

*Customer Data Security:
PCI and Beyond
Benchmark Study 2008*

By:
Brian Kilcourse, Managing Partner
Steve Rowen, Partner



Sponsored by:



Table of Contents

Executive Summary	1
Business Challenge	1
Opportunities	1
Organizational Inhibitors	1
Technology Enablers.....	1
Bootstrap Recommendations.....	2
SECTION I: Overview.....	3
Why The Study Was Conducted	3
Methodology	3
Defining Retail Winners and Why They Win.....	3
Survey Respondent Characteristics	5
SECTION II: Business Challenges.....	7
A Retail Paradox: How to Use Customer Data and Still Protect Privacy?	7
Collection Of Customer Data Varies For Different Retailing Tiers	8
Customer-Specific Demand Data Drives the 21 st Century Retail Value Chain	8
Customer-Specific Data Needs To Be Protected Differently Than Other Operational Data.....	9
What Is Compliance, Anyway?	10
SECTION III: Opportunities.....	12
Solving the Paradox: Using Consumer-specific Information ... <i>And</i> Ensuring Privacy and Security.....	12
The PCI Mandate Drives a More Proactive Approach to Data Security.....	14
The PCI Mandate Can Drive Other Benefits.....	16
SECTION IV: Organizational Inhibitors.....	18
‘PCI Compliance’ Doesn’t Mean ‘Security’.....	18
It Isn’t Easy to Change.....	18

SECTION V: Technology Enablers	20
Assessing Both Technology and Process.....	20
Logging & Monitoring – Every Step of the Way.....	21
Solutions Providers: Trust, but Verify	22
SECTION VI: BootStrap Recommendations	23
Do the Assessment and Map Mandates to The Business.....	23
Lock it Up	23
Let it Go	23
Get a Handle on the Network.....	23
Customer Data Security Much More Than a Compliance Project	23
APPENDIX A: The BOOT Methodology	a
APPENDIX B: About Our Sponsors	b
APPENDIX C: About RSR.....	c

Figures

Figure 1: The Value of Customer Data.....	4
Figure 2: Most Retailers Keep Customer-Specific Data for Years.....	5
Figure 3: Where Retailers Get Customer Data	7
Figure 4: Big Retailers Have Big Appetites for Customer-Specific Data.....	8
Figure 5: Shared Demand Data Drives the Value Chain	9
Figure 5: PCI Compliance: “Working on It”	10
Figure 6: Larger Organizations are Closer to Compliance	11
Figure 7: Today’s Retailers Usually Have Multi-Channel Operations	12
Figure 8: Open Access to Customer-specific Data is Common.....	13
Figure 9: The Spreadsheet Reigns as the Most Common Analysis Tool	14
Figure 10: 70% of Retailers Have A Plan In Place	15
Figure 11: More than Just Avoiding Risks.....	16
Figure 12: Business Policy and Process Changes are Hard to Implement	19
Figure 13: Top-Tiered Winners Certify Business Applications.....	19
Figure 14: Assessing the Scope.....	20
Figure 15: Encrypt It or Get Rid of It.....	21
Figure 16: Where is it Encrypted?	21

EXECUTIVE SUMMARY

2007 proved to be a landmark year for the security of customer-specific information in retail. And while the topic has never been hotter, most of what has generated interest and attention has been **reactive** in nature. Public headlines of massive data breaches (and the ease by which they can be conducted) have raised the public's concern; industry mandates calling for enhanced information security have raised the retail Board of Directors' ire.

2008, by comparison, must be a year in which retailers who take this matter seriously demonstrate decidedly more **proactive** behavior. The Customer Data Security Benchmark Study 2008 is intended to reveal how retailers not only continue to approach the PCI mandate, but beyond that, what proactive steps they are taking now to minimize the risks associated with the capture, retention, and use of customer-specific data.

BUSINESS CHALLENGE

Because the collection of customer-specific data has become prerequisite practice for virtually *every* retailer looking to offer an enhanced shopping experience, the time for discussing how to protect information before it is attacked is well past-due. In fact, as organized crime rings continually conduct "smarter" criminal operations, it is entirely plausible that several major retail hacks have already occurred that will not come to light until many months after-the-fact. Card-present retailers, in particular, have become targets. Payment data resulting from these hacks is openly sold on the black-market, often times not used until as long as 18 months after theft has occurred. The retail industry would be best served to seize its narrowing window of opportunity to self-regulate. At the time of this report, 40 individual US states impose some level of data security law, and retailers have a vested interest in limiting data breach occurrences. Not only is the U.S. Federal government looking at the issue, but other countries such as Canada are acting. As a result, retailers currently playing "catch-up" are truly engaged in a highly dangerous game.

OPPORTUNITIES

Those who wish to tackle this issue from a proactive standpoint *must successfully incorporate their payment-specific security measures into larger, business-driven initiatives*. This generates a tremendous opportunity to do more than just "patch the dam." Forward-thinking retailers are reassessing their entire customer-specific data model: Utilizing the current need to become PCI compliant as a means to proactively restructure the generation, flow, and access of *all* personal customer data. This restructure can not only help avoid fines, but as we see in this report, breathe new life into existing practices and technologies.

ORGANIZATIONAL INHIBITORS

To no surprise, cost remains the primary inhibitor to retailers taking a more proactive approach to better protect customer data. However, support from the executive level of the organization has become the proven cornerstone to overturning any internal roadblocks that exist. As this year's findings draw out, winners are concentrating far more effort than their peers on ensuring that internal applications - not just one time processes - comply.

TECHNOLOGY ENABLERS

Viewing compliance as a "checkbox" project is simply not enough. Security is a fluid process. To that, myriad new technologies exist to help retailers not only become compliant, but to regulate the generation, flow, and access of customer data far more responsibly than in years' past. Experts urge retailers to follow the #1 rule of risk avoidance, "Don't store it if you don't need it." Although encrypting customer specific data and implementing logging and monitoring at every point in the data chain is critical, ultimately resolving fundamental issues in legacy operational systems to proactively manage the integrity and security of customer-specific data to prevent the opportunities for

data compromise is essential.

BOOTSTRAP RECOMMENDATIONS

To improve data security efforts all retailers should conduct a wall-to-wall assessment of where customer-specific information is held, especially personal account information. Surprisingly, only 40% have yet done so. It is also highly important to encrypt data in all life stages - particularly when it is in motion – and implement logging and monitoring at every step of the data chain. This is even more critical when data travels via wireless channels. Retailers must assign a single point of responsibility for data security and empower that function. A comprehensive breach plan is essential, and that plan should be periodically reviewed and tested. Agreements with systems providers should be reviewed and updated with proof of compliance to data security standards and “best practices,” mandates, and government regulations.

Finally, retailers must make the privacy and security of customer-specific data a Board of Directors issue, since the current vs. and desired state of data security may represent fiduciary risk and potentially impact the company’s ability to execute on its business strategy.

SECTION I: OVERVIEW

WHY THE STUDY WAS CONDUCTED

With customer-specific data captured at the point of sale, retailers can not only understand what products sell where and when, but also *who* buys those products and *how* they sell. Using sophisticated analytics, retailers are able to learn the relationships between product purchases and customer preferences, based on actual purchase behaviors, and to use that information to offer more relevant solutions to customers. Every interaction with a consumer is an opportunity to reinforce the retailer's brand identity and to increase customer loyalty by presenting compelling *value* that is based on consumer preferences.

But with this capability comes a new responsibility – ensuring the security and confidentiality of consumer data. With well publicized customer data security breaches in the headlines, this has become a pervasive societal, regulatory, and business issue in the last few years. Responding to the need for greater accountability in the safeguarding of sensitive customer payment data, VISA and MASTERCARD joined with other network payment processors to establish a commercial standard known as the *Payment Card Industry Data Security Standard* ("PCI DSS" or simply "PCI"), and have compelled retailers to comply with 12 mandates intended to ensure the privacy of stored customer-payment data.

The most notable data security breach in the public eye in 2007 was the TJX breach, where information for at least 94 million credit and debit cards was stolen. The estimated cost of replacing the cards alone is in excess of \$2 billion (paid for by the issuing banks), but additionally, as of October, 2007 the breach was estimated to cost TJX \$256 million, including \$880,000 in VISA fines. This single event, although not the only reported breach of consumer information (earlier breaches at BJ Wholesale and ChoicePoint were well covered by the press), has been a true "wake up call" to the entire retail industry.

The Customer Data Security 2007-08 Benchmark Study is intended to reveal how quickly and how well retailers are responding to the PCI mandate, and beyond that, what measures retailers are taking now to minimize the risks associated with the capture, retention, and use of customer-specific data.

