with Other Regs.



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

PCI Checklist Products

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

PCI Leaders fight to get the tools they need to manage their biggest risks

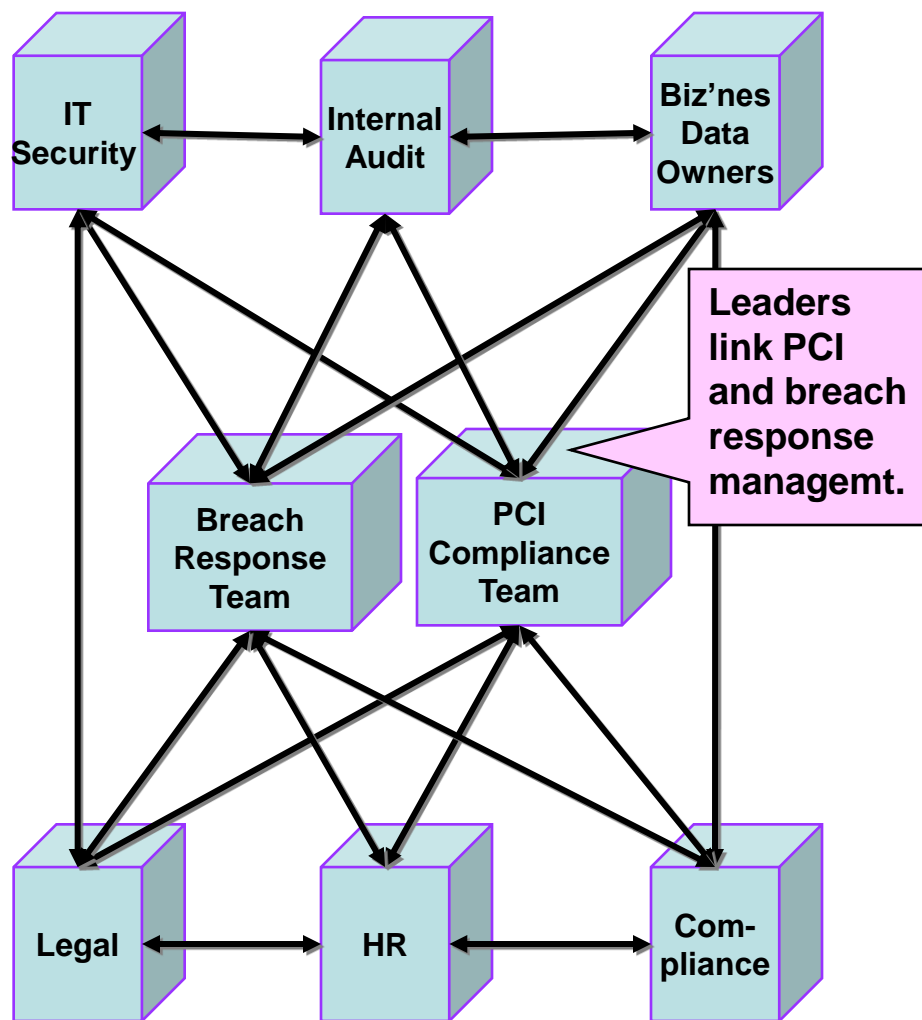
Strategic Products

- 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

Security Management

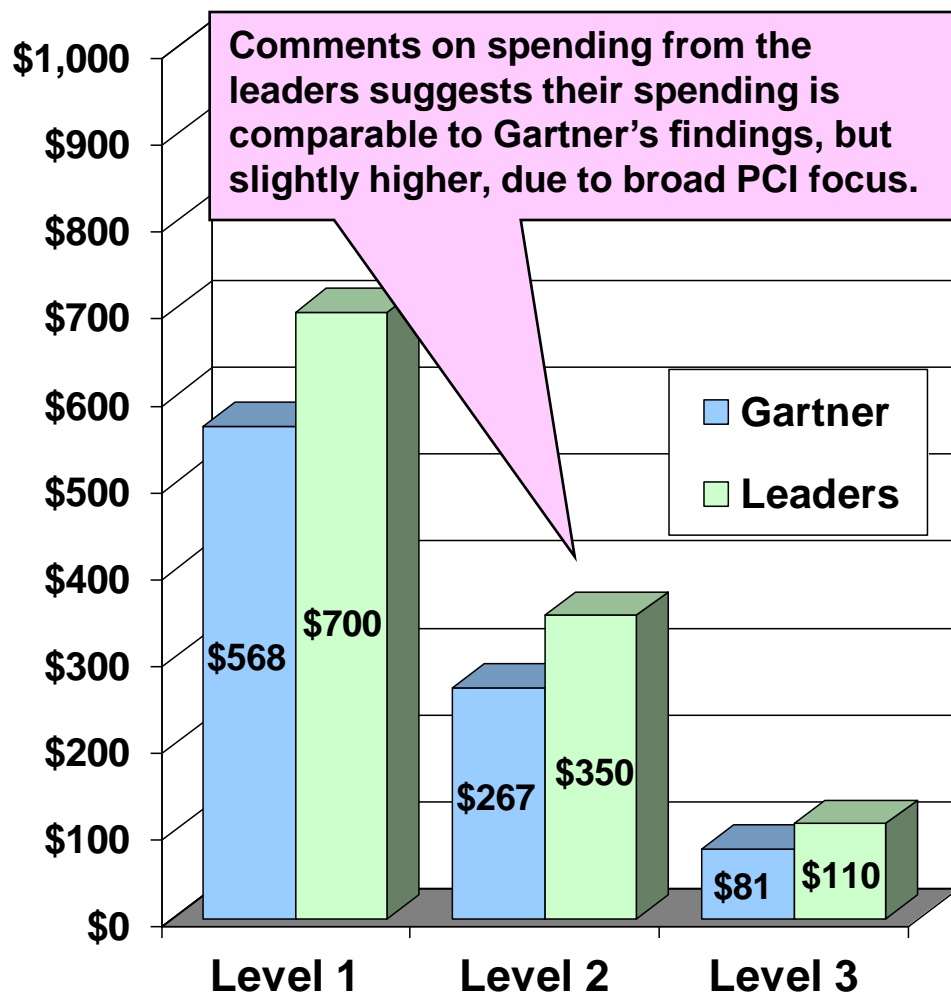
Leaders “Deputize” Internal Audit to “Operationalize” PCI Compliance



- **LEADER'S VIEW:** 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 would be 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. These people don't have the skills to do PCI auditing (Source: Level 2 merchant).

Source: PCI Knowledge Base, May 2008

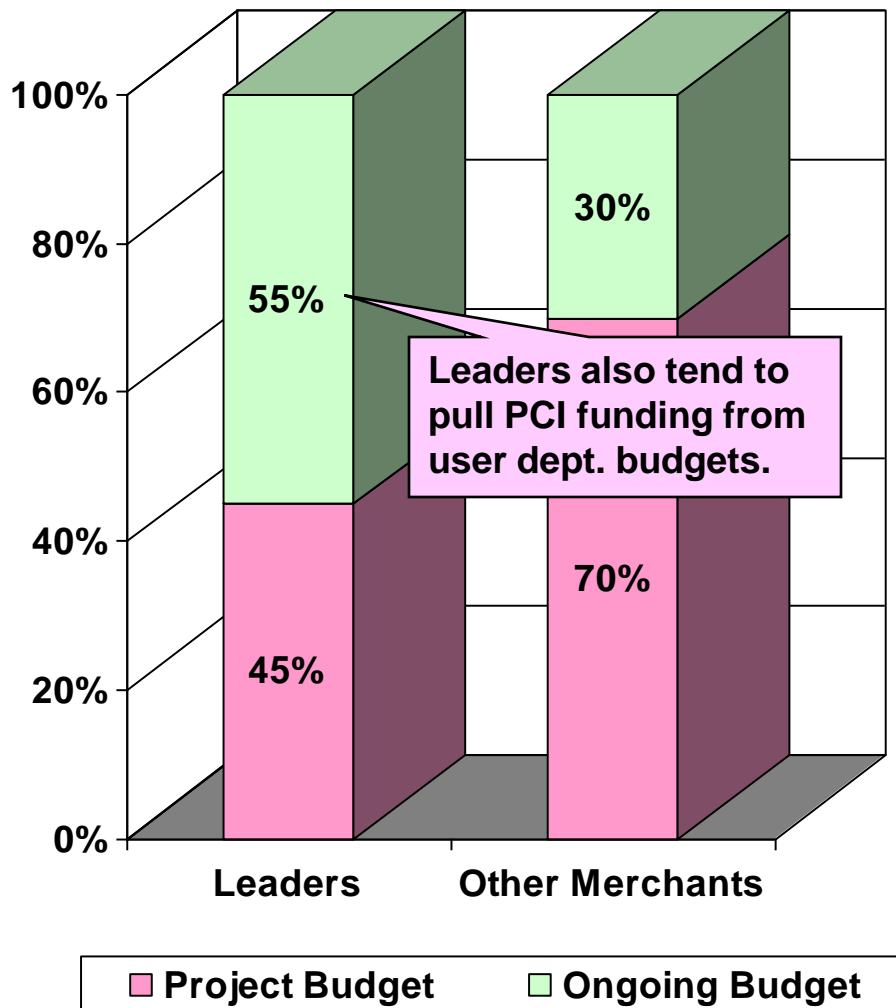
PCI Leaders Spend about 20% More Than Average, Per Gartner Study



- For 2008, our PCI project budget will be about \$350K, that's beyond salaries, and mainly to pay for the assessment and several specific software acquisitions (Source: Level 2 Merchant).
- Most of the money we spent on IT for PCI compliance was not in the "PCI Budget." That came from the IT budget, but those items got funded largely because of PCI. But the only things in the actual PCI budget were the costs of the assessment itself, and the network scans. Not even over \$50K per year. But the indirect spend would be several \$100K. (Source: Level 3 Merchant).

