

# paymetrić

*Presents:*



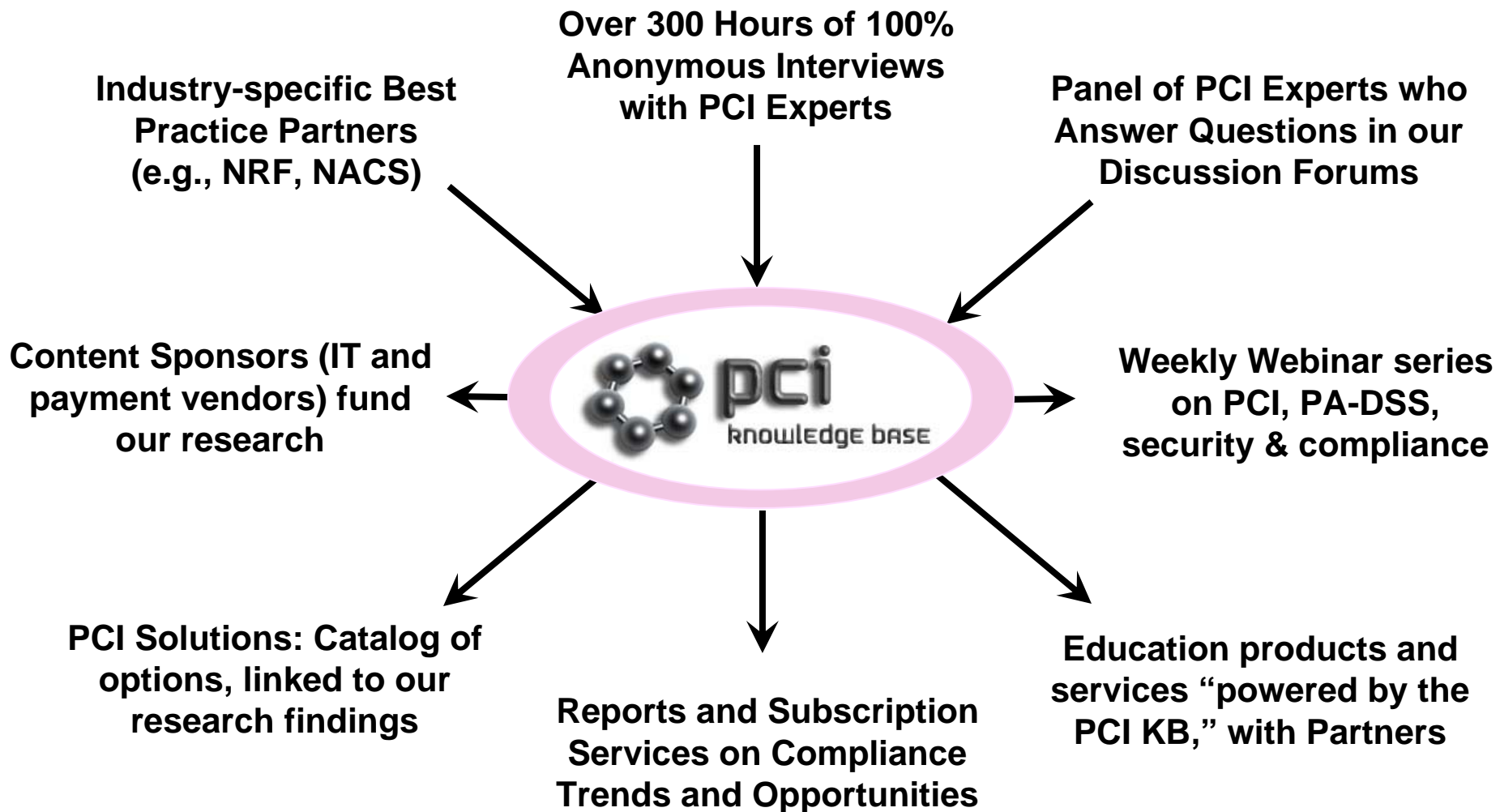
***“Cost-Effective Compliance”***

*Featuring:*

**The Latest Findings