
Retail Data Security

*Value vs. Vigilance:
Using and Securing Consumer-specific Data*



2nd Annual Benchmark Study 2006-2007

Sponsored By



WRITTEN BY
BRIAN KILCOURSE
CEO



Table of Contents

SECTION I: Overview	3
Why the Study Was Conducted.....	3
Methodology	3
Defining Retail Winners	3
Survey Respondent Characteristics	4
SECTION II: The Business Challenge.....	5
Value vs Vigilance.....	5
SECTION III: Opportunities	7
Using Consumer-specific Information to Better Understand Demand - While Still Ensuring Privacy and Security	7
SECTION IV: organizational barriers.....	10
While Steps are Being Taken to Establish Organizational Accountability, Retailers are Reacting Slowly	10
SECTION V: technology enablers.....	13
The Good News: Technologies Will Help Mitigate Risk – If They Are Used.....	13
SECTION VI: Bootstrap Recommendations	15
Do It Now	15
“Bootstrap” Recommendations.....	15
Report Sponsors.....	17

Figures

Figure 1: Customer-specific Data Captured at POS.....	5
Figure 2: Use of Consumer-specific Payment Data.....	6
Figure 3: POS Transactions Linked to Consumer-specific Data.....	7
Figure 4: Retailers Who Rank Customers for Lifetime Value.....	8
Figure 5: Sharing Consumer-specific Data with Trading Partners	9
Figure 6: Retailers’ Level of Compliance.....	10
Figure 7: Adhoc Queries to Consumer-specific Data	11
Figure 8: How Data is Shared with Trading Partners.....	13

EXECUTIVE SUMMARY

The security and confidentiality of consumer data has become a pervasive societal issue in 2006. Well-documented breaches have heightened the public's – and regulatory agencies' - concerns about how well companies are securing consumer-specific information captured at the point-of-sale.

The Retail Data Security 2005 Benchmark Study revealed that while many retailers are collecting and keeping data about specific consumer purchases, there was room for improvement in securing consumer-specific data. Although many companies have taken steps to protect their computing environments via state-of-the-art network architectures, secure VPNs, firewalls, "DMZ's," malware filters and patch management, the question remains whether retailers are taking extra measures to ensure that consumer-specific information digitally stored within operational databases is kept confidential and secure. *The objective of the Retail Data Security Benchmark Study 2006-2007 was to get an update on how consumer-specific information is acquired, used, and secured by companies in the extended retail industry today.*

THE BUSINESS CHALLENGE

Retailers are continuously challenged to provide compelling value to consumers, beyond mere product pricing, availability, and convenience. New technologies make it increasingly feasible for retailers to relate item movement to specific customer information, and to analyze that relationship to develop merchandising strategies that are more relevant to individual customers' needs. Retail winners are more aggressive in the use of consumer-specific information to differentiate from competitors' ubiquitous product-oriented merchandising strategies. However, consumers, government regulatory agencies, and financial networks are growing increasingly concerned that consumer privacy is jeopardized by the potential of security breaches within retailers' technology environments.

OPPORTUNITIES

The goal of a customer centric merchandising strategy is to present a compelling value proposition in a way that is meaningful to individual consumers. Many retailers' merchandising strategies are increasingly consumer-oriented and driven by sophisticated analytics that link consumers to purchase history. Retailers are now able to understand who their "best" customers are and how best to merchandise to them. A retailer's brand proposition is improved by the effective use of consumer-specific information to be more *customer-centric*. Even though most retailers are now capturing vast amounts of customer data from the point-of-sale, many are only using that information to better focus their traditional product oriented merchandising strategies.

ORGANIZATIONAL BARRIERS

Although the picture has improved since the 2005 Benchmark, the majority of retailers still have not gone far beyond usual and customary measures to ensure the privacy and integrity of that data.