Source: PCI Knowledge Base, May 2008 and Gartner 2007

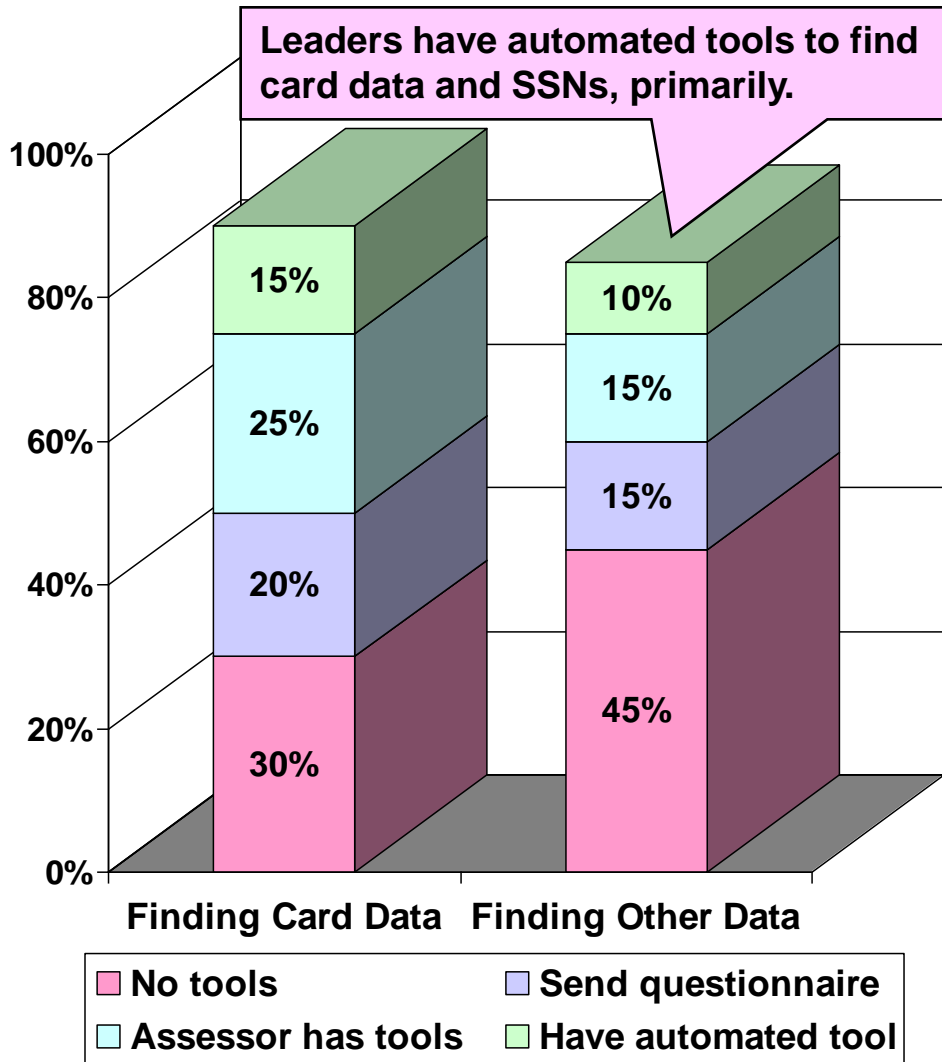
PCI Leaders Less Often Have “Project” Budgets & Spread Funding Wider



- **LEADER'S VIEW:** There is no PCI budget. What we buy, and the spending level, depends on what we're trying to accomplish. We're not driven as much by compliance. Our spending and vendor selection is based on a risk assessment (Source: Level 1 Merchant).
- **LEADER'S VIEW:** We had a PCI project budget for 2007. We used the money to buy some software and HW appliances. We also did training and got internal audit and finance departments involved in PCI compliance management. For 2008, we've added PCI into regular policies and procedures and assigned a person in IT operations to work on the PCI issues on ongoing basis (Source: Level 1 Retailer).

Source: PCI Knowledge Base, May 2008

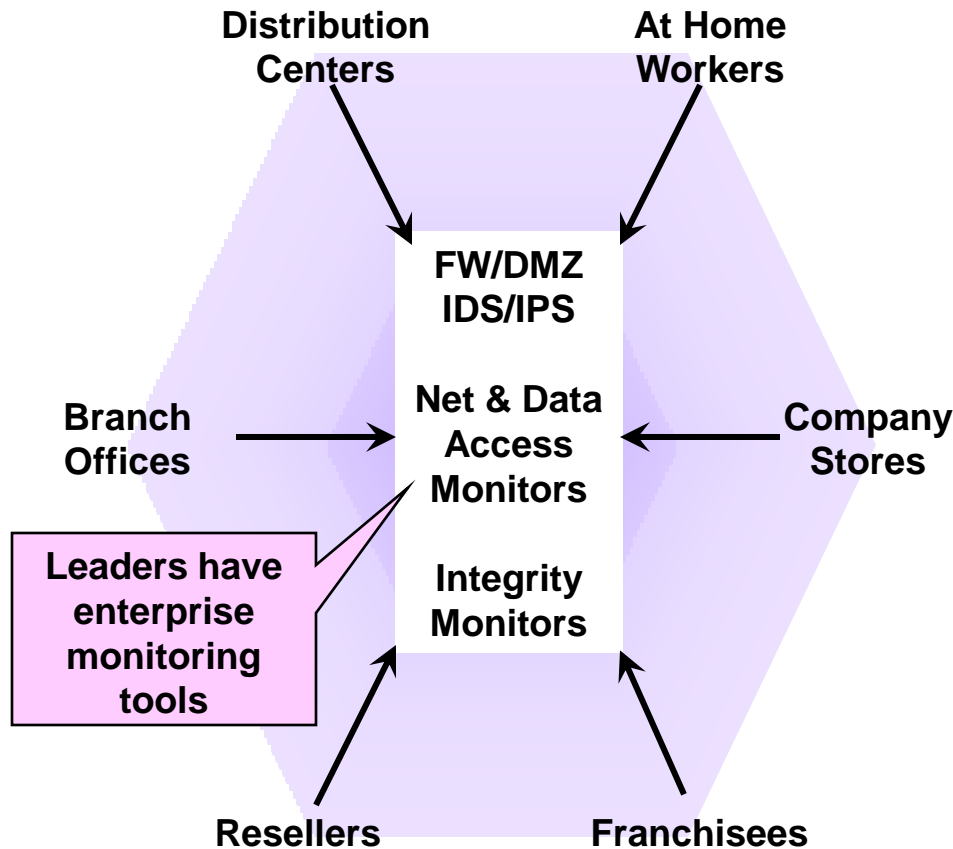
Leaders Have Tools to Find their Confidential Data to Secure it



- 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

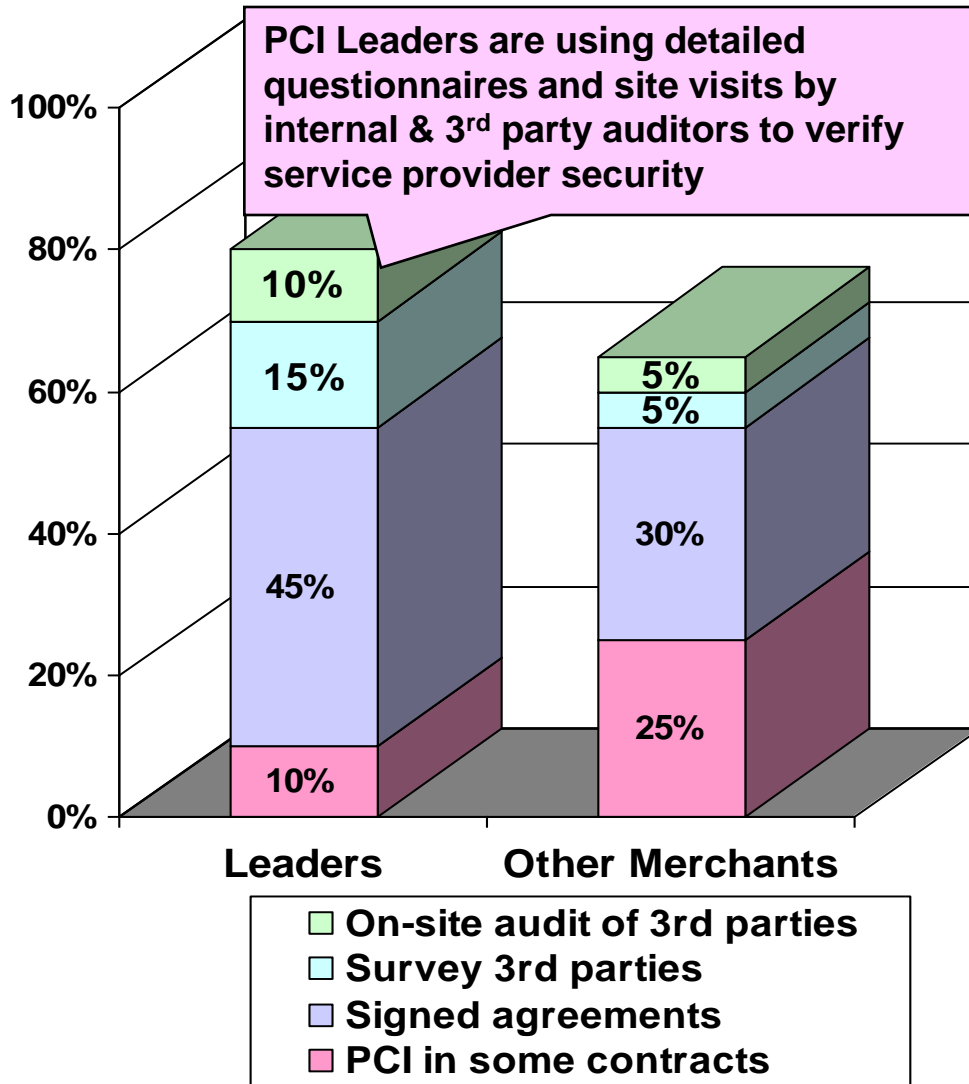
Leaders Have Higher Awareness of Remote Location Vulnerabilities



- When a company uses a tool to find rogue wireless networks, they typically only do it at corporate. Assessors often don't visit stores, but it's stores that offer the best opportunities for "war driving" (Source; PCI Consultant).
- 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).

Source: PCI Knowledge Base, May 2008

Leaders do Due Diligence of Their Suppliers' & Partners' Security

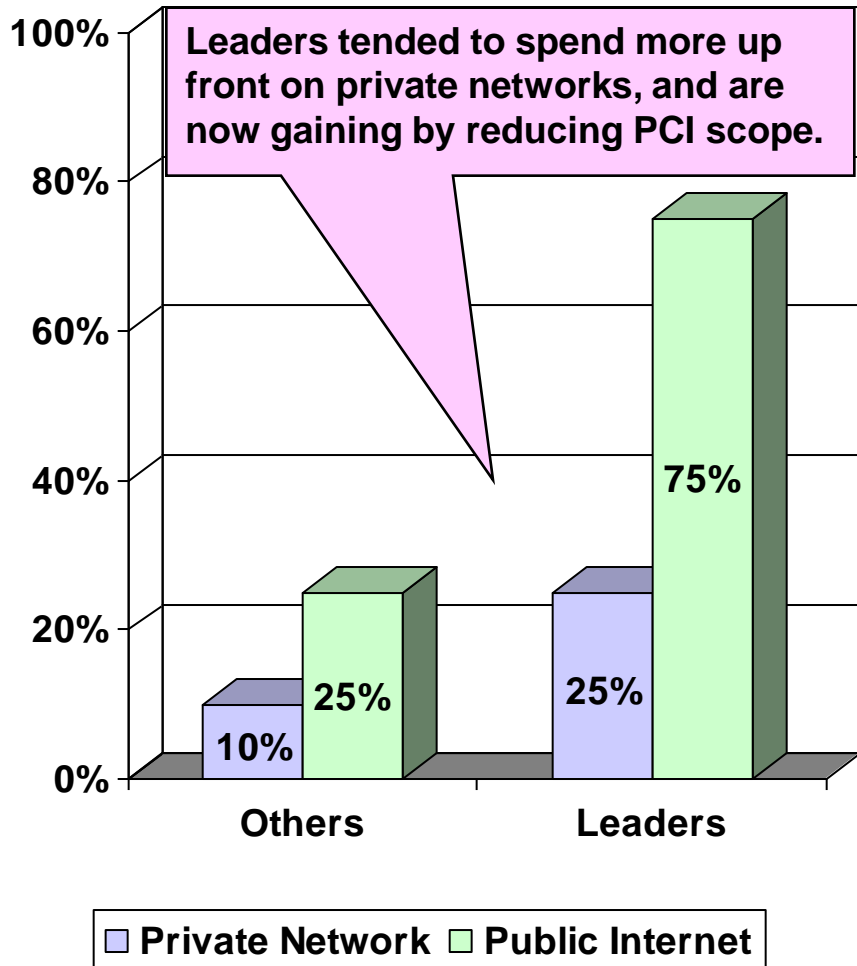


- **LEADER'S VIEW:** We make sure that PCI compliance is mentioned in all our service provider contracts. We also do due diligence and measure our service providers' security effectiveness. We have our own form for that. Having an industry standard would be better, but we cannot wait for that (Source: 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