from the PCI Knowledge Base**

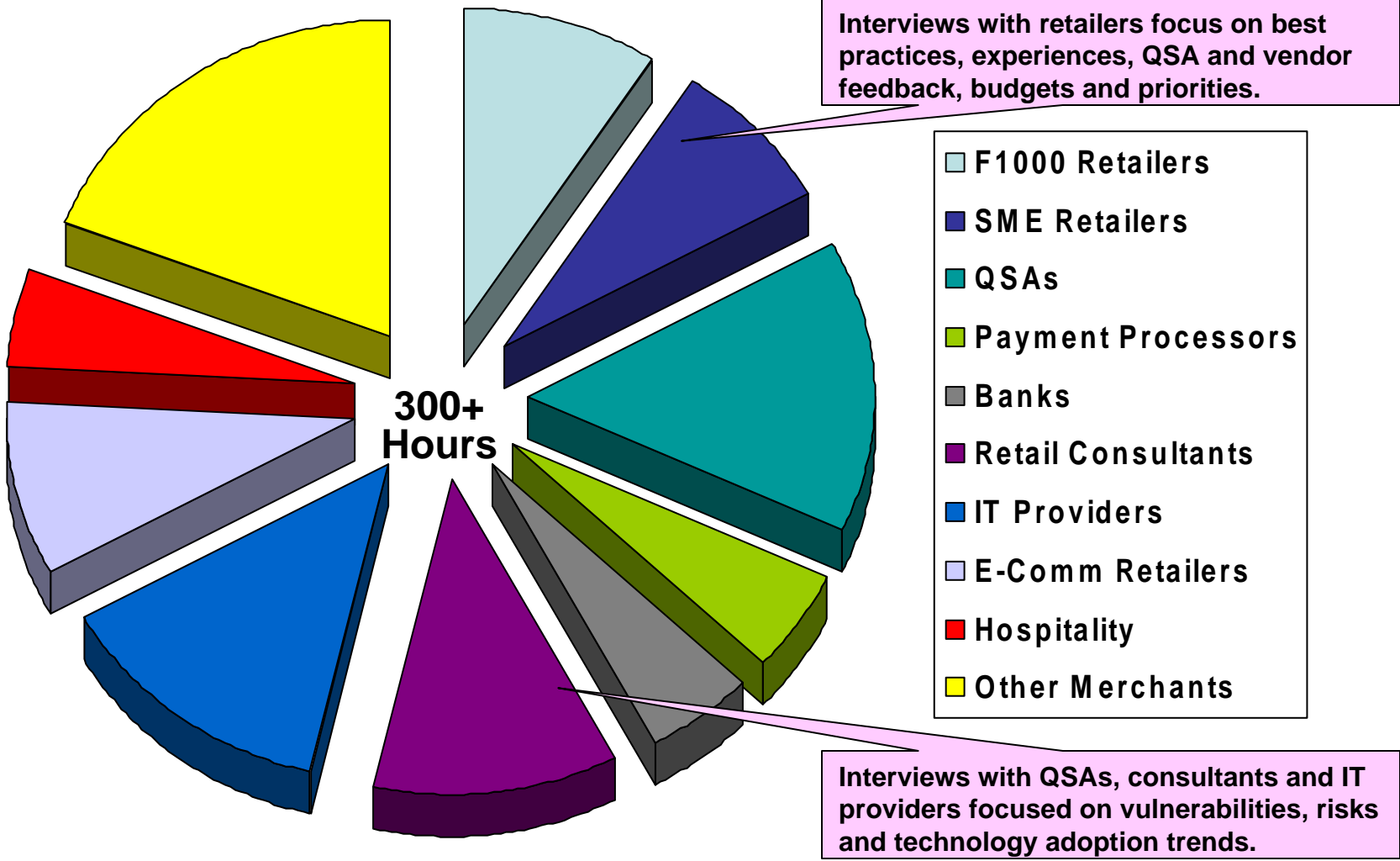
**Presented by: Dr. David Taylor, CISSP  
David.Taylor@KnowPCI.com**