TECHNOLOGY ENABLERS

Technologies such as network architectures, data encryption, access control, and forensic tools for examining logfiles exist now to help companies ensure the privacy and security of consumer-specific information. Additionally, sophisticated methodologies are available to test the efficacy of security measures. Industry standards, such as PCI, have been developed to prescribe best practices for ensuring the privacy and integrity of consumer-specific information.

"BOOTSTRAP" RECOMENDATIONS

We believe the evidence is clear: **Now** is the time to address the organizational and technical issues surrounding the effective use and security of consumer-specific information. Those companies that effectively use this information to drive customer value while at the same time ensuring its privacy and integrity, will be rewarded with increased customer loyalty and improved earnings. Failure to secure consumer-specific data will result in brand erosion and crippling scrutiny from regulatory agencies and financial networks.

SECTION I: OVERVIEW

WHY THE STUDY WAS CONDUCTED

Retail Systems Alert Group (RSAG) initiated the 2nd *Annual Retail Data Security Benchmark Survey 2006-2007* to update the baseline for how retailers are ensuring the privacy and security of consumer-specific data today. We wanted to understand the most typical methods used by retailers to capture and use consumer specific data, and to determine the extent to which companies are using advanced technologies and methods to secure that data.

METHODOLOGY

RSAG uses its own model, called “BOOT,” to analyze issues in the Extended Retail Industry (ERI). This model is built with our proprietary survey instruments. Specifically, the BOOT methodology is designed to reveal and prioritize the following:

- **Business Challenges** – RSAG queries enterprises to help them self-identify the biggest external challenges they face. These issues provide a business context for the subject being discussed.
- **Opportunities** – Every challenge brings with it a set of opportunities, or ways to change and overcome that challenge. RSAG’s surveys ask respondents how they’re choosing to meet their challenges.
- **Organizational Inhibitors** – Even as enterprises find opportunities to overcome their external challenges, they may find internal organizational inhibitors that keep them from executing upon their vision. Opportunities can be found to overcome these inhibitors as well. RSAG’s surveys help respondents determine what their organizational inhibitors are and how to conquer internal challenges.
- **Technology Enablers** – The Extended Retail Industry can no longer function without a strong technology foundation. RSAG surveys question retailers about the technologies they employ to solve their business challenges.

RSAG believes winning is not an accident in the Extended Retail Industry. **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 retail winners and their peers.

DEFINING RETAIL WINNERS

Our definition of retail winners is straightforward. We follow Wall Street. Wall Street judges retailers by their year-over-year comparable store sales improvements, and RSAG does the same. Assuming an industry average comparable store sales growth of three percent, we define retailers with sales above this hurdle as “winners,” those at the sales growth rate as “average,” and those below this sales growth rate as “laggards” or “also-rans”.



SURVEY RESPONDENT CHARACTERISTICS

RSAG conducted an online survey between August and October, 2006 and received complete sets of answers from 51 retail respondents. Respondent demographics are as follows:

- **Functional Area:** Twenty-four percent of respondents were CEOs and CIOs, 6 percent from line-of-business managers, with the remainder from IT and other areas.
- **Revenue:** Forty-three percent of respondents had annual revenues of \$499 million or less, 18 percent had annual revenues of \$500 million to \$999 million, with the remainder having annual revenues of over \$1 billion.
- **Retail Segments:** Ten percent were General Merchandisers, 8 percent were Convenience Operators, 4 percent came from Grocery/Drug, 36 percent identified themselves as Specialty, 10 percent from Apparel, with the remainder coming from hardgoods, electronics, and other retail categories.
- **Retail Channels:** Eighty-three percent report that 75 percent or more of their revenue is achieved via physical retail stores. Eight percent of respondents reported that less than 25 percent of their revenue comes from physical stores.
- **Year-Over-Year Comparable Store Sales Growth Rates:** Assuming average comparable store revenue growth of three percent, 54 percent reported better than average results, 34 percent reported average results, and 12 percent self-identified as below average.