Specific PCI Requirements

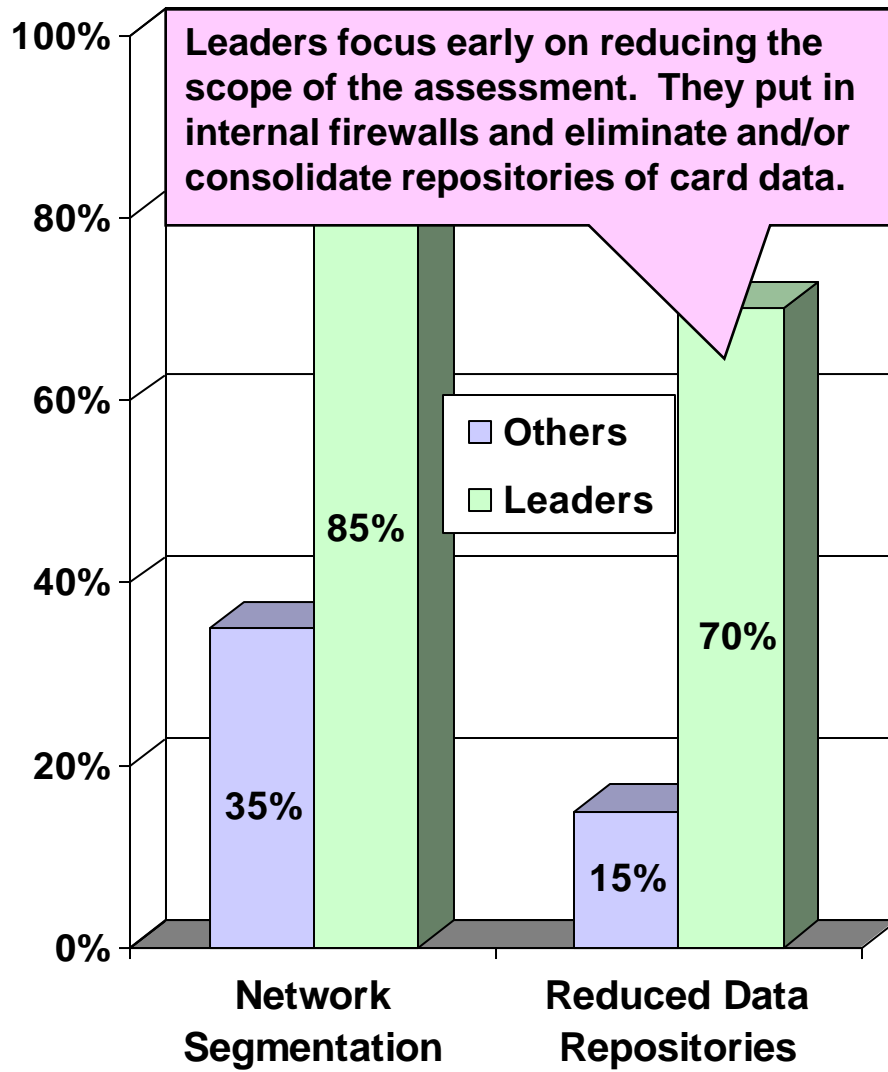
Leaders Using Private Networks to Stores, and Not Encrypting Traffic



- **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

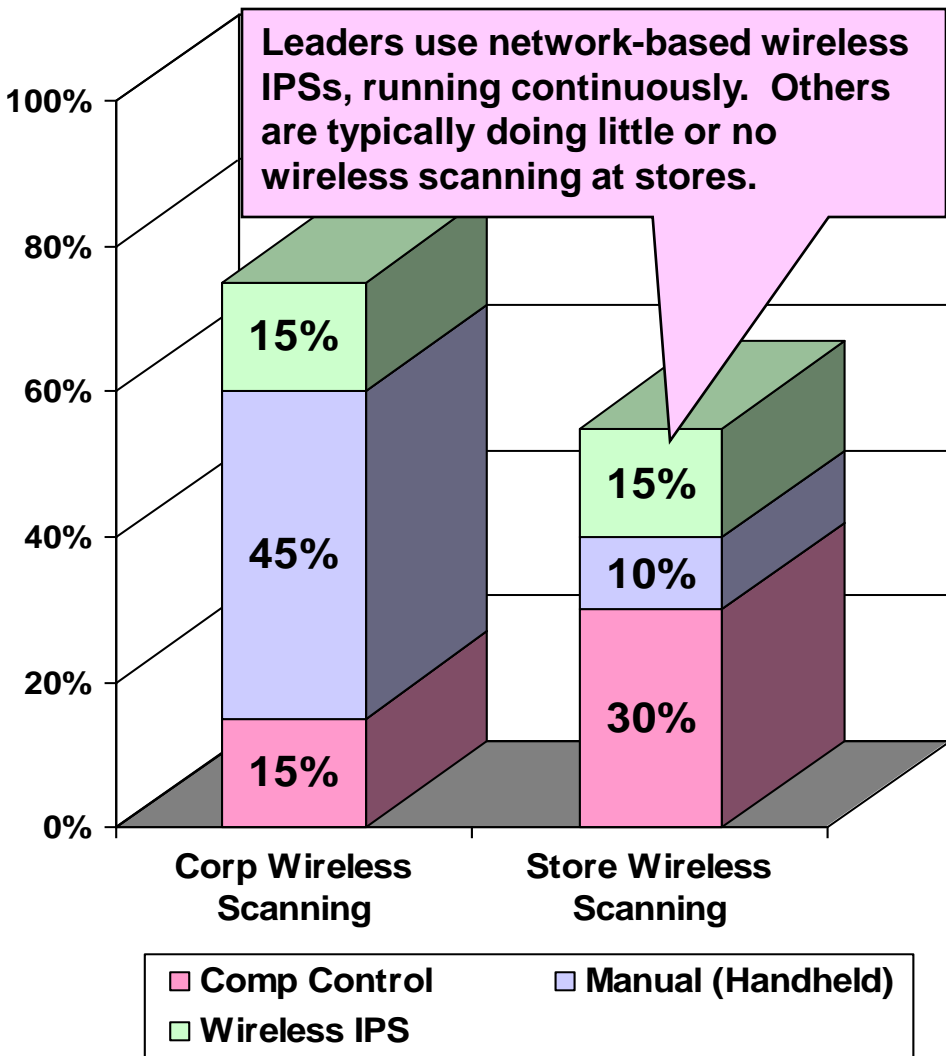
Leaders Have Reduced Scope & Costs by Segmenting their Networks



- **LEADER'S VIEW:** One of the best things we did was that our network was already segmented. We had created a DMZ, using a series of internal firewalls (Source: Level 1 Merchant).
- **LEADER'S VIEW:** My best advice for companies trying to achieve PCI compliance: Centralize all card data on the fewest possible platforms and servers, and segment those servers from the rest of the internal network using internal firewalls, then encrypt the card data on those servers where you absolutely must retain it (Source: Level 2 Merchant).

Source: PCI Knowledge Base, May 2008

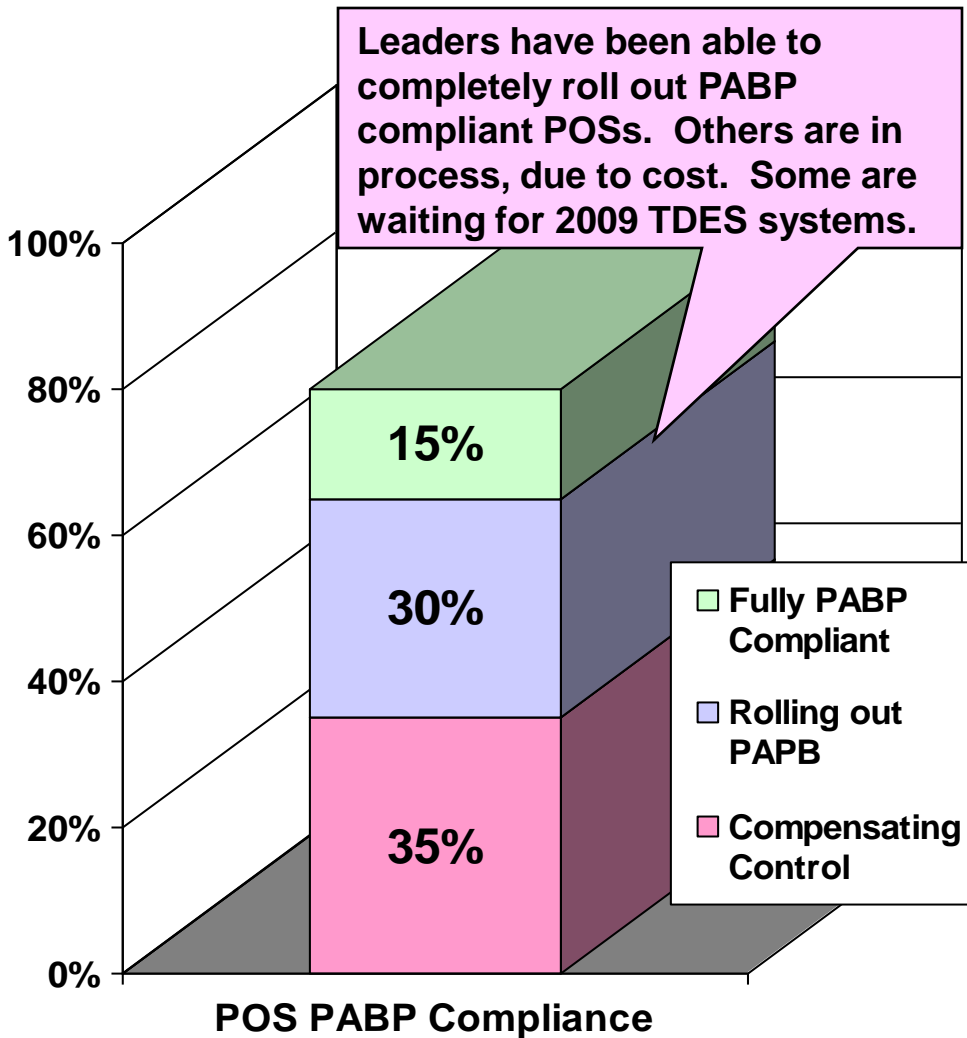
Leaders Have Tools Which do Daily Scans of their Wireless Networks