# What is The PCI Knowledge Base?



Source: PCI Knowledge Base, January 2009

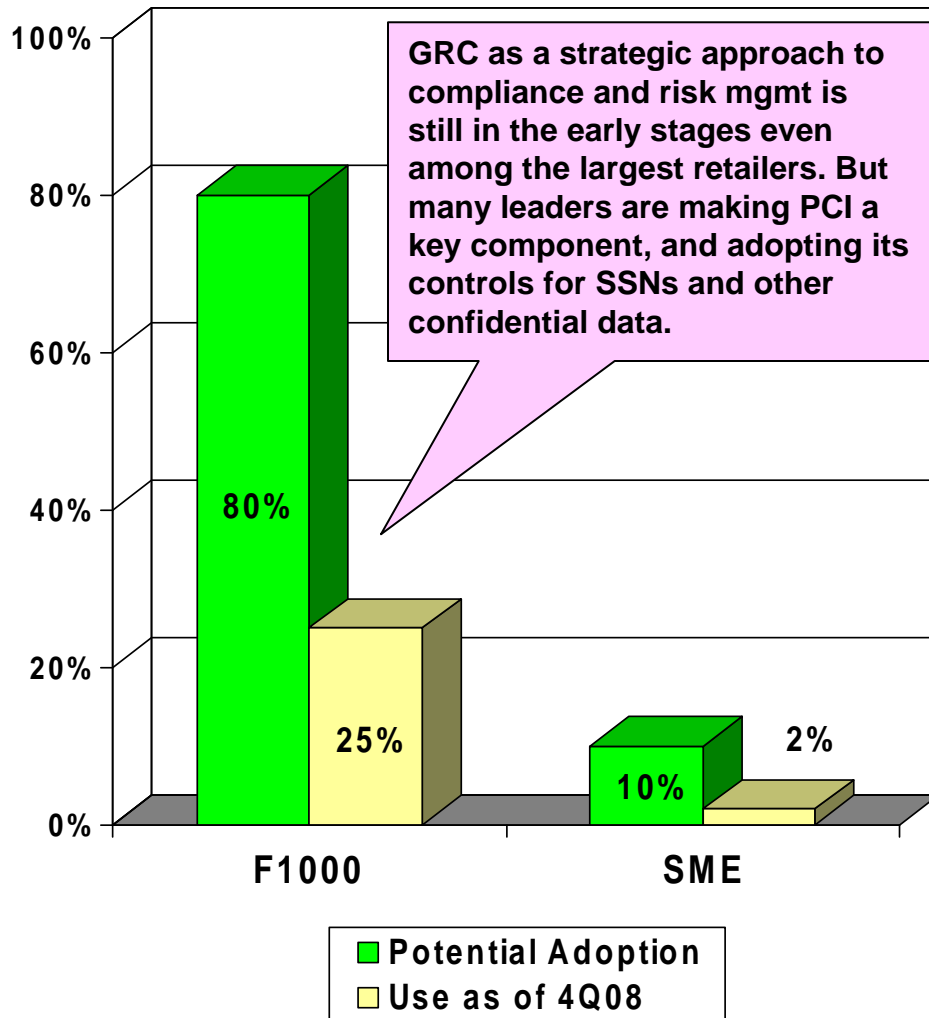
# Based on Over 300 Hours of 100% Anonymous Interviews – Not a Survey