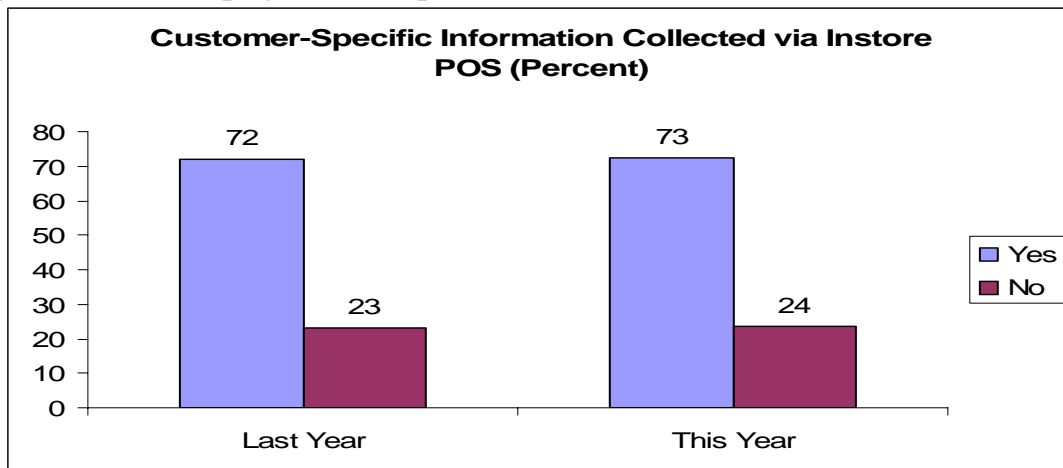
SECTION II: THE BUSINESS CHALLENGE

VALUE VS VIGILANCE

In an environment where price and convenience have long dominated retailers' value offerings to consumers; it has now become increasingly important for retailers to emphasize service as a way to deliver meaningfully differentiated value. Consumers now have multi-channel options for their shopping needs, and low price and availability are baseline expectations. Many retailers' merchandising strategies are increasingly consumer-oriented and driven by sophisticated analytics that link consumers to purchase history. The strategies reveal buying preferences as well as revenue and profit value of individual consumers. These retailers take every interaction as an opportunity to reinforce their brand identity and to increase customer loyalty by presenting compelling *value* to consumers that is based on consumer preferences as revealed by past purchases. However, because of the sensitivity of consumer-specific information and the risk associated with failure to adequately secure that information, retailers must be *vigilant*, and go beyond past practices to ensure that customers' privacy is protected.

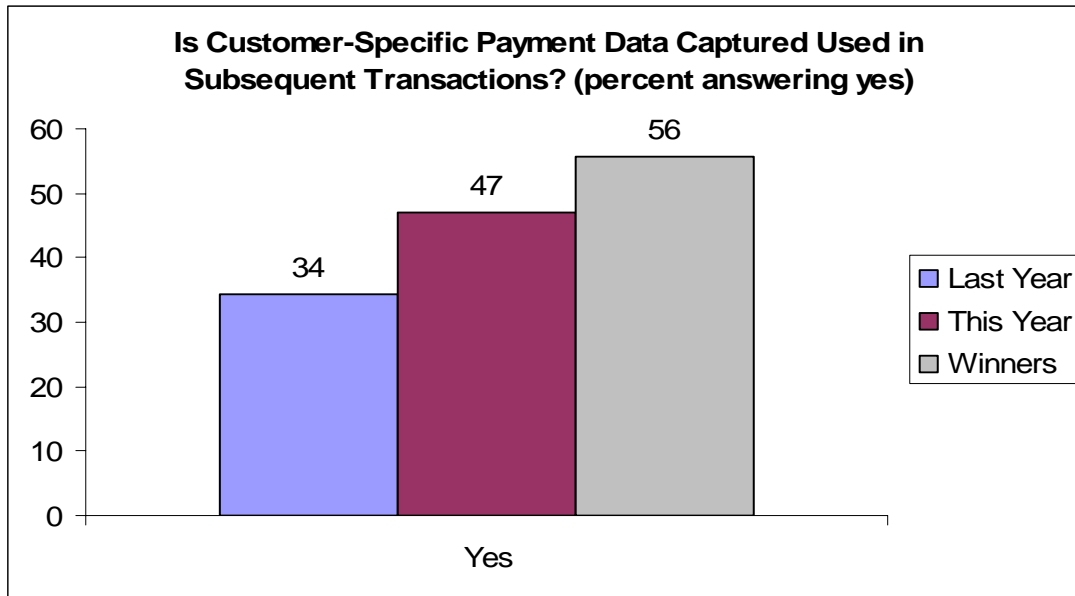
The Retail Data Security Benchmark 2006-2007 reveals that over 72 percent of Extended Retail Industry companies are using consumer specific data captured at the point-of-sale to move toward more demand-driven merchandising, analyze marketbaskets to better understand affinities between consumer purchases, and to learn who their "best" customers are. For those companies that are collecting customer-specific information, consumers are identified individually, according to most respondents. Most retailers, who capture consumer-specific data, identify customers individually (84 percent). For 57 percent of survey respondents, individual customers are linked to POS transaction data for subsequent analysis. Retail winners are more aggressive, both in the capture of consumer-specific data at the point-of-sale as well as using customer payment information captured at the point-of-sale in subsequent transactions (*figures 1 & 2*).