- 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

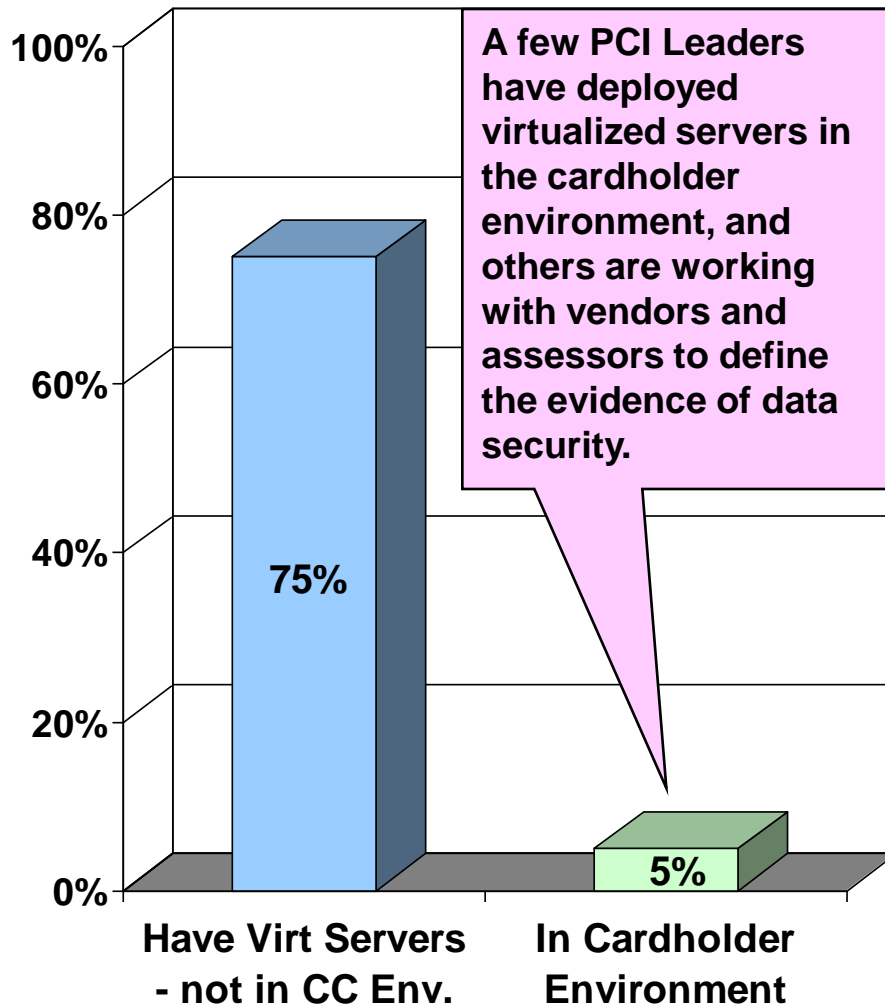
Leaders Have Upgraded Their POS Systems to PABP Compliance



- **LEADER'S VIEW:** We're replacing POSs at the company-owned stores. There are a dozen different POS configurations in the company owned stores (Source: Level 1 merchant).
- We have a variety of POS systems in our company owned and independent stores. We cannot justify a wholesale replacement of the POSs. We have used compensating controls for this (Source: Level 1 retailer).
- Upgrading POS in petroleum is a real problem. By 2009 they have to support 3DES encryption. The deployment process will cost the retailers \$1500 per terminal (Source: Processor).

Source: PCI Knowledge Base, May 2008

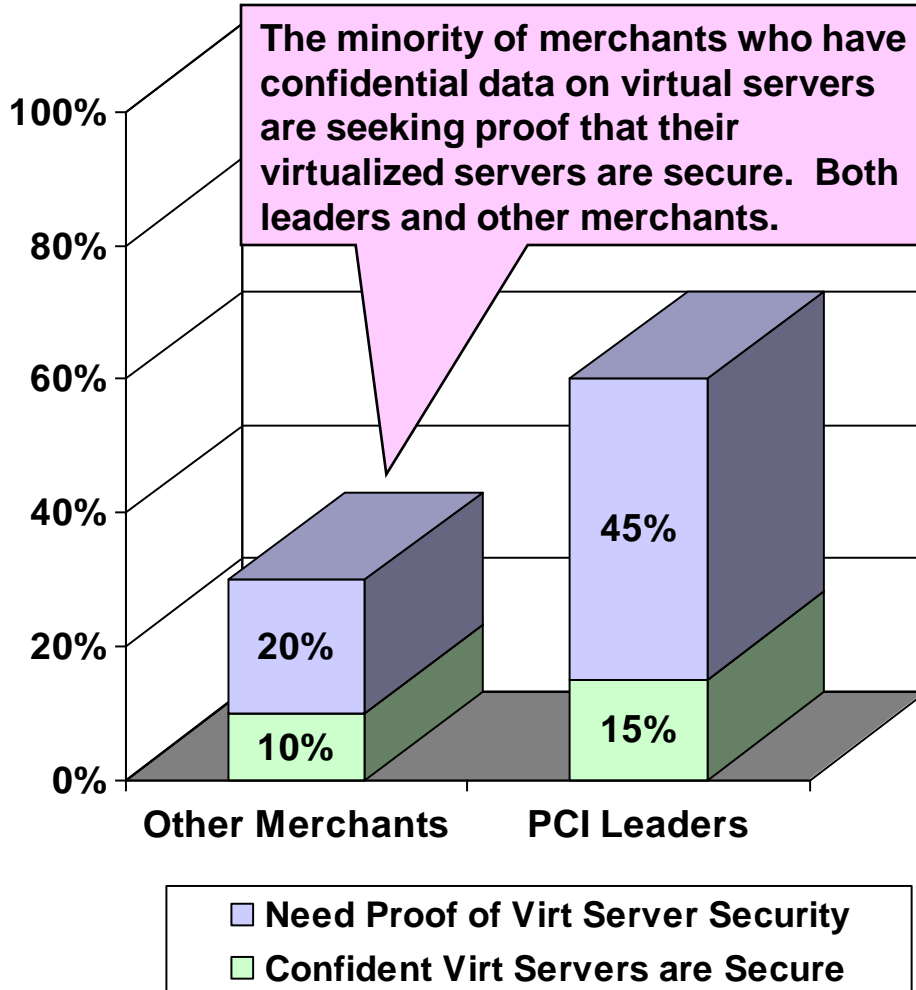
Some Leaders Have Virtualized Servers in the Cardholder Environment



- **LEADER'S VIEW:** We have server virtualization within the cardholder environment. But it does not affect PCI compliance, because we drive server configuration by the data classification policy (Source: Level 2 merchant).
- We are deploying more virtualized servers over 2008. We have not used them for applications involving card data because of the PCI requirement that servers have to be single function (Source: Level 1 merchant).
- If a company has virtualized servers, I would not want to see a mix of applications and data classes on the same physical server (Source: PCI Assessor)

Source: PCI Knowledge Base, May 2008

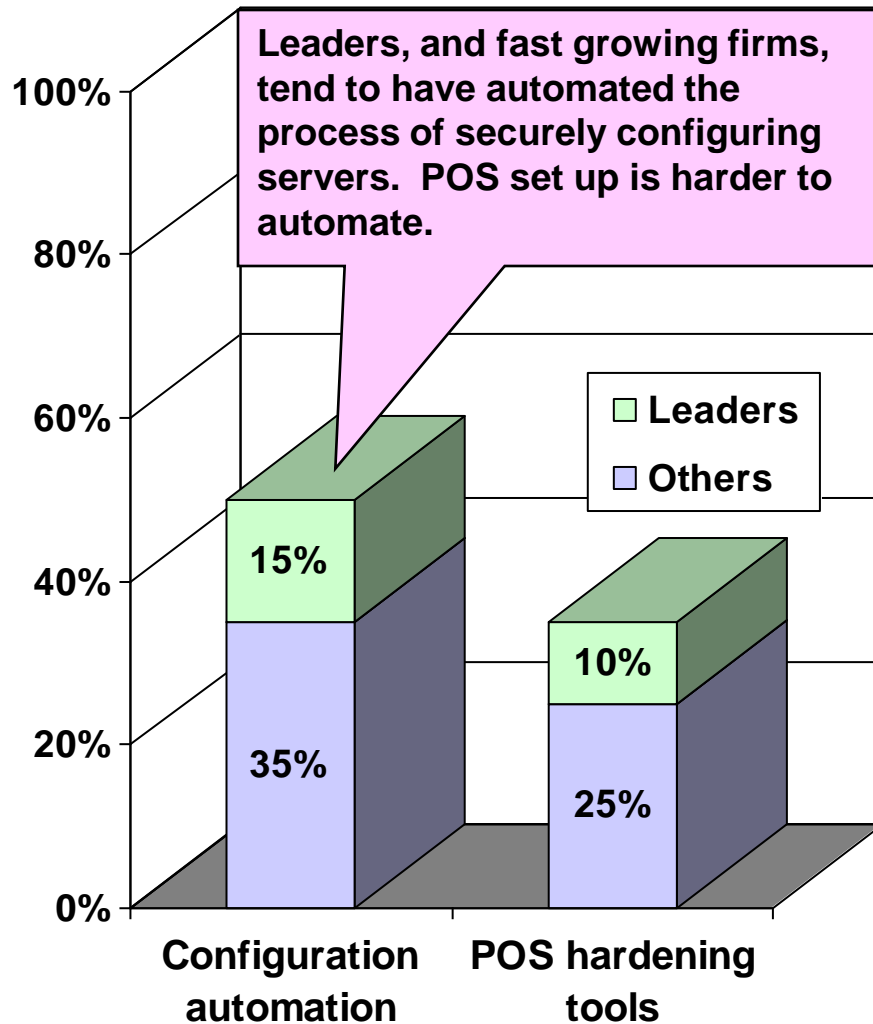
Very Few Merchants are Confident their Virtual Servers are Secure



- **LEADER'S VIEW:** We're deploying a couple of virtualized servers now. We're using Citrix's XenServer. We're running Netware, Windows and Linux VMs. VM security is going to be an issue for us because we have so much HIPAA and PCI - related data. We've been told they're secure. But we want more proof (Source: Level 2 merchant).
- We are implementing server virtualization using VM ware. We were told by the company that did our PCI gap analysis that if we implement virtual machines, that the other virtual machines on the same physical server are not in scope for PCI. But we still want to confirm that with Visa or an assessor (Source: Level 4 merchant).