Source: PCI Knowledge Base, January 2009

# PCI Should Drive or Integrate With Overall GRC Strategy

Current vs Potential Use of Integrated GRC

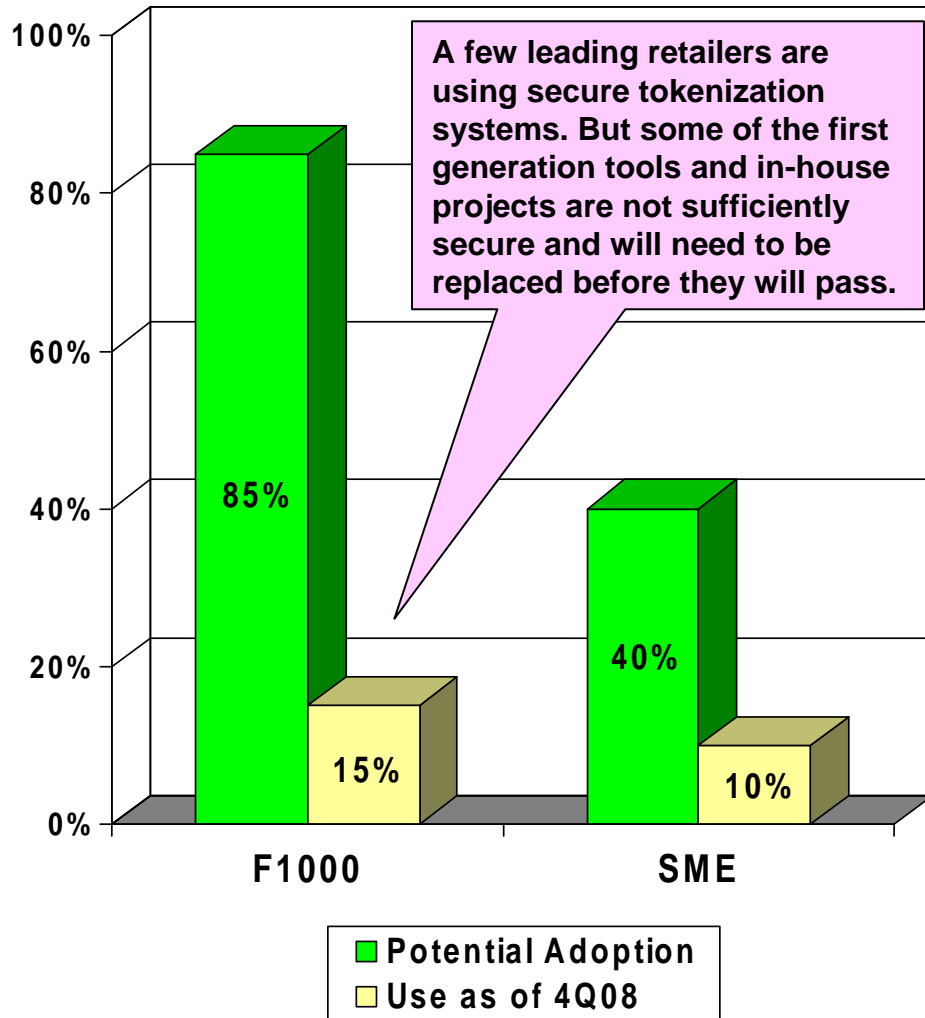


<b>Best Practice Description</b>	PCI should be a part of, or even a driver of a corporate Governance, Risk Management and Compliance (GRC) program. It should not be dismissed as too technical or managed only by IT security. Integrate it with SOX, etc.
<b>Level of Investment</b>	\$10,000 – 30,000 in SW licensing costs for integration of compliance mgmt tools.
<b>Potential Savings</b>	\$30,000 – 50,000 wasted on control-specific tools that cannot be integrated with overall security management SW.
<b>Best for</b>	F1000 retailers who have purchased (or plan to purchase) discrete security tools.
<b>Primary Dept Owner</b>	IT Infrastructure and IT Networking.
<b>PCI Reqmts Met</b>	All