Figure 1: Customer-specific Data Captured at POS



Retailers are aggressive in capturing consumer-specific data at the point-of-sale. Winners are even more so.

Figure 2: Use of Consumer-specific Payment Data



Winners are also more aggressive in re-using consumer-specific payment data in subsequent transactions.

However, although sensitivity appears to be increasing about the need to adequately ensure the privacy of customer information, this year's survey results indicate that adequate measures have yet to be taken by a majority of retailers. Although 67 percent of retailers have established a data security coordinator (up from 57 percent last year), only 53 percent have a formal incident response plan in place; 51 percent perform network penetration testing; 47 percent encrypt customer-specific information; 49 percent capture forensic data about how customer specific data is accessed, and only 28 percent fully comply with such data security standards as PCI.

With 14 percent of survey respondents indicating that they have suffered a customer data security breach, it is clear that there is a tremendous risk to retailers' brands from failure to act more proactively. Retailers, however, are concerned that proposed or pending regulations and standards will impact their businesses, and don't feel that trade associations are adequately representing retailer issues to state and federal regulators. And, retailers appear to be quite concerned about RFID's potential to become a privacy concern. The time is **now** for retailers to move from reactive to proactive mode on the important issue of ensuring the security and confidentiality of the customer-specific data that is being collected and used by the business.

SECTION III: OPPORTUNITIES

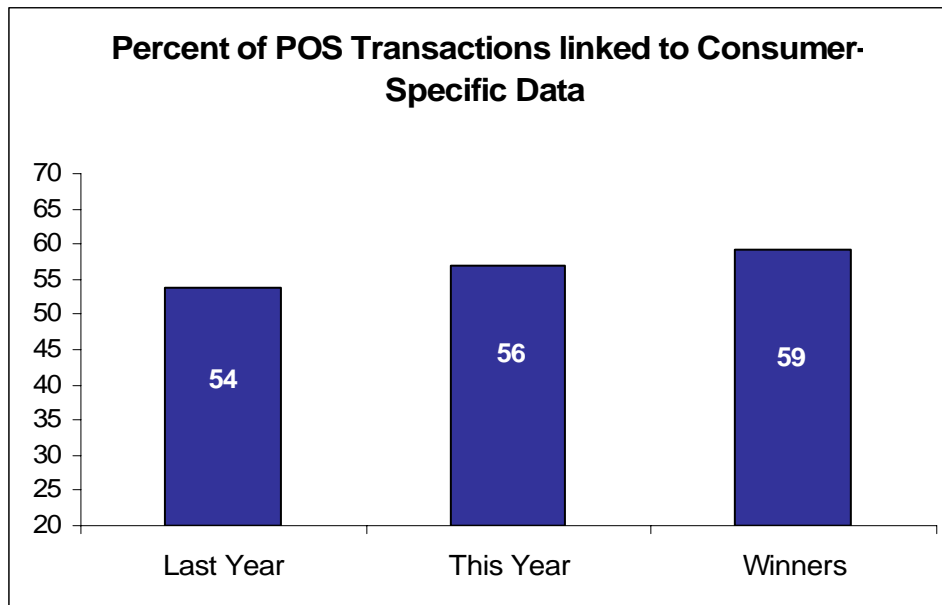
USING CONSUMER-SPECIFIC INFORMATION TO BETTER UNDERSTAND DEMAND - WHILE STILL ENSURING PRIVACY AND SECURITY