Source: PCI Knowledge Base, May 2008

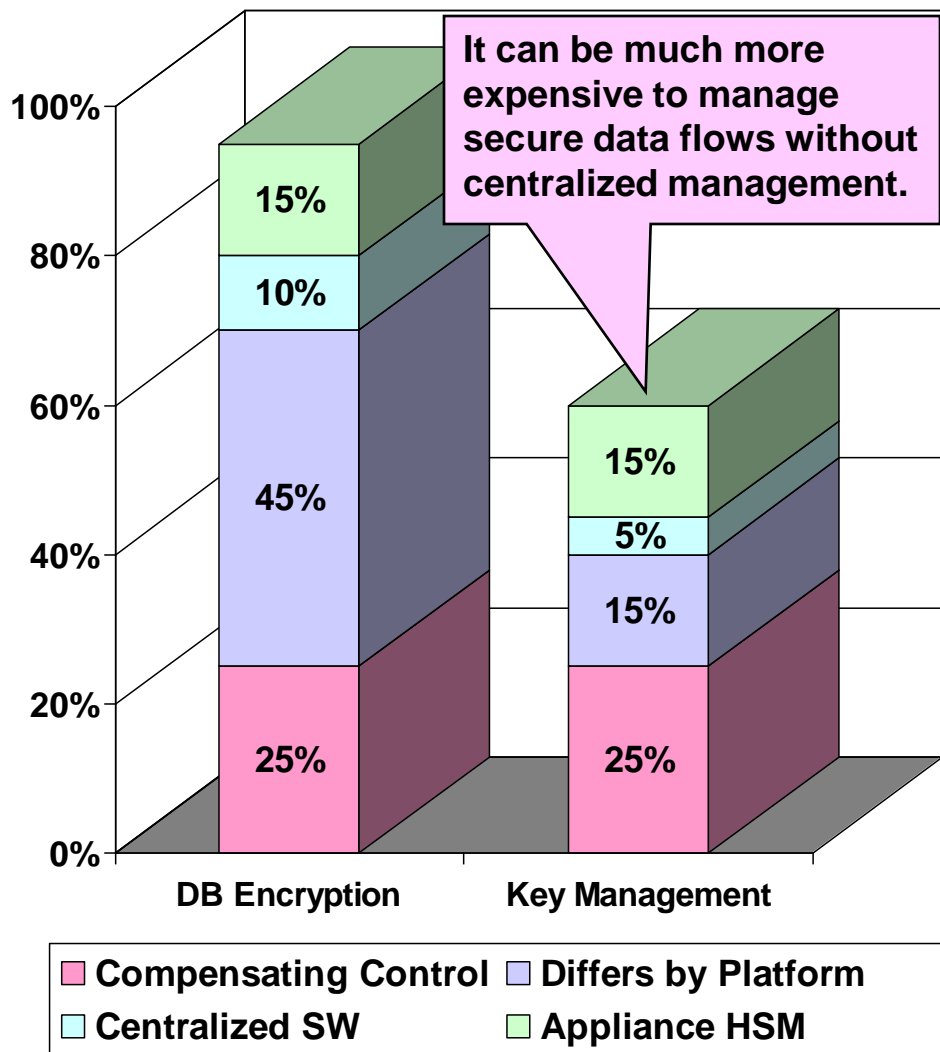
Leaders Have Automated Server Hardening & Configuration Management



- **LEADER'S VIEW:** Server hardening for us is fully automated. We put in 100s of servers per week. We have to have a standard build & request process (Source: Level 1 Service Provider).
- We developed a "gold load" standard configuration for each department (Source: Level 1 Retailer).
- We really don't have any tools for automating or simplifying the setup of servers. Also, when we did the PCI review, our assessors found that our procedures were poorly documented. We are still looking for tools to simplify server configuration and hardening (Source: Level 1 Acquiring Bank).

Source: PCI Knowledge Base, May 2008

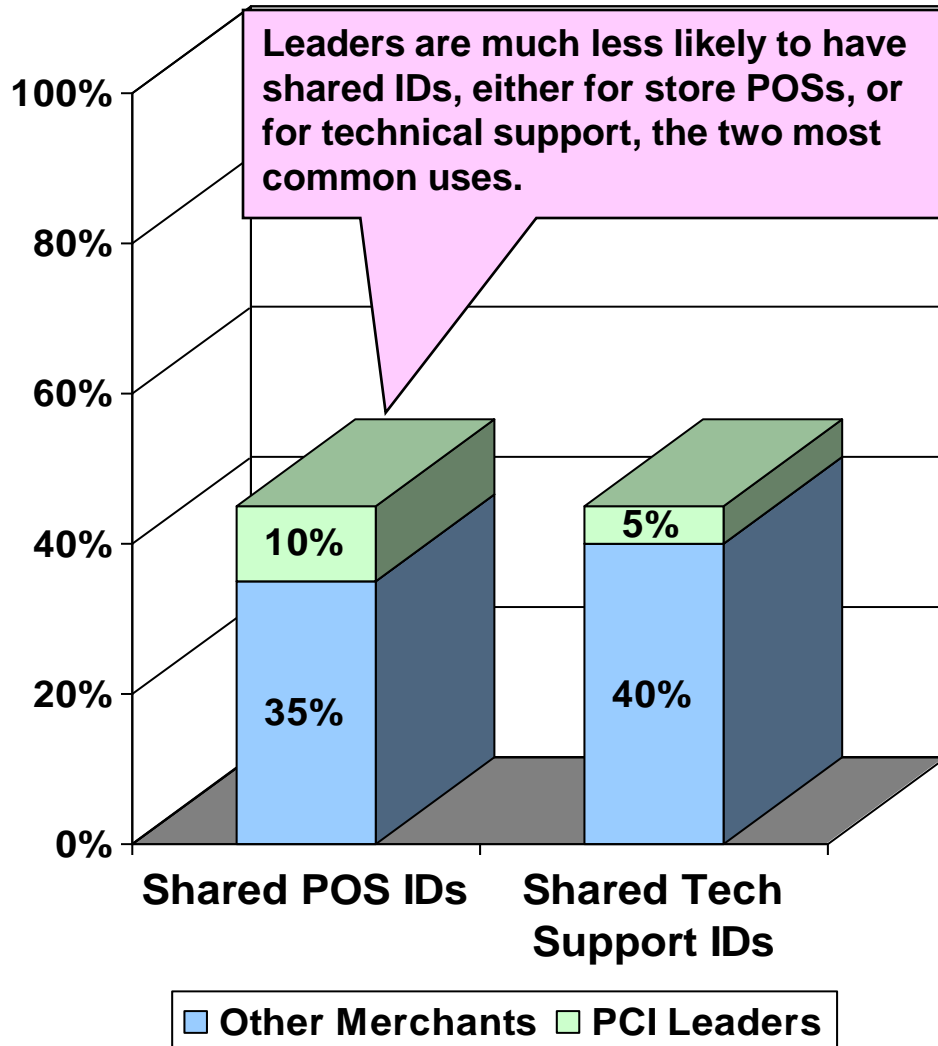
Leaders are Centralizing Encryption and Key Management



- Encryption is a pain to manage, because we do it differently using native functionality on each platform. We wound up defining compensating controls based on net segmentation and access controls, but this is really just a stop gap measure. We need to deploy encryption across the platforms (Source: Level 1 Financial institution).
- We were ready to spend nearly \$100K or so to encrypt our Oracle DBs. But, we found a product, NetLib's Encryptionizer, which works on SQL Server. So, we switched from Oracle DB to SQL Server, and wound up saving a lot of money on encryption, management (Source: Level 1 merchant).

Source: PCI Knowledge Base, May 2008

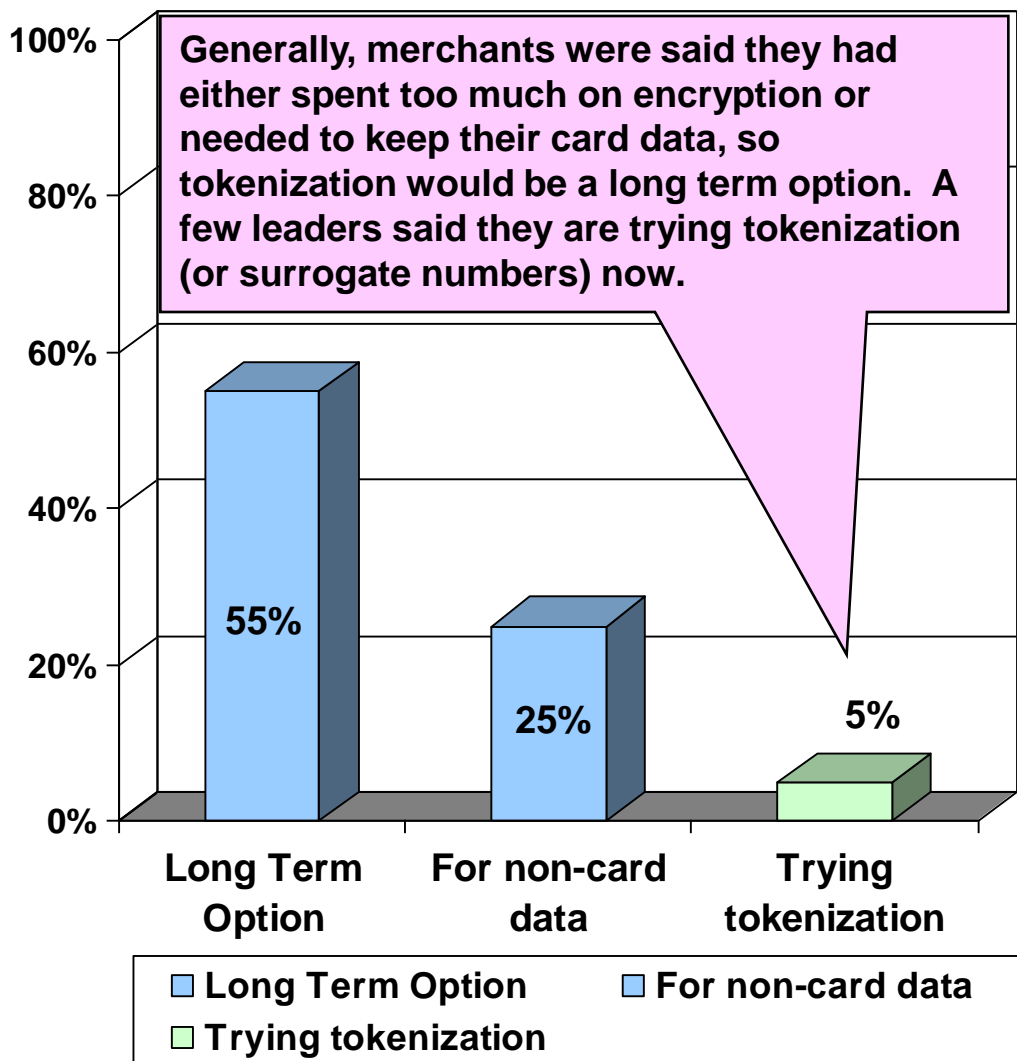
PCI Leaders Less Likely to Have Shared IDs



- **LEADER'S VIEW:** We have zero shared IDs. I do a continuous audit, but our provisioning process is still largely manual. I'm looking at IAM tools now (Source: Level 2 merchant).
- We have shared IDs, where several people know a password that doesn't change. We have internal people who share an application server login; these are IT folks who probably don't need all the access they have (Source: Level 1 merchant).
- We had shared passwords on the POS systems. With high turnover in the stores, we were using shared IDs and passwords to access the POS (Source: Level 1 merchant).