Source: PCI Knowledge Base, January 2009

# Adopt “Secure Tokenization” to Remove Card Data But Retain Analytics

Current vs Potential Use of Secure Tokenization

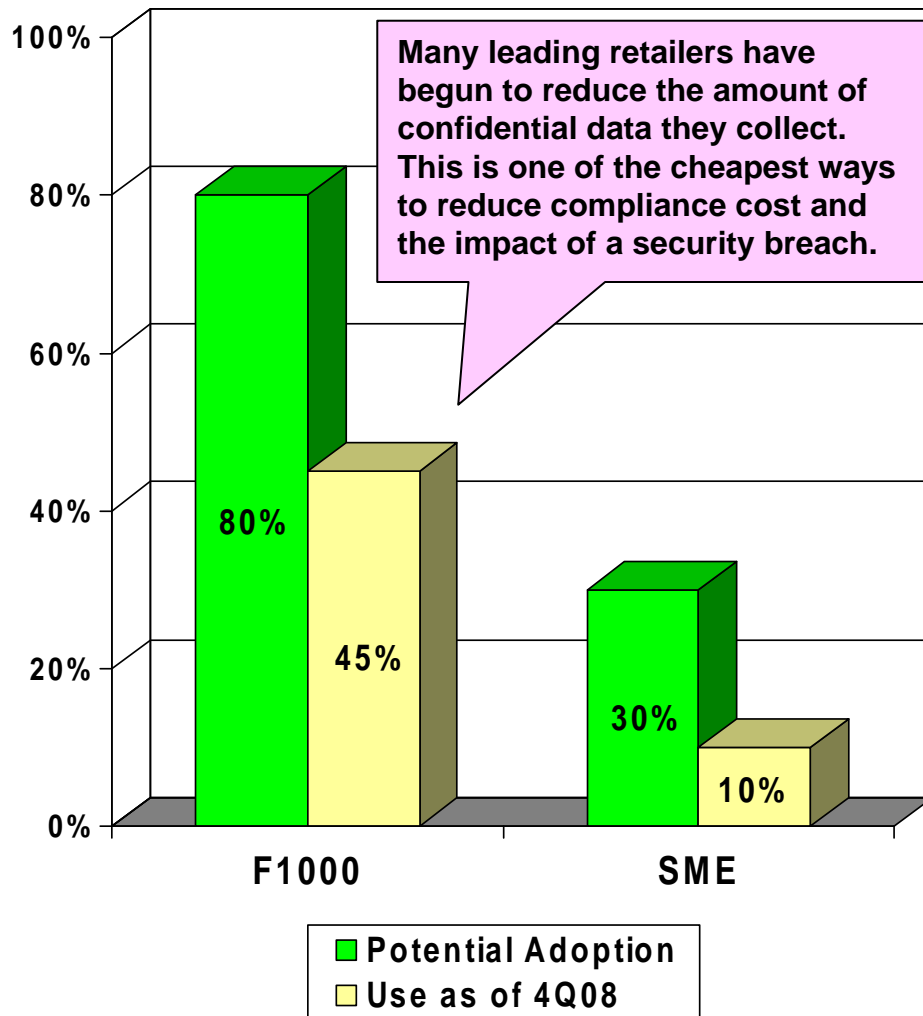


<b>Best Practice Description</b>	Use “secure” tokenization tools or services to create a centralized, encrypted repository of card data and use surrogate and/or partially masked data to validate transaction records for sales audit and marketing analysis. How tokens are created and managed is key to this best practice.
<b>Level of Investment</b>	\$5,000 – 40,000 in SW licensing and increased transaction costs.
<b>Potential Savings</b>	\$10,000 – 100,000 in reduced assessment costs and security control cost avoidance costs.
<b>Best for</b>	F1000 retailers who cannot segment networks and have card data throughout the enterprise.
<b>Primary Dept Owner</b>	IT Infrastructure, with support from CFO on switching processors.
<b>PCI Reqmts Met</b>	3, 4