METHODOLOGY

RSR uses its own model, called the "BOOT," to analyze Retail Industry issues. This model is built with our survey instruments. An explanation of the methodology can be found in Appendix A.

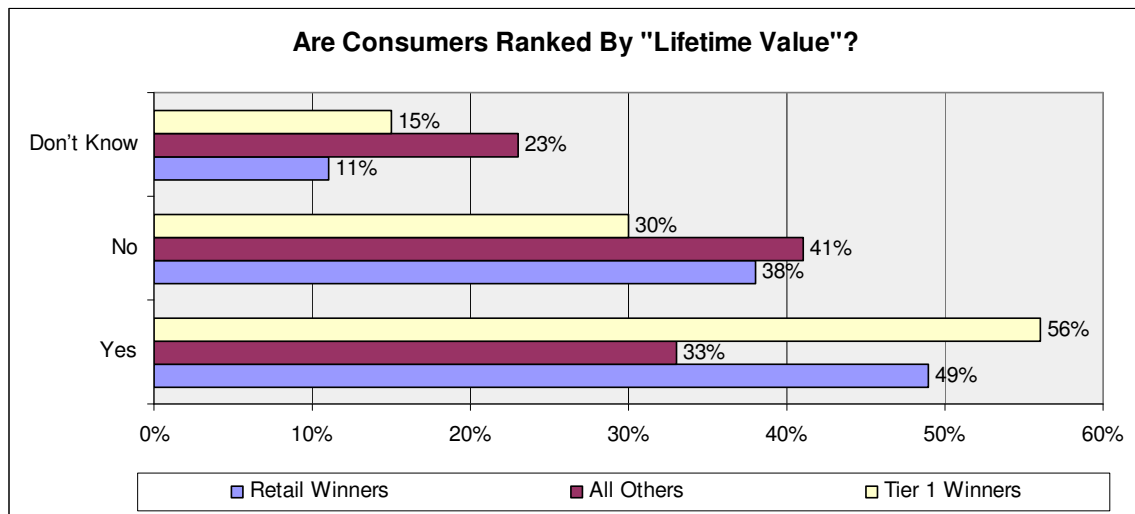
Winning is not an accident in the world of Retail. Customers vote with their wallets. Sustainable sales improvement and successful execution of brand vision are direct results of an enterprise's recognition of external and internal business issues, its ability to take advantage of opportunities for improvement, and its use of technology enablers to simplify and rationalize business processes. Data that emerges from the BOOT model helps us understand the behavioral and technological differences between winners and their peers.

DEFINING RETAIL WINNERS AND WHY THEY WIN

Our definition of Retail Winners is straightforward. We choose to follow Wall Street. Wall Street judges retailers by year-over-year comparable store sales improvements, and we do the same. Assuming industry average comparable store sales growth of three percent, we define retailers with sales above this hurdle as "winners," those at this sales growth rate as "average," and those below this sales growth rate as "laggards" or "also-rans." It is consistent throughout much of RSR's research findings that Winners don't merely do "the same things better," they tend to "do different things."

For example, in Figure 1, we can see that Retail Winners put tremendous value on using the Customer dimension to understand the “lifetime value” of their customers. Tier 1 Winners (those winners with over \$1B in top line sales) place even more importance on the customer dimension to understand “lifetime value.”

*Figure 1:
The Value of Customer Data*

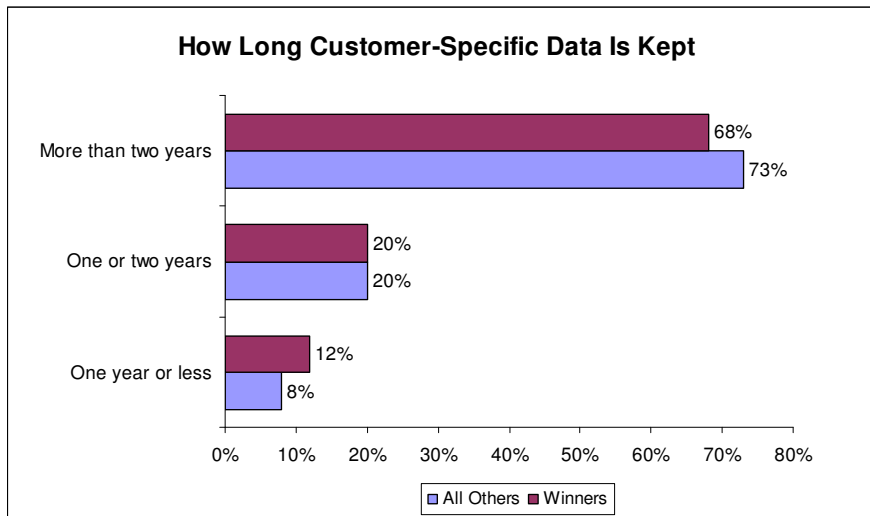


Source: RSR Research, November 2007

This begs the question: ***Does implementing technology itself create differences in performance, or are there other germane business issues driving business success?*** Of course, the answer is yes, there is more to it than just the technology. The price/performance of data storage and processing no longer restricts business intelligence applications to “the big guys.” Responses to our survey indicate that most retailers store customer-specific data for more than two years, with not much difference between winners and all others (Figure 2). But Retail Winners have a different perspective on the usefulness of the customer dimension of data. RSR’s July 2007 Benchmark ***The Next Generation of Business Intelligence¹***, showed that Retail Winners use the customer dimension of data to improve the value of the customer relationship, whereas other retailers tend to use the data to improve product merchandising effectiveness – a subtle but important difference in perspectives.

¹ ***The Next Generation of Business Intelligence: Driving Customer Insights across the Retail Enterprise- Benchmark Study: July 2007***, Brian Kilcourse & Paula Rosenblum, Copyright© 2007 by Retail Systems Research LLC

*Figure 2:
Most Retailers Keep Customer-Specific Data for Years*



Source: RSR Research, November 2007

SURVEY RESPONDENT CHARACTERISTICS

RSR conducted an online survey in October and November 2007 and received answers from 174 respondents. Respondent demographics are as follows:

- **Job Title:**

IT Management (Director, Manager, Project Lead)	21%
Audit/Security	16%
Store/Operations Management	7%
Online Channel Management	2%
C-Level/VP	21%
Other Business Function	33%

- **Revenue:**

\$499 Million or less	45%
\$500 - \$999 Million	10%
\$1 Billion - \$1.99 Billion	11%
\$2 Billion - \$4.99 Billion	18%
\$5 Billion or over	16%

- **Segments:**

General Merchandise	18%
Grocery/Drug	11%
Convenience	9%
Specialty	22%
Apparel/Softgoods	16%

Hardgoods	9%
Electronics	8
Other	8

- **Year-Over-Year Comparable Store Sales Growth Rates:**
 - Better than Average: 42 percent
 - Average: 46 percent
 - Worse than average: 12 percent

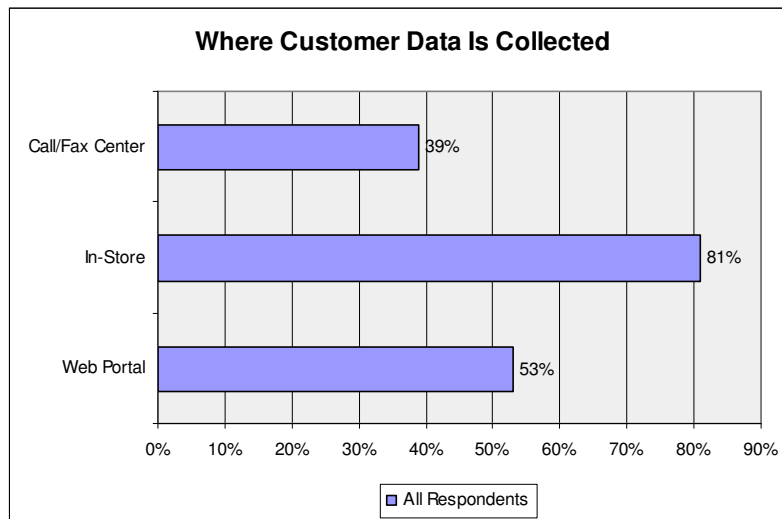
SECTION II: BUSINESS CHALLENGES

A RETAIL PARADOX: HOW TO USE CUSTOMER DATA AND STILL PROTECT PRIVACY?

Customer data matters. Retailers need customer data to respond more quickly to changes in demand patterns, to reduce out-of-stocks, to match product offerings with customers who want to buy them, and to improve their customer service. Customers are demanding a more responsive and relevant combination of products and services, tuned to their particular lifestyles.

To move towards a more customer-centric offering, retailers are using customer-specific data for business analytics, employing new technologies, and sharing that data with business partners. Massive quantities of personal data are collected and stored, from market basket transaction data captured primarily in the stores, and also from customer call centers and online offerings (Figure 3).