The goal of a customer centric merchandising strategy is to present a compelling value proposition in a way that is meaningful to individual consumers. It is clear that this sell-side strategy is on many retailers' minds as a way of competing with channel masters such as Wal-Mart and Home Depot, who excel on the buy-side of the business and pass savings along to customers in the form of competitive prices. Additionally, most retailers (84 percent) identify consumers as individuals within their databases.

Survey responses indicate that many retailers' merchandising strategies are increasingly driven by analytics that consider the Customer Data Dimension (in addition to established dimensions of Product, Location, and Time). Over one-half of the survey respondents link POS transactions to consumer-specific data to enable market basket analysis. As with the collection of consumer data at the point-of-sale, winners are more aggressive in this regard (*figure 3*). However, from the data, it also appears that over 20 percent of retailers who collect consumer data at the point-of-sale aren't linking item movement to customer profiles at this point.

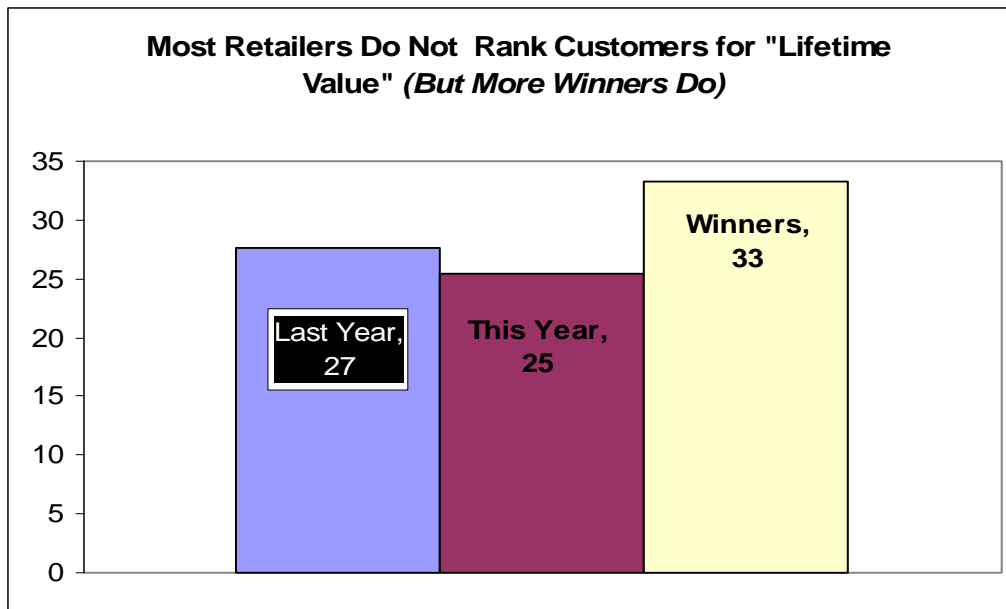
With items sales linked to customer profiles, retailers should be able to understand who their best customers are and how best to merchandise to them. However, it is clear from the data that most retailers are not doing so, even retail winners (*figure 4*).

Figure 3: POS Transactions Linked to Consumer-specific Data



Winners are more aggressive in linking transactions to consumer-specific data.