Source: PCI Knowledge Base, May 2008

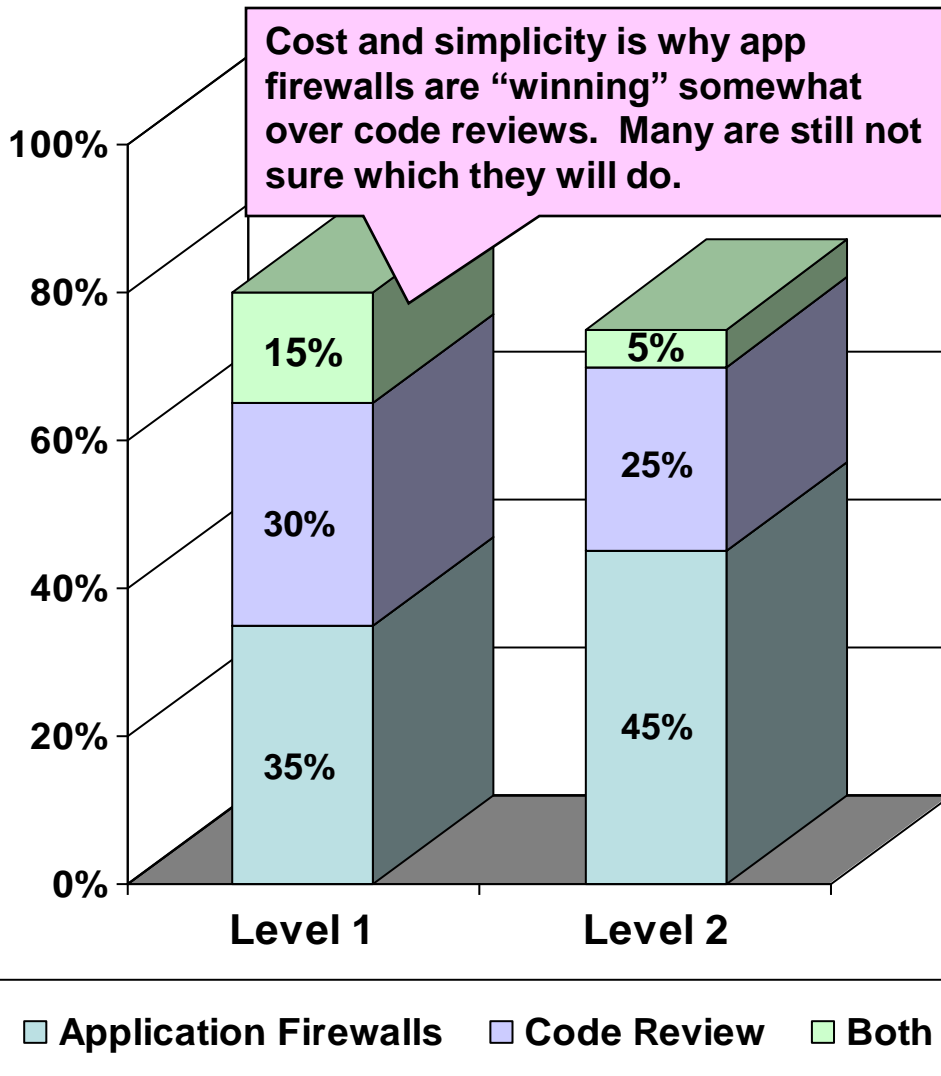
A Few Leaders are Implementing Tokenization Technology Now



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

Source: PCI Knowledge Base, May 2008

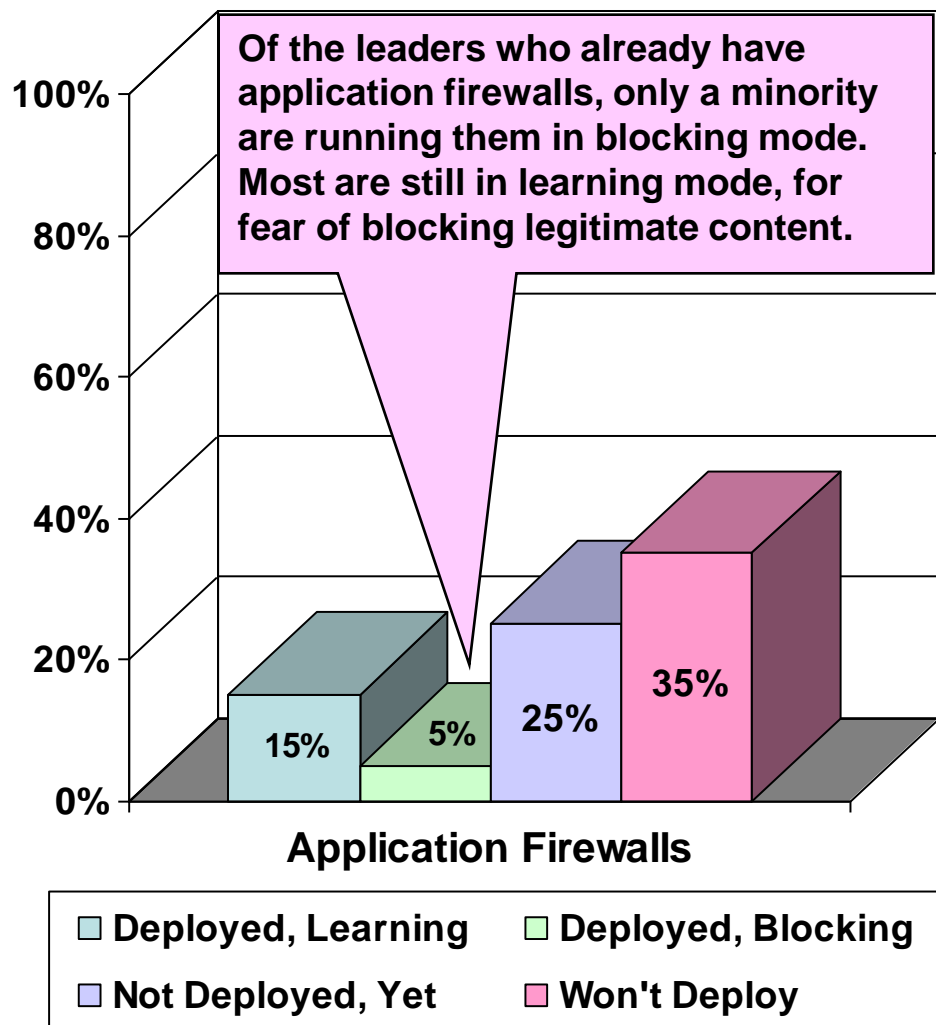
Leaders are Doing Both Application Firewalls and Code Reviews for 6.6



- 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.)

Source: PCI Knowledge Base, May 2008

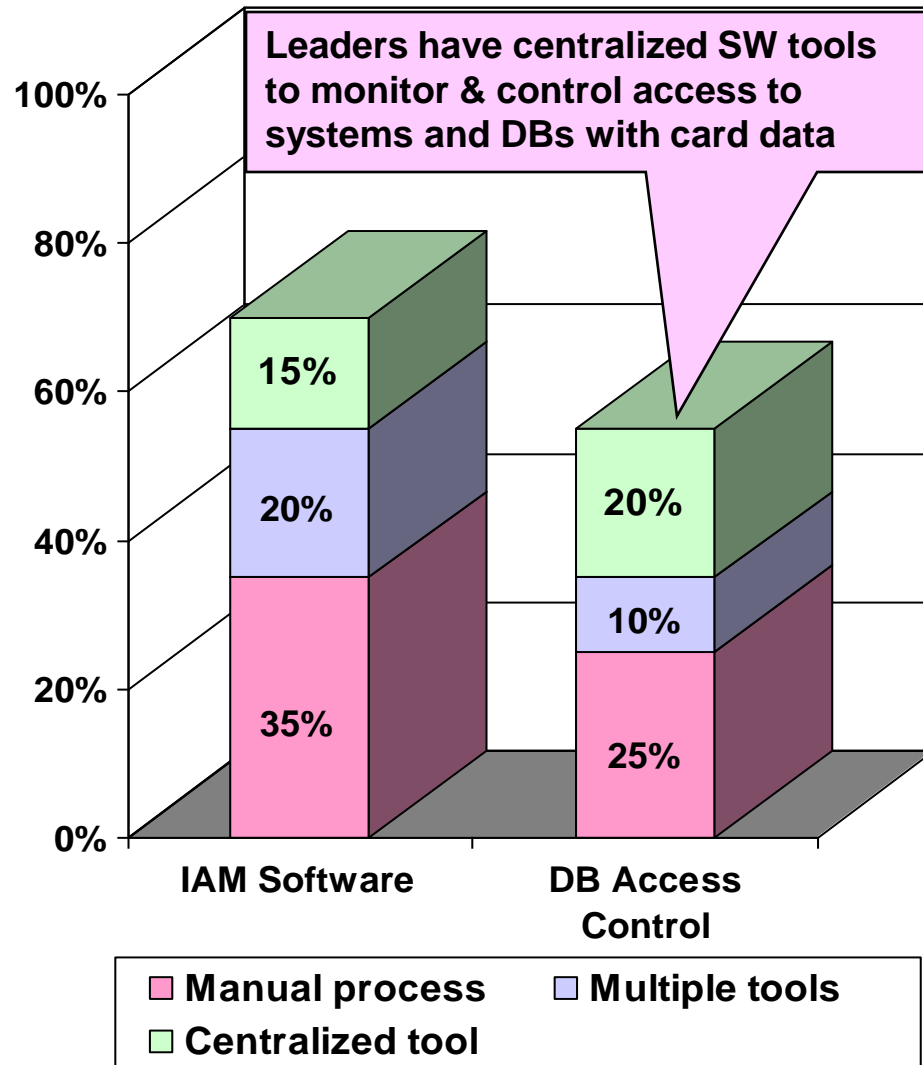
Leaders are More Often Running Their App Firewalls in Blocking Mode



- We talked to several other companies who were using application firewalls, and none of them was running their application firewalls in blocking mode - so why even have them (Source: Level 3 Web Merchant).
- We already have application firewalls, but we will also use service providers to review our homegrown code. Since a lot of our code has been around for 20 years, it makes sense to have it reviewed, even if we could pass 6.6 without it (Source: Level 1 Travel Co.).
- We need to get the application firewall in place first, while we do the code reviews, which will take months or maybe a year (Source: Level 1 Retail).