Source: PCI Knowledge Base, January 2009

# Stop Collecting and Storing Confidential Data That is Not Used

Current vs Potential Use of Data Collection Cutbacks

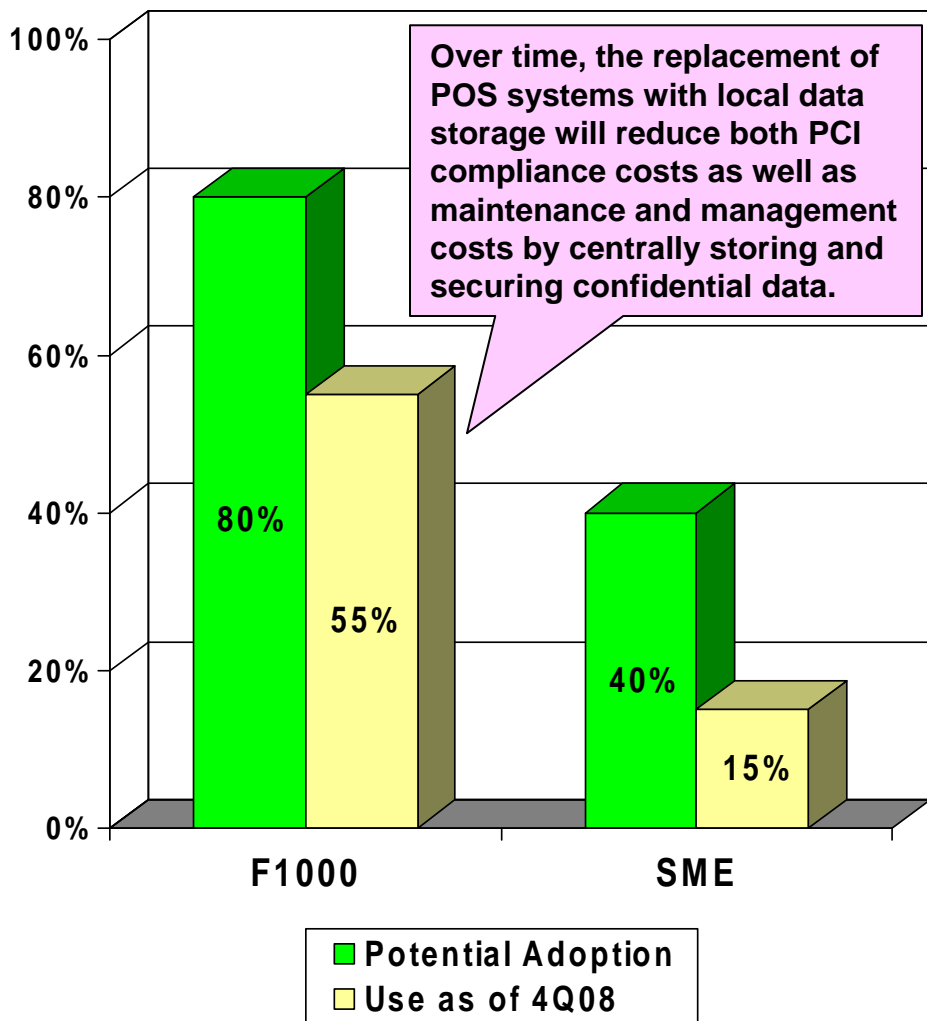


<b>Best Practice Description</b>	Stop collecting CCN & other confidential data you don't use. Marketing and other departments that collect confidential customer data must justify what is done with this data and determine what alternatives exist to collecting full CCN or SSN or other confidential data.
<b>Level of Investment</b>	Near \$zero for the project itself, but \$10K – 30K to make changes to procedures and applications.
<b>Potential Savings</b>	\$10K – 30K from reducing PCI scope, and much more value from reducing data security risks.
<b>Best for</b>	F1000s who have developed loyalty programs, or online stores with forms that collect this data.
<b>Primary Dept Owner</b>	Business owners, Marketing
<b>PCI Reqmts Met</b>	3.1, 6.3