*Figure 3:
Where Retailers Get Customer Data*



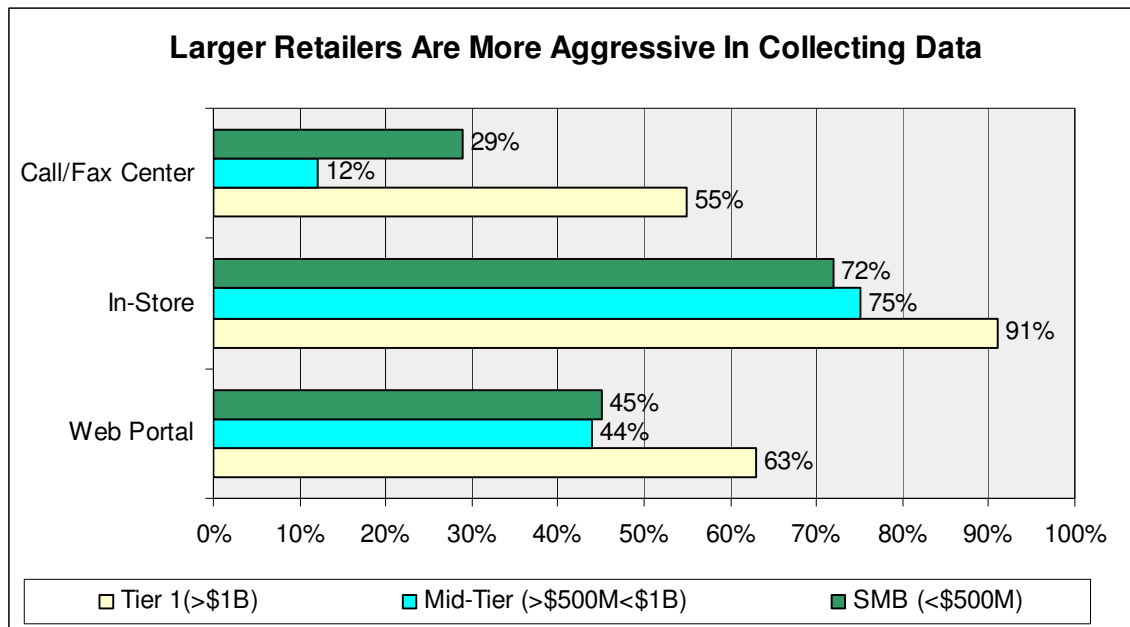
Source: RSR Research, November 2007

Retailers identify customers within their databases individually 86% of the time, according to our survey responses. Additionally, detailed transactional data is linked to specific customers by 59% of surveyed retailers, and 29% augment those customer profiles with demographic information. Customer "payment" data (for example, account or identification numbers) is stored for use in subsequent transactions, according to 45% of the total respondent group (and surprisingly, by 62% of "laggards").

COLLECTION OF CUSTOMER DATA VARIES FOR DIFFERENT RETAILING TIERS

In *The Next Generation of Business Intelligence Benchmark Study*², we learned that only 56% of retailers with annual revenues less than \$500 million use customer-specific data for business intelligence, versus 93% of retailers with annual revenue of \$1 billion or more. The Customer Data Security benchmark supports this finding; Tier 1 retailers (those retailers with annual revenue of \$1 billion or more) are more aggressive than others in collecting customer-specific data from every channel (Figure 4), and “large Tier 1” retailers (\$5B or more) are particularly aggressive in capturing that information from their web portals (79%) and call centers (62%).

*Figure 4:
Big Retailers Have Big Appetites for Customer-Specific Data*



Source: RSR Research, November 2007

CUSTOMER-SPECIFIC DEMAND DATA DRIVES THE 21ST CENTURY RETAIL VALUE CHAIN

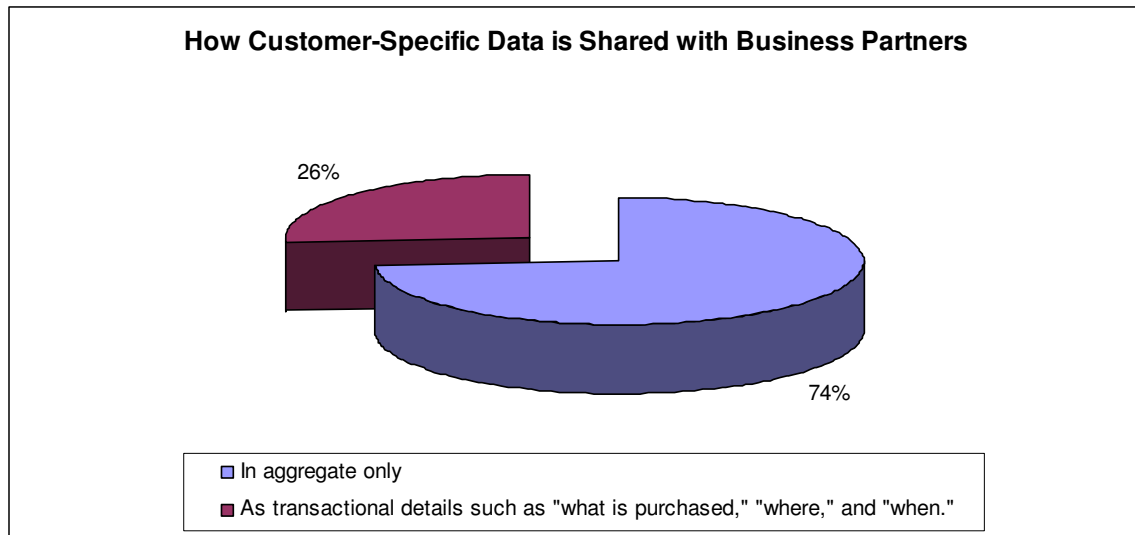
Retailers and their partners understand the value of sharing data from the point of demand (the selling environment) to where demand meets the supply chain, in order to synchronize forecasts. Retail Winners in particular are using customer-specific data to address the seemingly intractable and mutually exclusive problems of out-of-stocks (56% compared to 24% of all others) and too much inventory (52% compared to 24% for all others)³. Demand data captured at the point of sale is increasingly shared with suppliers to

² *The Next Generation of Business Intelligence: Driving Customer Insights across the Retail Enterprise- Benchmark Study: July 2007*, *ibid.*, Page 7

³ *The Next Generation of Business Intelligence: Driving Customer Insights across the Retail Enterprise- Benchmark Study: July 2007*, *ibid.*, page 5

enable a more nimble response to changes in demand while maintaining a good in-stock position – *without bloating inventories*. In The Customer Data Security study, we asked retailers to describe how they share customer-specific data with their partners. Almost three-quarters of respondents indicated that they share this information in aggregate only (Figure 5). This split is fairly consistent across all sized retailers, with minor variation.

Figure 5:
Shared Demand Data Drives the Value Chain



Source: RSR Research, November 2007

CUSTOMER-SPECIFIC DATA NEEDS TO BE PROTECTED DIFFERENTLY THAN OTHER OPERATIONAL DATA

Customer-specific data enables retailers and their partners to target their product and service offerings with more granularity to get closer to the neighborhoods that their stores operate in and offer solutions that are more relevant to specific consumers. From the customer’s perspective, this in many ways is the way retailing “used to be,” but on a potentially much larger scale. Many retailers now store credit cardholder information as a key to detailed customer purchase histories, so that they can better understand consumer demand. However, failure to secure consumer-specific data will result in brand erosion and crippling scrutiny from regulatory agencies and financial networks.