Source: PCI Knowledge Base, May 2008

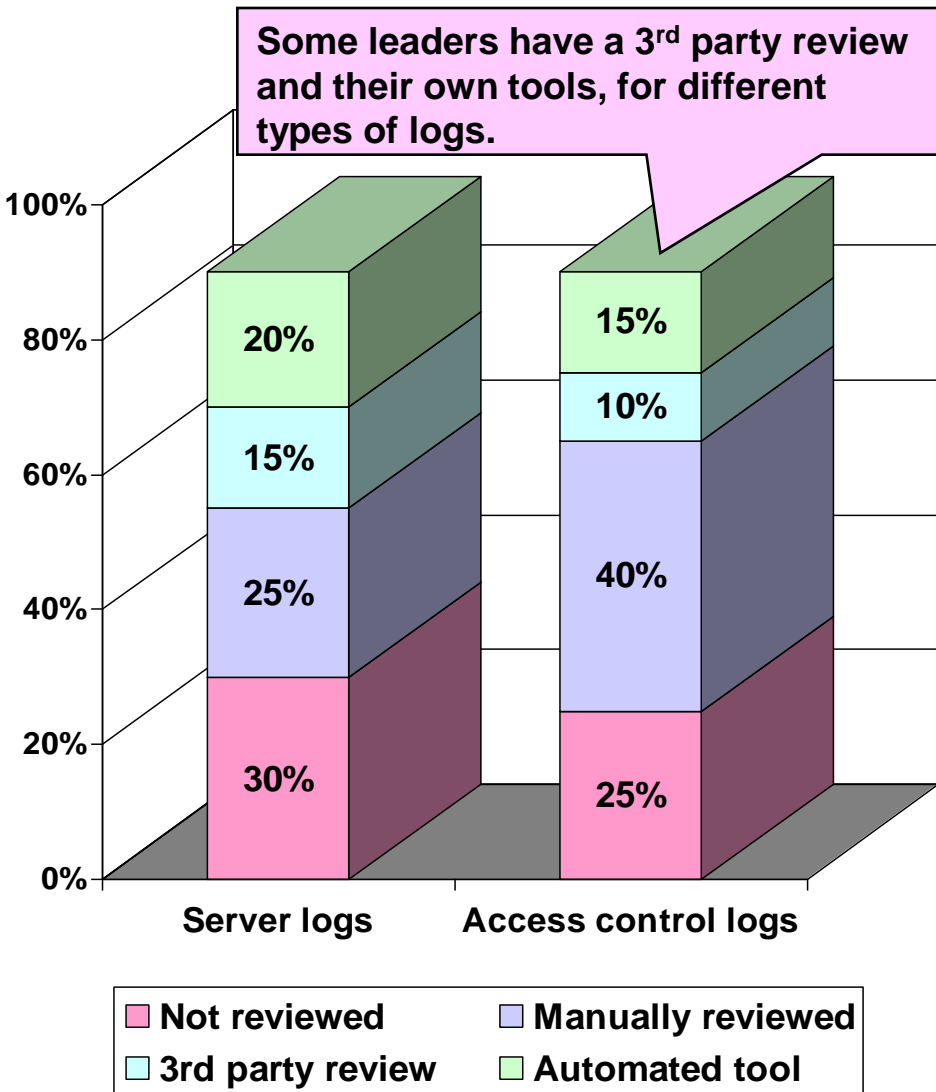
Leaders Have IAM & DB Access Tools to Track Individual Access to Data



- 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

Leaders Have Tools and Service Providers Review Security Log Data

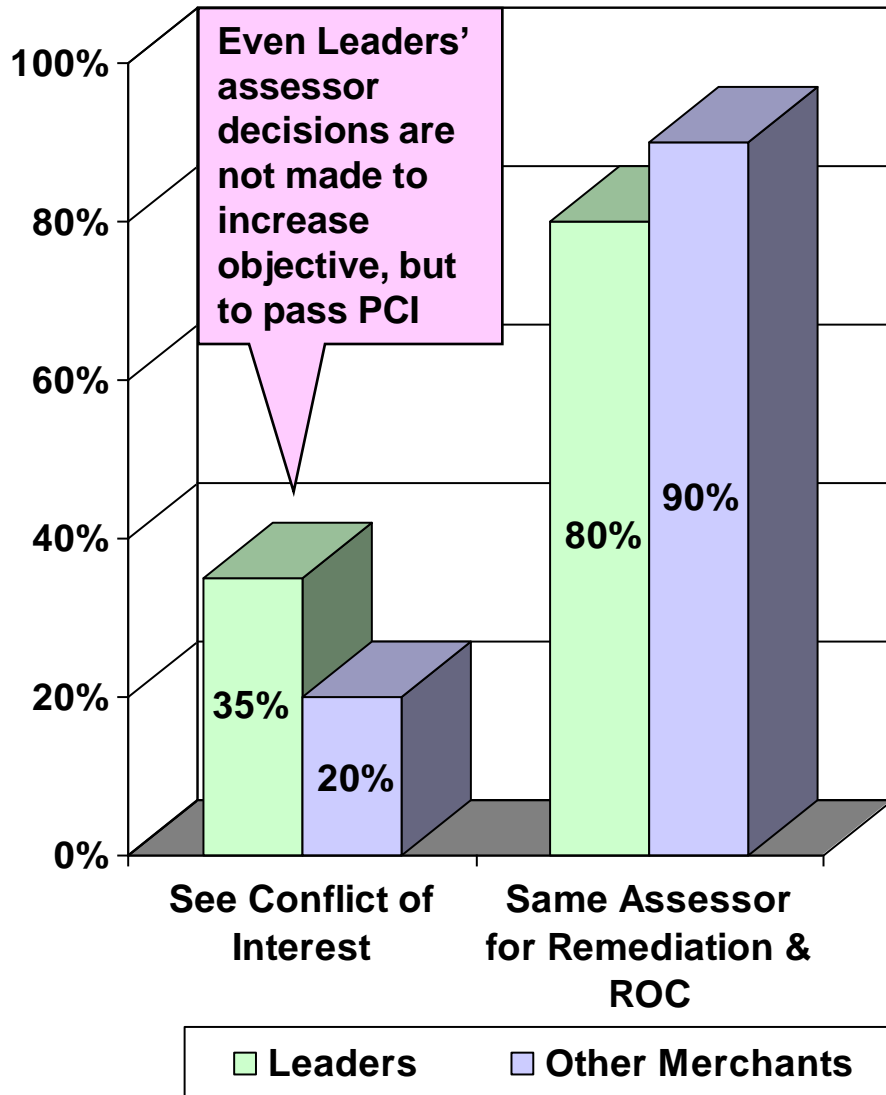


- **LEADER'S VIEW:** The native logging tools such as Cisco MARS are not comprehensive. We need a overall data logging and monitoring tool that is manageable (Source: Level 2 merchant)
- **LEADER'S VIEW:** Most merchants cite SYSLOG as their approach to server log management. While I know some assessors 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

PCI Audit Process

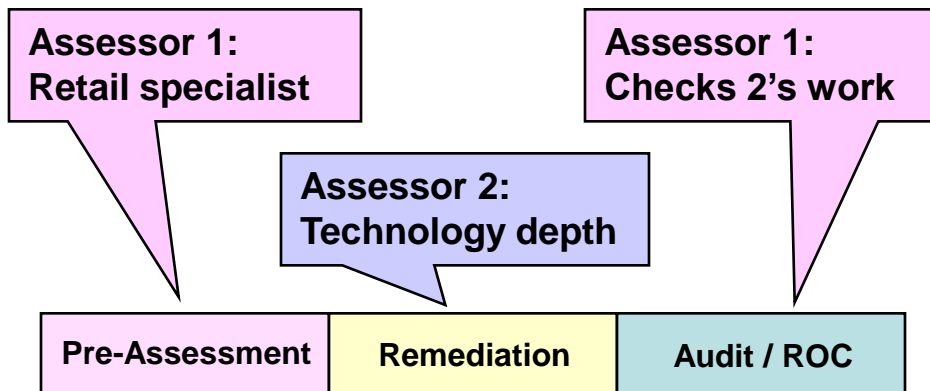
Leaders are Not Much More Concerned About Assessor Independence



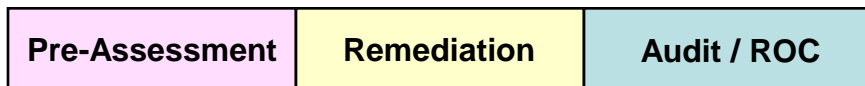
- We use our PCI auditors as security consultants. We we run our ideas for controls by them. I'm not worried about any conflict of interest issue (Source: Level 1 Merchant).
- Our assessor, Solutionary, does not resell security products. We first engaged them to do pen testing. They also did remediation work for us, and then they signed off on our ROC. Even though that could be a conflict, and they were reluctant, we asked their Activeguard group to work with their Assessor group to make sure that the money we were spending on remediation was going to result in a finding of compliance (Source: Level 1 Service Provider).

Source: PCI Knowledge Base, May 2008

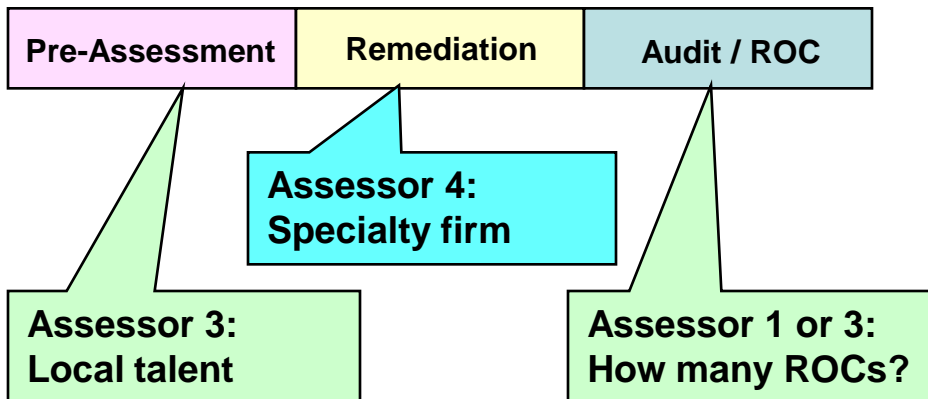
Leaders Tend to Use Different Assessors for Remediation and Audit