Source: PCI Knowledge Base, January 2009

# Reduce Store Data Volume Size and Retention Periods for Card Data

Current vs Potential Use of Data Reduction Process



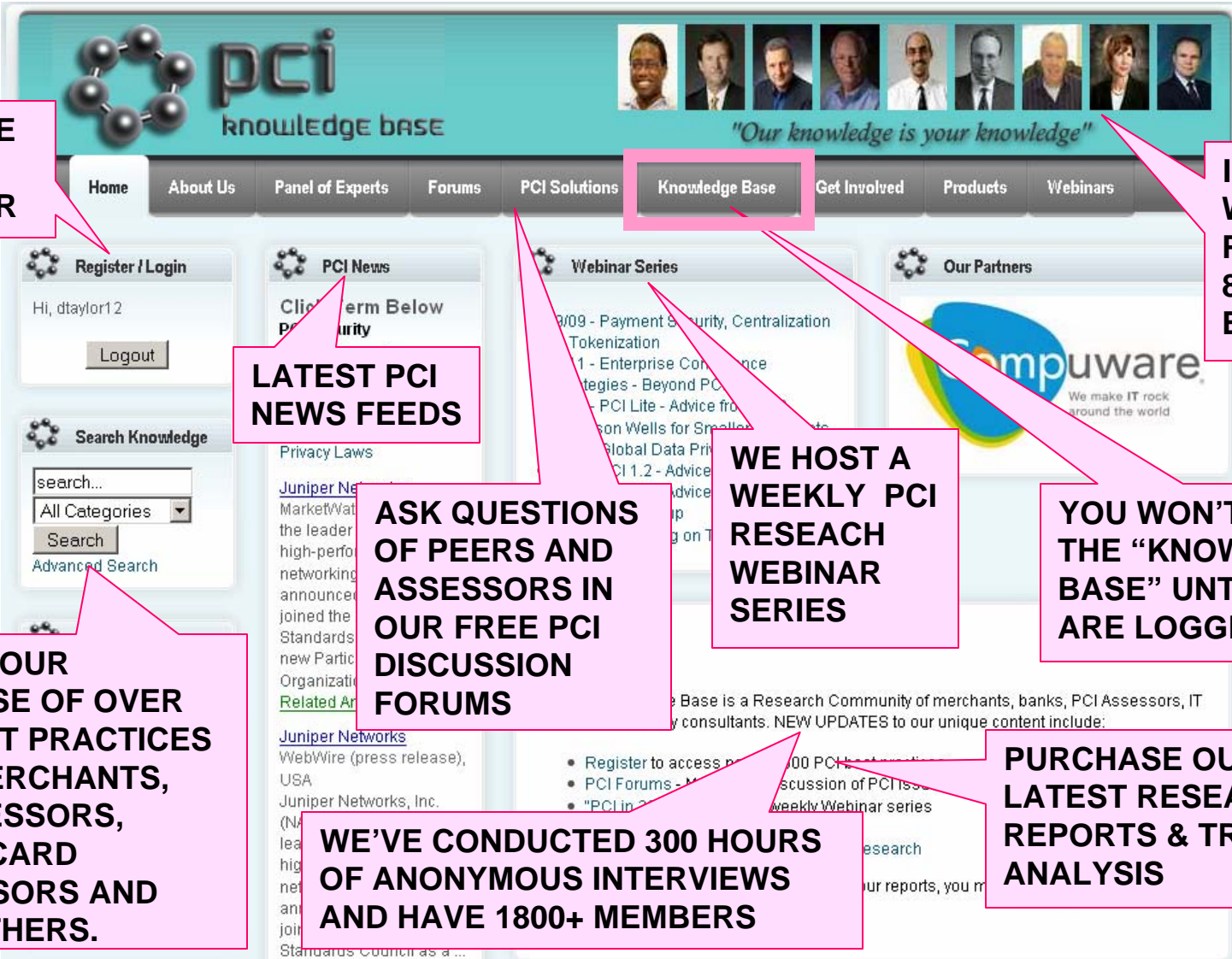
<b>Best Practice Description</b>	Reduce confidential data volumes on POS, and other in store systems to the minimum possible retention period, given business requirements. The goal is to retain no confidential data at remote locations, or the technical minimum volume of data required by the application. But the POS is still in scope for PCI, even if data's encrypted.
<b>Level of Investment</b>	Near \$Zero, except for the project costs of designing a tool and procedure to remove the data.
<b>Potential Savings</b>	\$5000 – 15,000 in store level assessments costs avoided.
<b>Best for</b>	Smaller retailers and those currently replacing their POS
<b>Primary Dept Owner</b>	Store Operations and/or Field IT
<b>PCI Reqmts Met</b>	3.1