The Payment Card Industry, not waiting for government regulation or a proactive response from retailers to the potential risks, has imposed a timeline for compliance to a set of data security standards known as the “PCI DSS” (or simply “PCI”) mandate. Failure to comply has the potential to significantly raise the costs associated with accepting credit cards for payment. Credit cardholder information is increasingly the target for cyber thieves, and according to some experts only 25% of retailers know that they’ve suffered a breach before acquiring banks or the payment network processors do, and it can be as much as 12-18 months before the first evidence is detected (typically, from counterfeit credit card transactions). This creates huge risk for retailers, since not only are they penalized for the actual card numbers that have fraudulent activity against them, but also all account numbers that have been exposed by the security compromise. Fines and other losses associated with an actual security compromise can be staggering

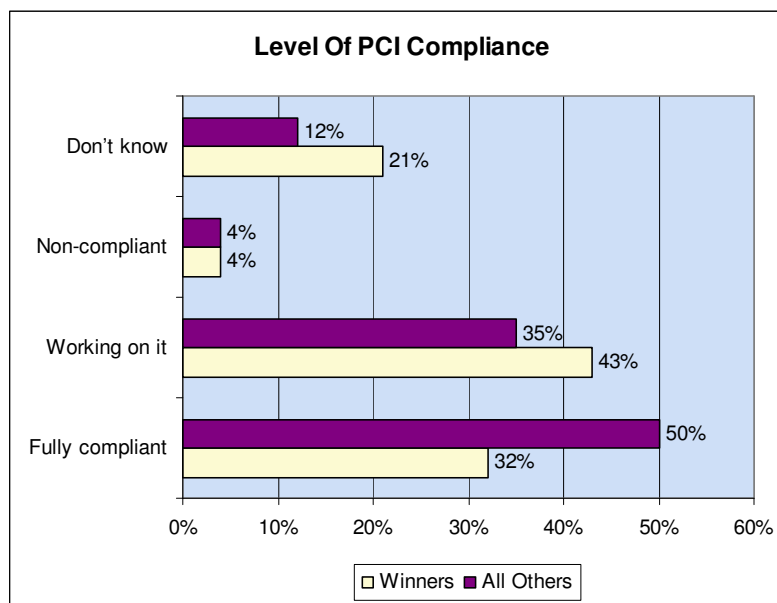
(compliance experts estimate that the fines associated with a compromise can equal \$25-35 on a per account number basis).

WHAT IS COMPLIANCE, ANYWAY?

Forty percent of our total respondent group claim to be fully compliant to the PCI 12-point mandate. Examination of the responses to other questions tends to support this claim. For example, 40% indicate that they have performed a wall-to-wall assessment of where customer-specific account data is held, and a similar number (41%) respond that they have addressed the problem of unencrypted in-flight data based on that assessment that either eliminates or encrypts that data.

Interestingly, fewer winners reported being fully compliant than all other respondents (Figure 5). In fact, a surprising number of Winners don't know what their level of compliance is. This is perhaps indicative that after several years' experience working with security experts, assessors, payment network processors, and banks, these retailers understand better than most how difficult true data security is.

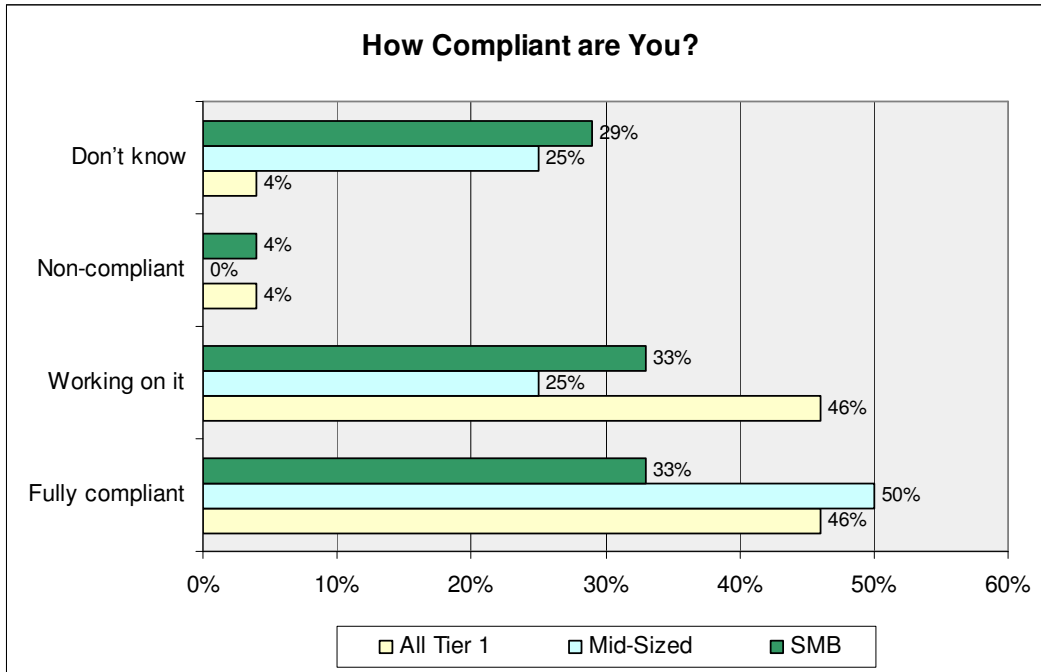
*Figure 5:
PCI Compliance: "Working on It"*



Source: RSR Research, November 2007

Looking more deeply into the issue of compliance, survey responses indicate that the level of compliance probably has to do with size and complexity of the technical environment (Figure 6). Aggregating “fully compliant” and “working on it” responses shows that all Tier 1 retailers (presumably the ones most likely to be negatively impacted by the PCI mandate since their business volume has historically enabled them to negotiate the most favorable fee structures based on their volume) may not be fully compliant, but they are closer to achieving overall compliance as a group (92%), more so than mid-tiered retailers (75%) or smaller retailers (66%). On the other hand, a surprising number of mid and small retailers admit to not knowing their state of compliance efforts (25% and 29%, respectively).

Figure 6:
Larger Organizations are Closer to Compliance



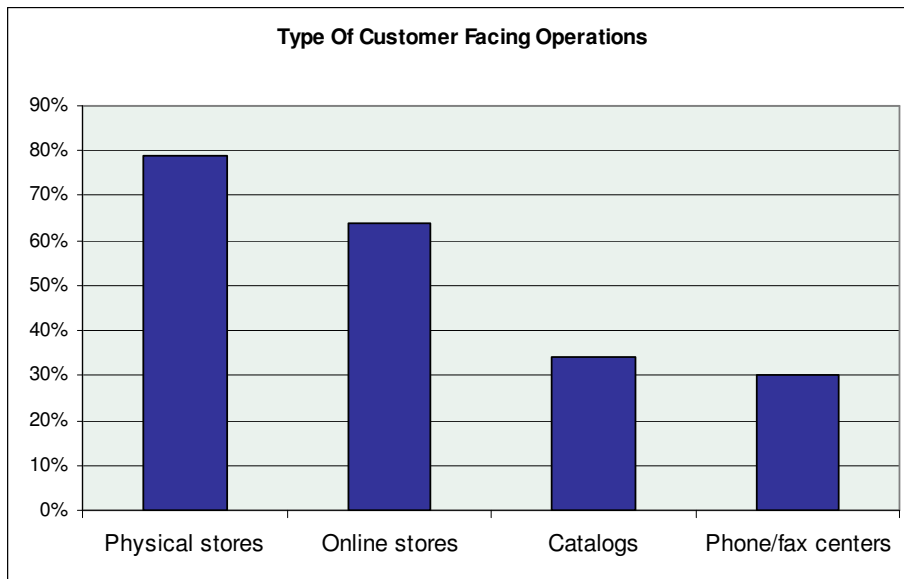
Source: RSR Research, November 2007

SECTION III: OPPORTUNITIES

SOLVING THE PARADOX: USING CONSUMER-SPECIFIC INFORMATION ... AND ENSURING PRIVACY AND SECURITY

Today, most retailers today operate not only stores but additionally one or more alternate channels (usually an e-Commerce site, Figure 7). Understanding not only market basket data but also cross-channel behaviors becomes an important aspect of merchandise planning. In a February 2007 study entitled ***Searching for the True Multi-Channel Retailer***⁴, results revealed that while “retailers are diligent about collecting customer information across virtually all selling channels... fully 40 percent of our respondents may collect this data, but they don’t use it...Only 30 percent have the integrated CRM systems needed for effective use of cross-channel customer management.”