Consumer Products Division



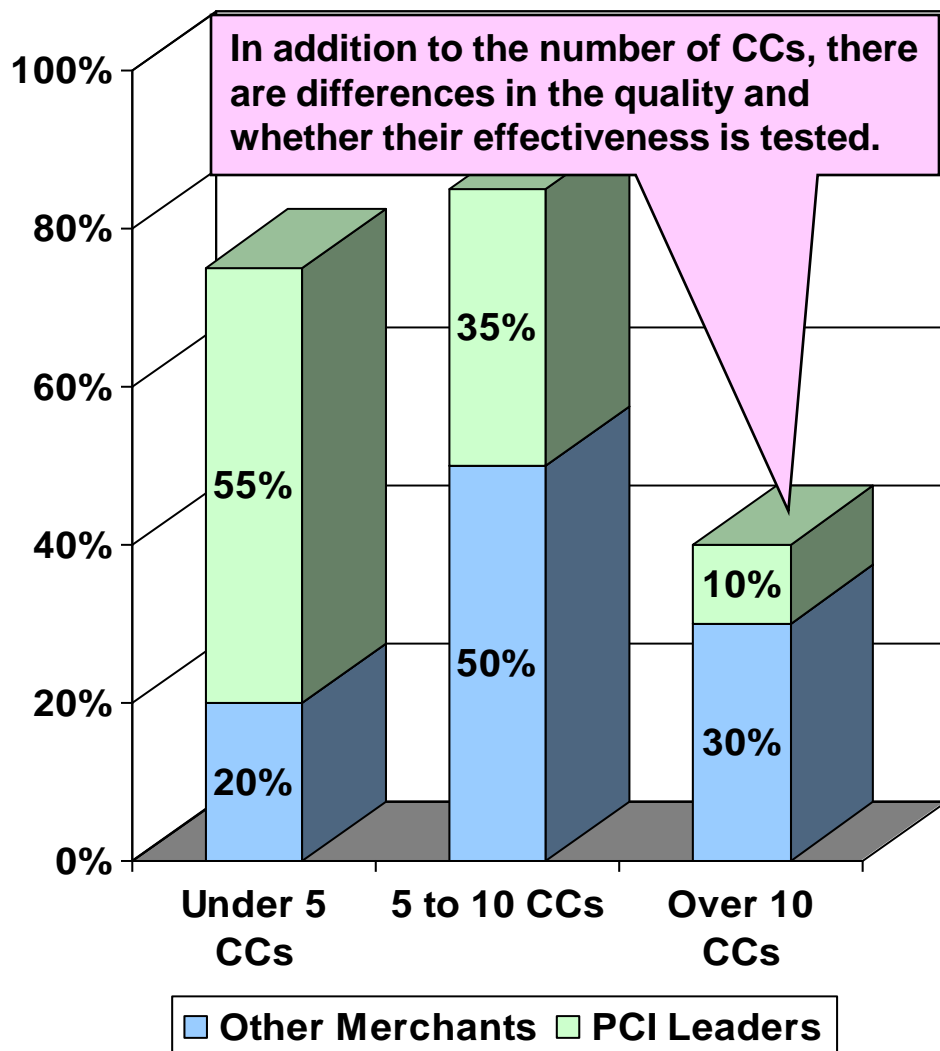
E-Commerce Channel



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

Source: PCI Knowledge Base, May 2008

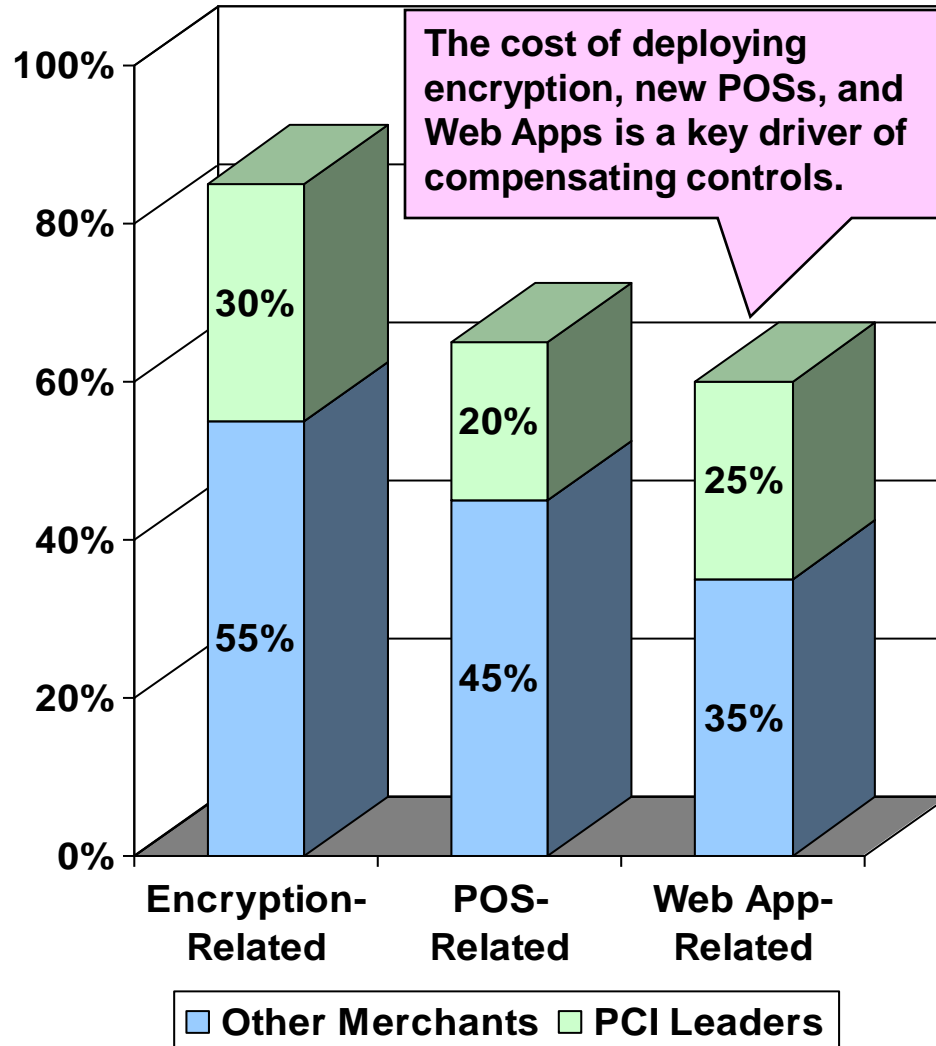
Leaders Use About 5 Compensating Controls, Others Use About 10



- 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

Leaders Use Fewer Compensating Controls, Mainly for #2, #3 and #6



- We had to use several compensating controls for encryption. We have user access controls and change mgmt as compensating controls, and we also have role-based access to the data (Source: Level 1 Merchant).
- Like most retailers, we cannot justify a wholesale replacement of the POSs. We have to roll out new ones over 1-2 years. We got waivers and used compensating controls for this (Source: Level 1 Merchant).
- For PCI 6.6, we're already seeing lots of compensating controls. I've seen compensating controls that allow merchants to use a network scanner as a substitute for an app firewall (Source: PCI Consultant).

Source: PCI Knowledge Base, May 2008

Summary -- How PCI Leaders are Different

1. **PCI Leaders leverage controls data to predict breaches** – Our study of PCI Leadership found that most companies rushed to get PCI compliant quickly, implementing controls as needed. Leaders focused more on Security Information and Event Management (SIEM) – using controls data to predict or stop problems before they became serious.
2. **PCI Leaders have tools or services to monitor their environment** -- Leaders know that security and compliance must be monitored continuously, and they have implemented automated Log Monitoring and alerting tools (or have engaged services) to sort through the vast reams of log data.
3. **PCI Leaders share ownership of PCI** – The most successful leaders do not try to run PCI all by themselves. They have “deputized” internal audit, HR, data owners and store managers and given them specific things to do, from employ education to access monitoring, to policy enforcement.
4. **PCI Leaders focus investment on tracking individual actions** – The leading firms have implemented Identity and Access Management and Data Loss Prevention tools to automate the provisioning of access and monitor privileged user access to confidential data, as well as role-based access, so that when roles change, so do permissions.
5. **PCI Leaders use risk management tools** – Because PCI requires a 100% score to pass, only leading firms have gone beyond this to manage their security based on a thorough risk analysis. Beyond a basic “stoplight” rating spreadsheet, a risk analysis requires that companies take specific actions to address identified risks, based on priority.
6. **PCI Leaders protect other data besides card numbers** – One of the clearest definitions of going “beyond PCI” is the organization that applies the PCI security controls to social security numbers, account numbers, and other confidential data. The key is defining and enforcing a “data classification” scheme.
7. **PCI Leaders monitor their service providers and partners** – PCI only requires a letter of agreement that a service provider will adhere to PCI. Leading firms are doing real due diligence of their service providers and partners. Some are sending out questionnaires, others are sending auditors to review the security of their service providers.
8. **PCI Leaders use fewer compensating controls** – Very few enterprises require no compensating controls to achieve PCI compliance. But leaders typically have 5 or fewer CCs, while the typical enterprise requires 10 or so CCs.

Source: PCI Knowledge Base, May 2008

Recommendations

- 1. Stop collecting card data and other confidential data you don't use.**
- 2. Reduce PCI scope via network segmentation and data purging.**
- 3. Turn on monitoring functions and fix any performance impacts.**
- 4. “Deputize” Internal Audit, HR, Legal and business managers to ensure that PCI isn't viewed as an “IT project”**
- 5. Ensure individual data access is tracked via ID management system.**
- 6. Implement a monthly risk and vulnerability review process.**
- 7. Extend PCI controls to SSNs and other confidential data.**
- 8. Implement PCI audits of service providers and partners.**
- 9. Plan to replace all compensating controls over the next 1-2 years,**
- 10. Use two different assessors – one for remediation and one for audit.**
- 11. Implement policies and procedures for server virtualization, if needed.**

What is the PCI Knowledge Base? – A Research Community

www.KnowPCI.com

We have over 100 hours of totally anonymous feedback from merchants, PCI assessors, banks & technologists.

Knowledge Base is free, but you must register first.

“PCI in 15 minutes” Weekly Webinars

PCI Discussion Forums. Ask questions of our Panel of Experts

The screenshot shows the PCI Knowledge Base website. At the top, there is a navigation bar with links: Home, Panel of Experts, About Us, Contact Us, Expert Interview, Get Involved, Resources, and Knowledgebase. Below the navigation bar, there are several content sections:

- Search Knowledge:** A search box with a dropdown menu for "All Categories" and a "Search" button. Below it is a link for "Advanced Search".
- Knowledge Base:** A directory of categories including Comment Type, Industry, Level, Module, and Role.
- Login:** A login form with fields for "Username" and "Password", a "Remember me" checkbox, and a "Login" button. Below the form are links for "Forgot Password?" and "Register".
- PCI News:** A section with the heading "Click Term Below" and a list of news items: "PCI Security Breach Data Security PCI Compliance", "Cancer relay for PCI St. Thomas Times-Journal, Canada Rae Gibson, vice-president of the student council, said the school wanted to stage its own event to encourage more participation from PCI students.", and "Security expert slams PCI VNUNet.com Chess added that the interesting thing about the case is that Hannaford Bros is believed to be fully PCI compliant and, as such, is unlikely to have to pay ...". There are also links for "Related Articles >" and "Getting Heart Attack DG News About 62% of the standard-of-care patients".
- Best of - Top Rated Items:** A list of three items: "1 Verizon to review our compensating controls", "2 We use the BITS standard when auditing our...", and "3 we have a daily security dashboard report to...". There is a "Show more..." link.
- Our Partners:** A section featuring the "Configuresoft" logo.
- What's in the PCI Knowledge Base?:** A list of bullet points: "Peer feedback on PCI -- Best practices, Lessons learned, Spending levels;", "Vendor feedback -- What customers like and why", "Assessor feedback -- Who's best, who's tough, who's easy", "Advice from our Panel of Experts -- Assessors, Bankers, CTOs and CISOs", "Hot Topics:" (with sub-points: "Compensating Controls", "Server Virtualization", "Tokenization"), and "It's FREE to join PCI Knowledge Base, just click on 'GET INVOLVED'".
- Preview of Knowledge Base Findings:** A table with columns for "Rating of Compliance", "Panel of Experts", and "Merchants".

How to Get the Most Value From the PCI Knowledge Base

1 Knowledge Base Directory

- Comment Type
- Industry
- Level
- Module
- Role

2 Comment Type Categories

- Advice (70)
- Experience (205)
- Needs / Plans (139)
- Vendor Feedback (201)
- Best Practice (197)
- General Knowledge (0)
- Process (20)
- Budget / Spending (54)
- Lesson Learned (262)
- Trend / Changes (60)

3 Best Practice Listings

There are 197 Listings in this Category.

wireless scan unreliable ★★★★★

We have tried doing wireless scans internally. But we picked up 65 networks and it took way ng to verify them all. We need a tool to automate the Wireless network scans and do

monitoring ★★★★★

part of the evolution of our security program. We do

re managing HIPAA and PCI together ★★★★★

a level 2, trying to become compliant. We have submitted the SAQ. We're working with

4 **wireless scan unreliable**

Region North America

Compliant Yes - 2+ Years

View of PCI Strategic View

Spend Level Over 1m

Expert Merchant

Submit review Recommend Report Problem Expert's Knowledge

Rating ★★★★★ 0 vote **5** ured: 0

1 Search Knowledge

search...

All Categories

Search

Advanced Search

Search for any word, e.g., "monitoring"

Find peers by industry, by PCI level, by compliance, spending level. The ratings you give the knols determines results order; you can email knols, review them, "favorite" them, etc.

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