Source: PCI Knowledge Base, January 2009

## Conclusions and Recommendations

1. Many merchants are not very secure, despite being PCI compliant.
2. Focus on a short list of control improvements that have the best ROI
3. PCI v1.2 shifts more focus on stores, requiring more store audits
4. Increased focus on service providers, requiring retailer due diligence
5. Major weaknesses in log management and log review are very common
6. PCI forced new security data collection, overloading security managers
7. Manual controls management should be replaced by automated tools
8. F1000 retailers have made major progress in 3 key areas:
  - a. Improved documentation of data flows of confidential data
  - b. Network segmentation, at corporate and also in the stores
  - c. Limiting / securing the use of production data in dev / test
9. Additional security effort is needed (and justifiable) in 4 key areas:
  - a. Wireless security – replacing WEP and implementing wireless IPS
  - b. Tokenization – deploying solutions to remove card data from scope
  - c. Virtual POS – to reduce / eliminate in-store collection of card data
  - d. PA-DSS – ensuring that payment application vendors are compliant
10. F1000 retailers should also be willing to train to be their own QSA

# The Major Features of the PCI Knowledge Base (www.KnowPCI.com)



**IT IS FREE TO REGISTER**

**INTERACT WITH OUR PANEL OF 85+ PCI EXPERTS**

**LATEST PCI NEWS FEEDS**

**WE HOST A WEEKLY PCI RESEARCH WEBINAR SERIES**

**YOU WON'T SEE THE "KNOWLEDGE BASE" UNTIL YOU ARE LOGGED IN**

**SEARCH OUR DATABASE OF OVER 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 300 HOURS OF ANONYMOUS INTERVIEWS AND HAVE 1800+ MEMBERS**

**PURCHASE OUR LATEST RESEARCH REPORTS & TREND ANALYSIS**

## Next Steps in Our PCI Best Practices Research for the NRF

1. **Develop a web-based repository for the PCI documentation we have collected, accessible to NRF members**
2. **Measure the cost of meeting the PCI PED TDES 7/1/2010 deadline**
3. **Measure the impact of PA-DSS on POS, E-Commerce, Call Centers, etc. Examine trends in adoption of the identified best practices**
4. **Measure PCI's impact on emerging technologies such as wireless POS and mobile payments**
5. **Develop best practices and education programs around PA-DSS and PCI PED standards, which are far less well known than PCI DSS**
6. **Work to develop a Level 4 retailer education / awareness program**
7. **Develop best practices related to PCI PED standards and upgrades**
8. **Respond to NRF member suggestions**
9. **Any suggestions? Comments? Questions?**

## For More Information:

- Research database
- Discussion forums
- Advisory services
- Solutions catalog
- Branded education



Dr. David Taylor, CISSP  
Founder, PCI Knowledge Base  
[David.Taylor@KnowPCI.com](mailto:David.Taylor@KnowPCI.com)  
203-569-7951