*Figure 7:
Today’s Retailers Usually Have Multi-Channel Operations*

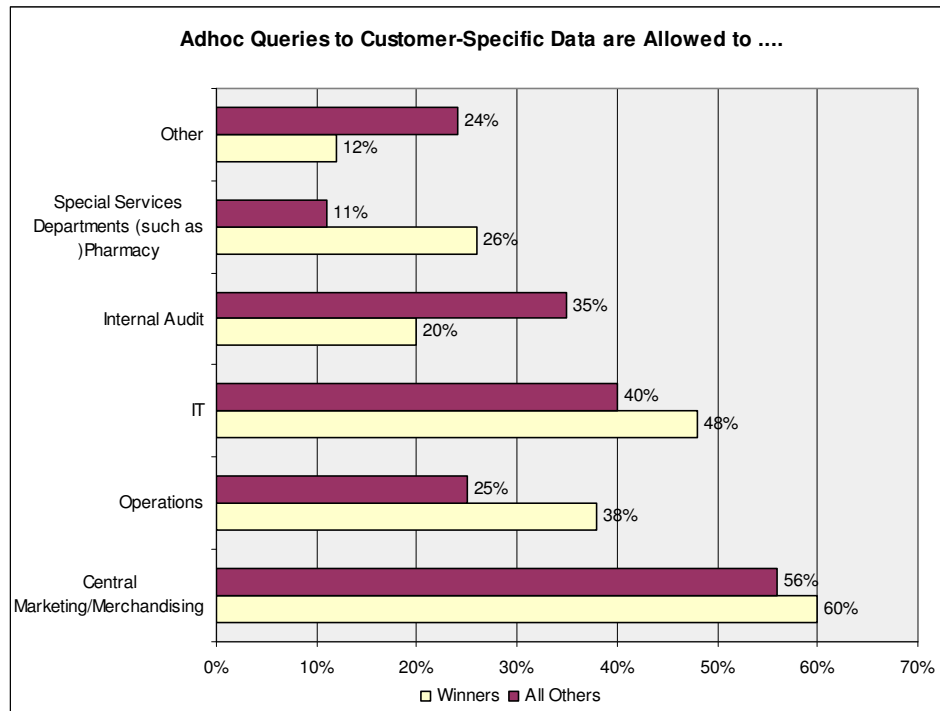


Source: RSR Research, November 2007

Although the earlier study indicated that lack of integrated merchandise planning remains an obstacle to multi-channel retailers, there is little doubt that the customer dimension of data is being heavily queried, particularly by Marketing/Merchandising Departments, as our survey responses show (Figure 8). Retailer Winners are slightly more aggressive in opening up the data to adhoc queries (60%), while tier-1 Winners show the most willingness, with 73% of those respondents granting open access of sensitive Customer data to Marketing/Merchandising.

⁴ *Searching for the True Multi-Channel Retailer, Benchmark Report 2006-2007*, Paula Rosenblum, licensed 2007 by RSR.

Figure 8:
Open Access to Customer-specific Data is Common...



Source: RSR Research, November 2007

With access capabilities comes a responsibility to ensure that the data is used by only those who have a legitimate business need, and in this regard, our respondents feel that the PCI mandate to “restrict access to data by business need-to-know” is not particularly difficult. Only 26% of our respondents identified this requirement as one of the top three most difficult mandates to comply with, below requirements to “Develop and maintain secure systems and applications,” “Track and monitor all access to the network,” and “Assign unique ID to each person with access” in difficulty to the respondent group as a whole.

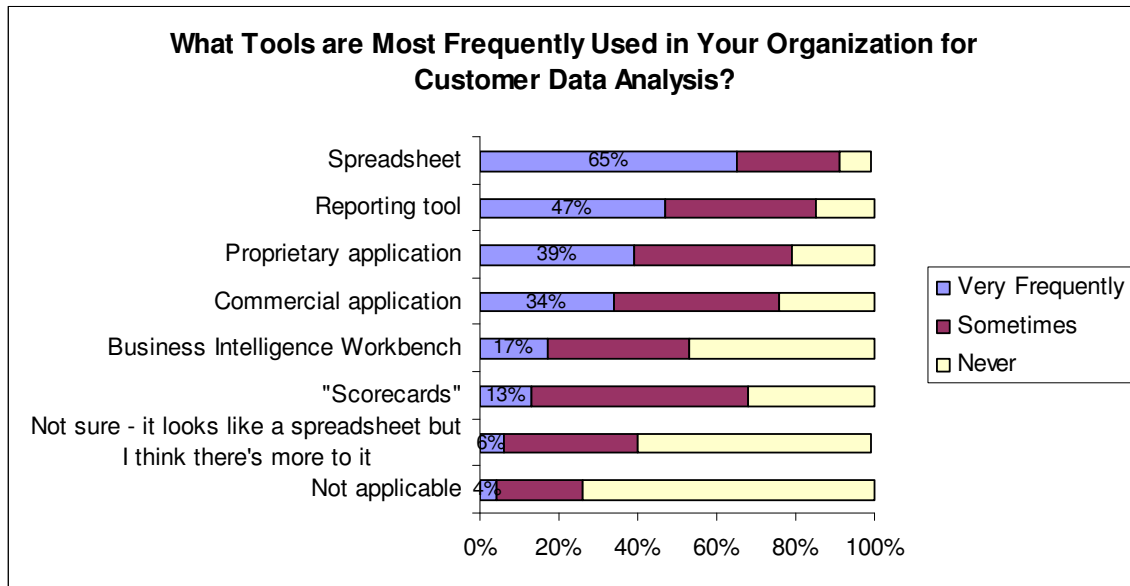
This result indicates that retailers don’t clearly understand the risk. It has become almost an urban legend that laptop PCs, in particular, pose one of the greatest threats to the security of customer specific data. Looking at the level of adhoc queries allowed to merchants and operations staff, we begin to understand how such access creates risk. RSR’s *Next Generation of Business Intelligence Benchmark Study*⁵ identified that the ubiquitous spreadsheet is the most commonly used tool for analysis of customer-specific data (Figure 9). This speaks as much to the state of legacy merchandise planning systems as to retailers’ awareness of the risks associated with uncontrolled access, as has been mentioned.

Many retailers seek to mitigate the risk of data breach with compensating controls such as audits, forensic data logging and analysis, monitoring, etc. Ultimately however, the need to integrate all channels of the

⁵ *The Next Generation of Business Intelligence: Driving Customer Insights across the Retail Enterprise- Benchmark Study: July 2007*, ibid.

business and utilize the customer dimension of data in business intelligence and merchandise planning processes also creates the opportunity to address the core data security problem, if retailers implement systems and processes that proactively control access to sensitive data, rather than merely providing the ability to discover policy breaches after-the-fact.

*Figure 9:
The Spreadsheet Reigns as the Most Common Analysis Tool*



Source: RSR Research, July 2007

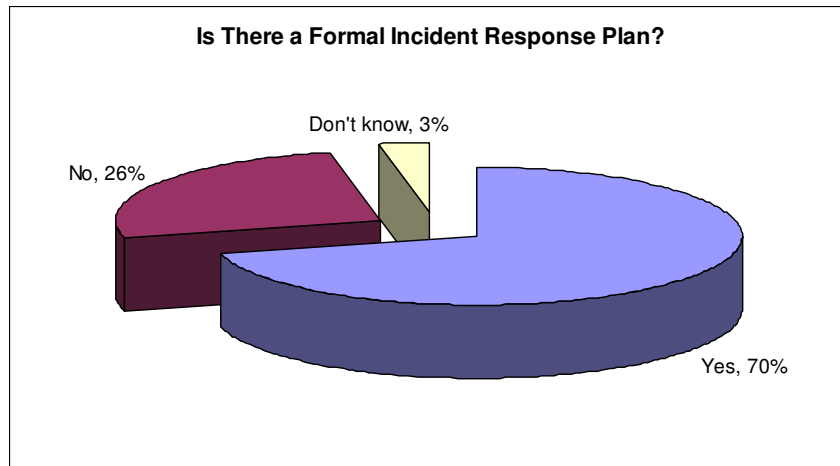
THE PCI MANDATE DRIVES A MORE PROACTIVE APPROACH TO DATA SECURITY

Past studies by RSR analysts have shown a steady improvement in retailers' attitudes about funding and staffing a single point of responsibility for data security. Our 2006 study indicated 67 percent of retailers had established a data security coordinator, up from 57 percent in 2005⁶. In this year's study, fully 83% of respondents indicate that their companies have designated a security program coordinator to address internal and external risks to the security confidentiality and integrity of personal information. This is a big improvement over prior years' studies; experts agree that one of the most important aspects of a data security program is to establish a single point of accountability and to empower that person to implement controls.

Eighty-seven percent of respondents indicated that their companies provide training for its employees regarding consumer privacy and information security, up from only 47% in the 2006-07 study. And whereas the 2006-07 study showed that only 53% of respondents had a formal incident plan in place, this year's study shows a remarkable improvement (Figure 10). As in prior years, far fewer have actually tested that plan. This year's respondents indicated that 49% test the plan at least annually, and 20% more frequently.

⁶ *Customer Data Security: Annual Benchmark Study 2006-2007*, Brian Kilcourse & Steve Rowen, Licensed by RSR

*Figure 10:
70% of Retailers Have A Plan In Place*



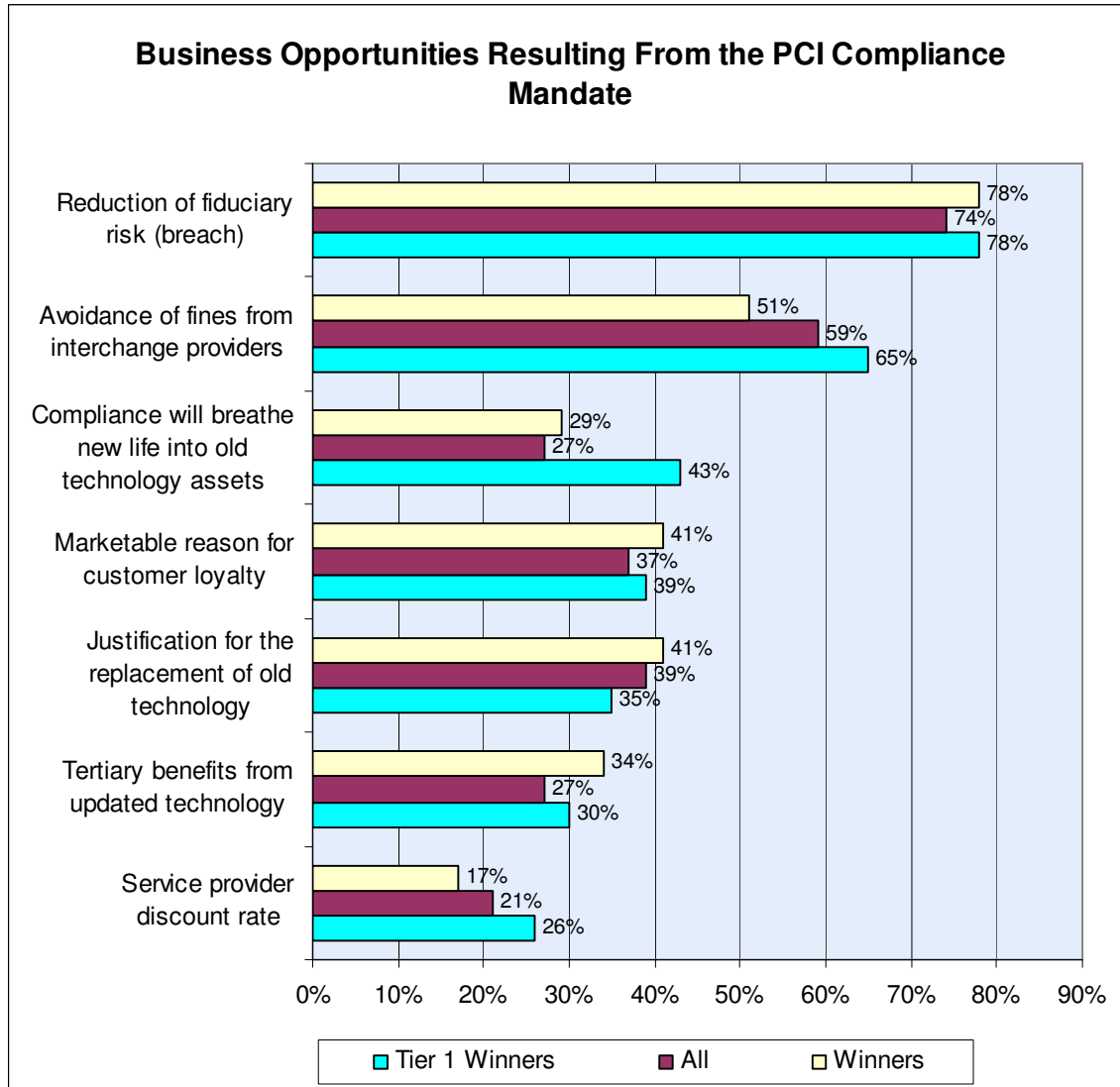
Source: RSR Research, November 2007

Any formal incident plan should include a communication plan that includes how to notify consumers, banks and financial networks, and law enforcement. The biggest danger is in doing nothing, even if not hearing complaints from irate customers. Smart hackers compromise more than one merchant, then wait often more than a year before initially using small samples of the stolen data.

THE PCI MANDATE CAN DRIVE OTHER BENEFITS

Although mitigating fiduciary risk and possible fines are the strongest benefits to be accrued from PCI compliance, our respondent group sees other potential benefits (Figure 11).

*Figure 11:
More than Just Avoiding Risks*



Source: RSR Research, November 2007

Tier-1 Winners in particular see PCI compliance as a way to breathe new life into old technology assets, according to 43% of respondents, compared to all Retail Winners, who see PCI compliance more as a justification for replacing old technology (41%). Large retailers have shown a remarkable ability to operate old store technology solutions long after their “book life” has expired. This is driven largely by the fact that merchandising and point-of-sale system replacements are among the most expensive and time consuming endeavors any retailer can undertake, because they impact stores. Therefore it is no surprise that larger retailers have a strong desire to renew, rather than replace, their technology, regardless of the

rationale for doing so. Interestingly, laggards put hope in PCI compliance as a justification for new technology, according to 50% of those respondents, perhaps indicating a hope that the mandate will break the logjam of stalled investment in store, multi-channel, merchandise planning, and business intelligence technologies.

All having been said, PCI compliance is perceived to have more “technology” benefit than “business” benefit according to our respondents, although 29% credited PCI compliance as having “great value” for their company. According to our survey results, retailers generally have not connected the dots to establish a connection between ensuring that customer-specific data is used to create differentiating value while still ensuring the security and privacy of that data, and being a **Retail Winner**.

SECTION IV: ORGANIZATIONAL INHIBITORS

'PCI COMPLIANCE' DOESN'T MEAN 'SECURITY'

The problem with the notion of “compliance” equaling “security” is that the nature of the threat is evolving and fluid. Criminals focus on credit card track data (the information stored on the magnetic stripe on credit cards) because counterfeit credit cards have a high street value. According to Visa, the frequency of reported data breaches has increased from seven per month in 2006 to 16 per month in 2007. Although restaurants are the single most frequent target (44%, according to Visa statistics), clothing retailers account for 68% of reported data compromises. In our survey, although 46% of retailers who self-identified as apparel/specialty operators claimed to be fully PCI compliant, another 31% said they don't know their company's status, and 54% don't have a single organizational point of responsibility for data security (compared to 83% for the total response group who do).

The extraordinarily cross-functional nature of the data security issue requires strong leadership coming from the top of the company, since ultimately this is an issue that can negatively affect the company's brand and its ability to execute on its business strategy. Because these are Boardroom issues, it is frequently the CFO, and not the CIO, who is the target for vendors trying to sell PCI compliance programs and technologies. A comprehensive plan to minimize risk needs to include not only end-to-end security management, monitoring and auditing, appropriate use policies, and a data breach response plan, but also avoidance as the first order of business. Many experts strongly advise retailers, “Don't store it if you don't need it” as the #1 rule of risk avoidance.

For example, unless a retailer has a loyalty program or a multi-channel offering, there may be little need to store customer addresses (if the retailer doesn't have customer address in its databases, which limits its liability to notify customers in the event of a breach). The problem with such an approach is that retailers' marketing and merchandise planning personnel want to use the data. As we saw in Figure 8, there is widespread adhoc access to customer-specific data by marketing/merchandising, operations, and IT staffs.

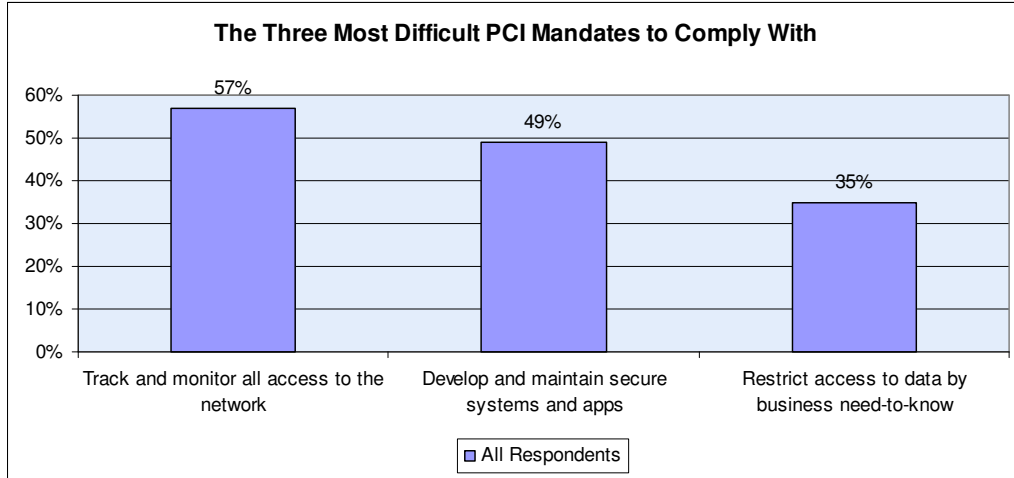
Fiduciary, technical, and marketing issues collide to create a witch's brew of challenges which can go unresolved until disaster strikes. What experts fear the most is that rather than deal with these issues, retailers will adopt a compliant-until-compromised attitude, exposing themselves and their customers to great risk. As one pundit put it recently, “It is the unknown unknowns that will get you.”⁷

IT ISN'T EASY TO CHANGE

Survey respondents identified action items installing and maintaining a firewall, using and updating anti-virus software, and not using vendor-supplied passwords, as the three easiest PCI mandates to comply with. It is fairly evident why; these mandates require one-time or very infrequent changes. However, other mandates that deal with fundamental business practices, such as establishing security policies and procedures, proactive monitoring, and certifying and maintaining secure applications, are much harder to comply with (Figure 12), because these things mean changing the “whatever it takes” culture so typical of retail companies.

⁷ Steve Hunt, Founder, 4AI Research

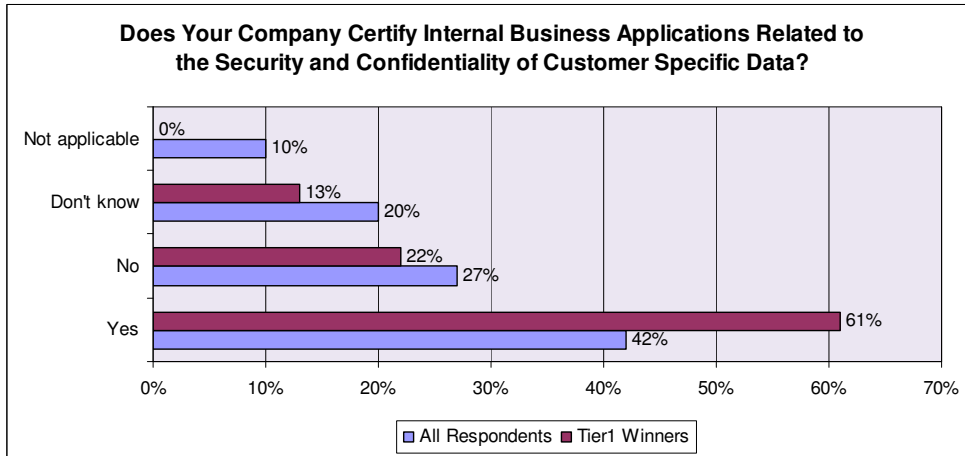
Figure 12:
Business Policy and Process Changes are Hard to Implement



Source: RSR Research, July 2007

Tier 1 retailers rated the requirement to develop and maintain secure systems and apps as the most difficult mandate with which to comply (58%). To overcome this concern, Tier 1 Winners have concentrated a significant amount of effort on ensuring that their internal applications comply with customer data security policies, far more than the “all respondent” group (Figure 13).

Figure 13:
Top-Tiered Winners Certify Business Applications



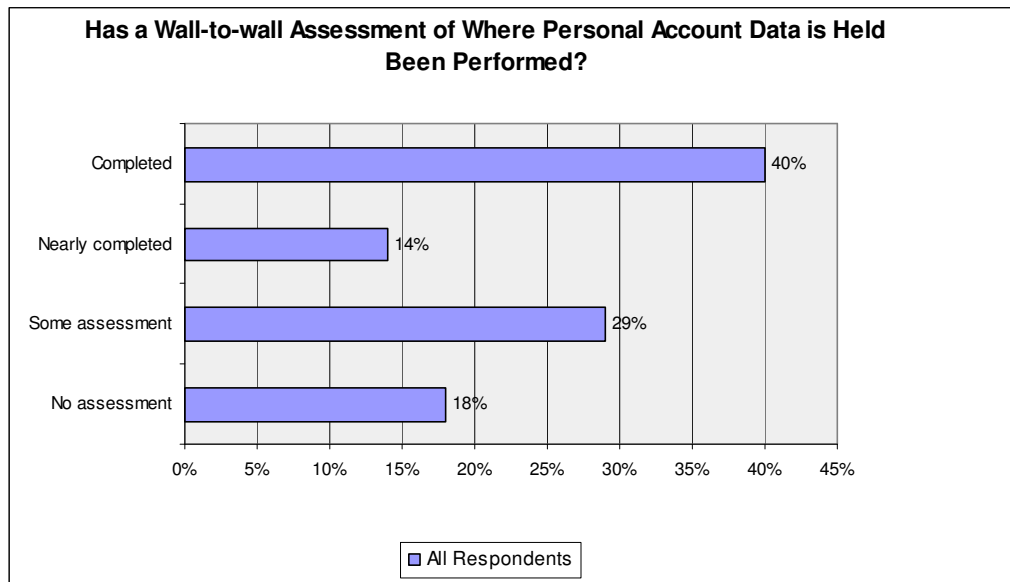
Source: RSR Research, November 2007

SECTION V: TECHNOLOGY ENABLERS

ASSESSING BOTH TECHNOLOGY AND PROCESS

In many ways, implementing a program to secure sensitive customer-specific data bears resemblance to the Y2K efforts of almost ten years ago. However, unlike Y2K, this isn't merely a technology-related issue; there are business policies and processes to be modified or implemented. Before all else, retailers need to take stock of where sensitive customer-specific data is (even temporarily), to scope both their technology and business process issues (Figure 14). Companies must find and classify the data, protect it, manage it, and be prepared for a breach, even after controls are put into place.

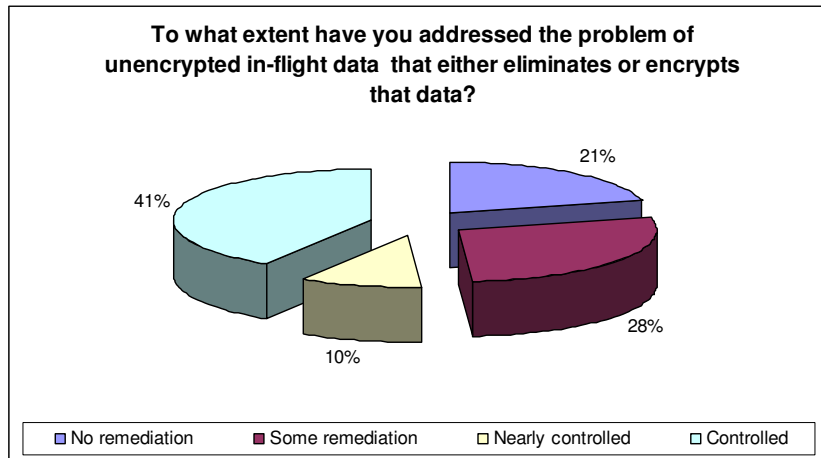
*Figure 14:
Assessing the Scope*



Source: RSR Research, November 2007

Once the assessment has been performed, then technical issues can begin to be addressed. Experts agree that it's the first order of importance to get rid of the data that the business doesn't need. Retailers should remove track data (since among other things, doing so greatly reduces the financial exposure from potential fines), then encrypt what is kept. As Figure 15 shows, a similar number of survey respondents who claim to be fully compliant also indicate that they have either encrypted or eliminated sensitive data in their technology environments.

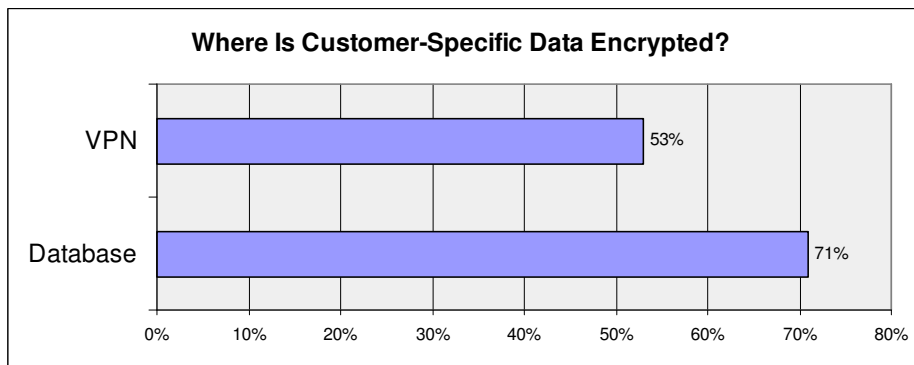
Figure 15:
Encrypt It or Get Rid of It



Source: RSR Research, November 2007

It is important that data needs to be protected both where it sits, and when it’s in motion. To understand retailers’ progress on both fronts, we asked “where” the data is encrypted (Figure 16). Although Winners track to the total response group on this question, 81% of Tier 1 retailers report that they encrypt at the database level. All groups of respondents indicate that there is still much work to be done to encrypt in-flight data, especially that which flows through their VPN connections.

Figure 16:
Where is it Encrypted?



Source: RSR Research, November 2007

LOGGING & MONITORING – EVERY STEP OF THE WAY

The importance of forensic logging *at each step in the data chain* cannot be overstated, according to risk assessors that RSR spoke to. Many tools exist in the market now to enable retailers to wrap logging around technologies that do not have such capabilities inherently; database logging and transactional logging are also important (but experts also remind us to *encrypt* transactional logs as well). Where

forensic logging isn't possible, compensating controls must be put in place that limits the company's exposure to data compromise. Finally, most experts recommend that active monitoring of every step of the data chain should be in place. When forensic exams are conducted, the first question that assessors ask is, "Were the controls reasonable?" Technologies exist now to ensure that that question can be answered in the affirmative.

SOLUTIONS PROVIDERS: TRUST, BUT VERIFY

Since many retailers depend on software and services providers, this poses a special risk. Experts contend that even very large and well-known solutions providers may not be compliant to the PCI mandate – while the retailer bears the risk. The most important protection for this potential risk is a well-crafted contract. Retailers should carefully review independent assessment results, insist that the assessment report is included in the contract and that the solution provider contractually accepts responsibility in the event of a breach.

SECTION VI: BOOTSTRAP RECOMMENDATIONS

DO THE ASSESSMENT AND MAP MANDATES TO THE BUSINESS

It came with great surprise that only 40% of respondents had conducted to completion a wall-to-wall assessment of where personal account data is held. Only once this assessment has been performed can retailers fully understand where their weaknesses exist and how to address these problems. Without assessment, virtually no retailer can dream of being anything more than reactive – at best – in their data security practice. As a result, this is a first-step recommendation. Once the assessment is completed, retailers should map PCI mandate requirements and government regulations to current business processes and systems. This is an important step since mandates and regulations may overlap. Once this mapping exercise has been completed, the company can then prioritize changes to both operational processes and systems.

LOCK IT UP

In an ideal world, all consumer-specific data – not just that pertaining to payment data – should be encrypted. For example, information transmitted via wireless must be protected beyond merely implementing WEP. While the PCI DSS is very specific in its requirement for encryption of personal account numbers, forward-thinking retailers will view this challenge/opportunity to remain at least one step ahead of industry mandates – and potential law. While SOX and HIPPA regulations are obvious tie-ins, retailers are well advised to consider what security and privacy issues may exist with the level of data the organization currently collects – and proactively secure accordingly.

LET IT GO

Many experts strongly advise retailers, “Don’t store it if you don’t need it” as the #1 rule of data security risk avoidance. The vast majority of retailers large and small hold on to sensitive data for more than two years, according to our survey results. Retailers really need to become more systematic in the destruction of transactional data once the business purpose for keeping it has expired.

GET A HANDLE ON THE NETWORK

While larger retailers seem to be more focused on ensuring that sensitive data remains secure throughout the lifecycle of business applications, retailers of all sizes indicated tracking and monitoring all access to the network as a major source of pain. This pain can be mitigated by enacting clear policies of network administration, but again, can only be accomplished once full understanding of the “real view” of current practices is attained. Logging and monitoring are key technology enablers in ensuring a secure network. Experts also recommend frequent network penetration tests.

CUSTOMER DATA SECURITY MUCH MORE THAN A COMPLIANCE PROJECT

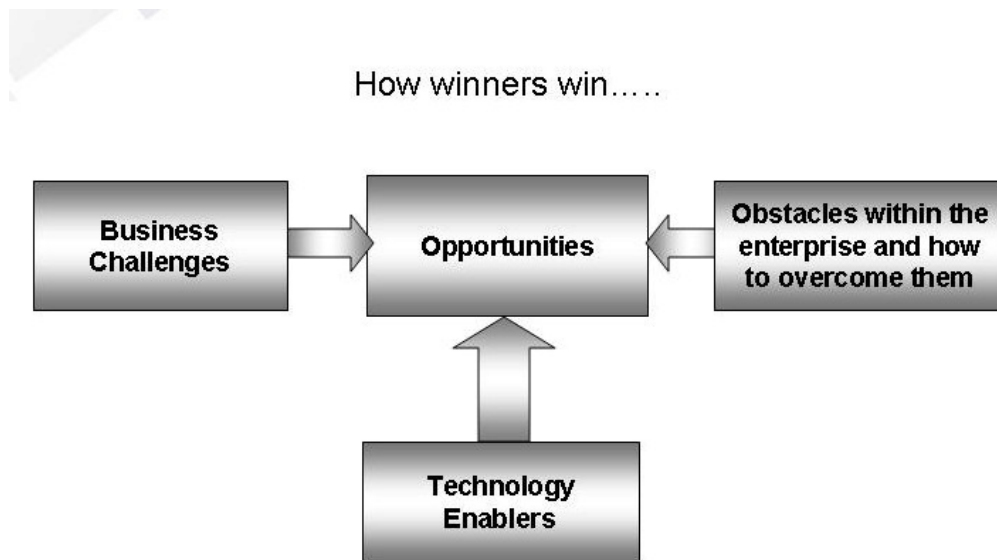
Since customer data security ultimately is an issue that can affect the company’s brand and its ability to execute on its business strategy, making discussion of the issue a regular agenda item for the Board of Directors is absolutely vital. Those retailers who’ve successfully demonstrated to their Board: a) what their current security practices are, b) where the dangers lie, and c) where their practices *should be* have a far greater likelihood of driving home the fiduciary risk that surrounds non-secured customer-specific data.

APPENDIX A: THE BOOT METHODOLOGY

The “BOOT” methodology is designed to reveal and prioritize the following:

- **Business Challenges** – Retailers of all shapes and sizes face significant **external** challenges. These issues provide a business context for the subject being discussed and drive decision-making across the enterprise.
- **Opportunities** – Every challenge brings with it a set of opportunities, or ways to change and overcome that challenge. **The ways retailers turn business challenges into opportunities often define the difference between winners and “also-rans.”** Within the BOOT, we can also identify opportunities missed – and describe leading edge models we believe drive success.
- **Organizational Inhibitors** – Even as enterprises find opportunities to overcome their external challenges, they may find **internal** organizational inhibitors that keep them from executing on their vision. Opportunities can be found to overcome these inhibitors as well. Winning retailers understand their organizational inhibitors and find creative, effective ways to overcome them.
- **Technology Enablers** – If a company can overcome its organizational inhibitors it can use technology as an enabler to take advantage of the opportunities it identifies. Retail Winners are most adept at judiciously and effectively using these enablers, often far earlier than their peers.

A graphical depiction of the BOOT follows:



APPENDIX B: ABOUT OUR SPONSORS



Apani® is the preeminent provider of cross-platform server isolation solutions for large companies, protecting servers and business-critical data within the corporate network.

Apani EpiForce®, the company's flagship product, is a software-based solution that enables two powerful disciplines – logical security zoning and policy-based encryption of data in motion. EpiForce is a distributed, centrally-managed solution that works seamlessly in both traditional and virtualized environments and is transparent to users, applications and infrastructure – making it quicker to deploy and less costly to manage than any hardware-centric solutions. Founded in 2003, Apani is privately held and based in Southern California.



BitArmor's powerful new DataControl™ software provides a faster, easier, more cost-effective way to protect and manage sensitive data throughout any retail organization. Unlike traditional solutions that only deal with information at specific points in the system, DataControl attaches a Smart Tag™ directly to the data – a tag that travels *with* data to secure, track, and control it wherever it is stored. BitArmor helps retailers protect sensitive customer information, achieve regulatory compliance, and manage data throughout its functional lifecycle.

To learn more, visit www.bitarmor.com.



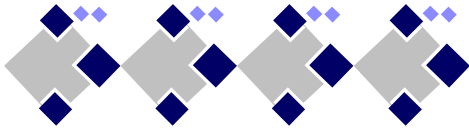
Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Cisco hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction and strengthen competitive advantage. The Cisco Intelligent Retail Network provides the foundation for delivering a set of common services to a broad range of devices and applications. This platform enables retailers to provide a single, centrally managed network for consistent and efficient data integration across functions and channels, as well as better security, manageability, and availability. Information on Cisco can be found at www.cisco.com. For Cisco Retail news, please go to www.cisco.com/go/retail.

APPENDIX C: ABOUT RSR



Retail Systems Research (“RSR”) is the only research company run by retailers for the retail industry. RSR provides insight into business and technology challenges facing the extended retail industry, providing thought leadership and advice on navigating these challenges for specific companies and the industry at large. We do this by:

- **Identifying information** that helps retailers and their trading partners to build more efficient and profitable businesses;
- **Identifying industry issues** that solutions providers must address to be relevant in the extended retail industry;
- **Providing insight and analysis** about a broad spectrum of issues and trends in the Extended Retail Industry.



Copyright© 2007 by Retail Systems Research LLC • All rights reserved.

No part of the contents of this document may be reproduced or transmitted in any form or by any means without the permission of the publisher. Contact research@rsrresearch.com for more information.