Figure 4: Retailers Who Rank Customers for Lifetime Value



Few retailers are using consumer-specific data to understand who their “best” customers are.

So why do retailers take on the difficult technical task of capturing and storing large amounts of consumer-specific data, let alone assume the business risk to the company’s brand if a security breach were to occur? The rationale is compelling. Even though most retailers do not use that data to create truly personalized value for individual consumers, they do consider it as an additional dimension to fine-tune traditional product-oriented merchandising strategies (i.e. use the customer dimension to tailor assortment, price, and/or promotions based on location sensitive market basket analyses). The customer dimension enables retailers to be more sensitive to true demand on a localized basis, and to develop merchandising plans accordingly (for example, Walnut Creek, CA and Newton, MA have similar demographics, but consumers in those cities may have very different buying preferences). For merchandise planning processes, some retailers now include not only buyers and financial analysts, but also statisticians, who can help buyers understand affinities between purchases by certain categories of customers.

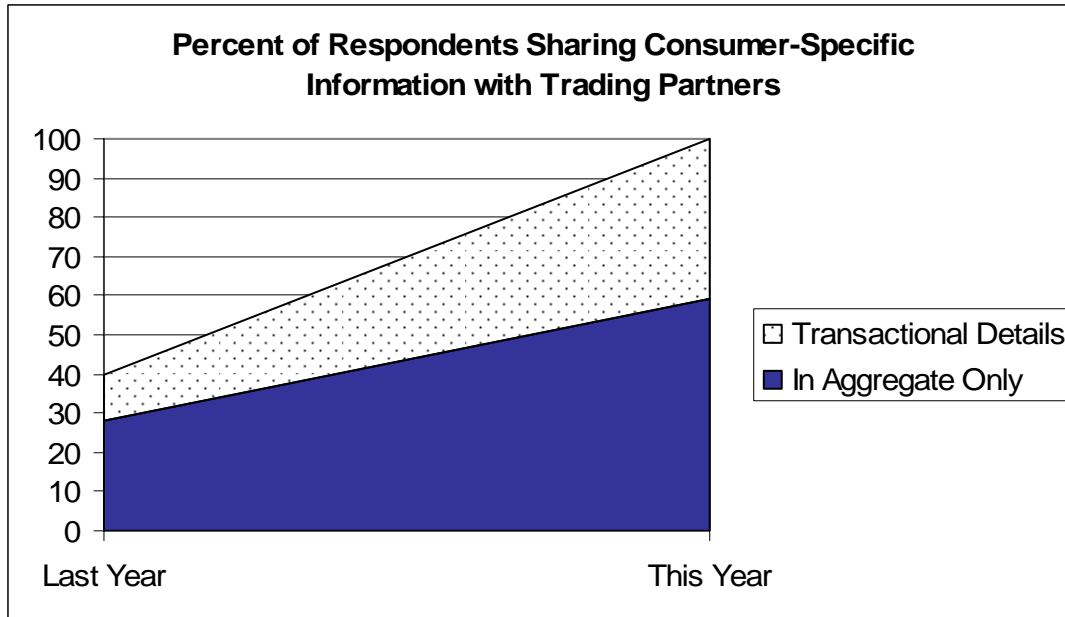
Given the highly sensitive nature of consumer-specific data, collecting and using that data is risky without proper organizational and technical precautions (as will be discussed in the next sections of this report). This may be one reason why retail winners tend to keep the data less than the overall response group. Whereas the most retailers keep consumer-specific data longer than 2 years (69.4 percent), 30.8 percent of retail winners report that they keep the data one year or less, compared to the overall response of 20.4 percent.

Risk of a breach apparently hasn’t slowed down retailers’ willingness to share consumer-specific data. In fact, that practice has increased since last year, and virtually all retailers share



the data with trading partners, either as aggregated data or detailed transaction information (figure 5).

Figure 5: Sharing Consumer-specific Data with Trading Partners



Virtually all retailers now share sensitive consumer-specific information with trading partners either in aggregate or in detail.

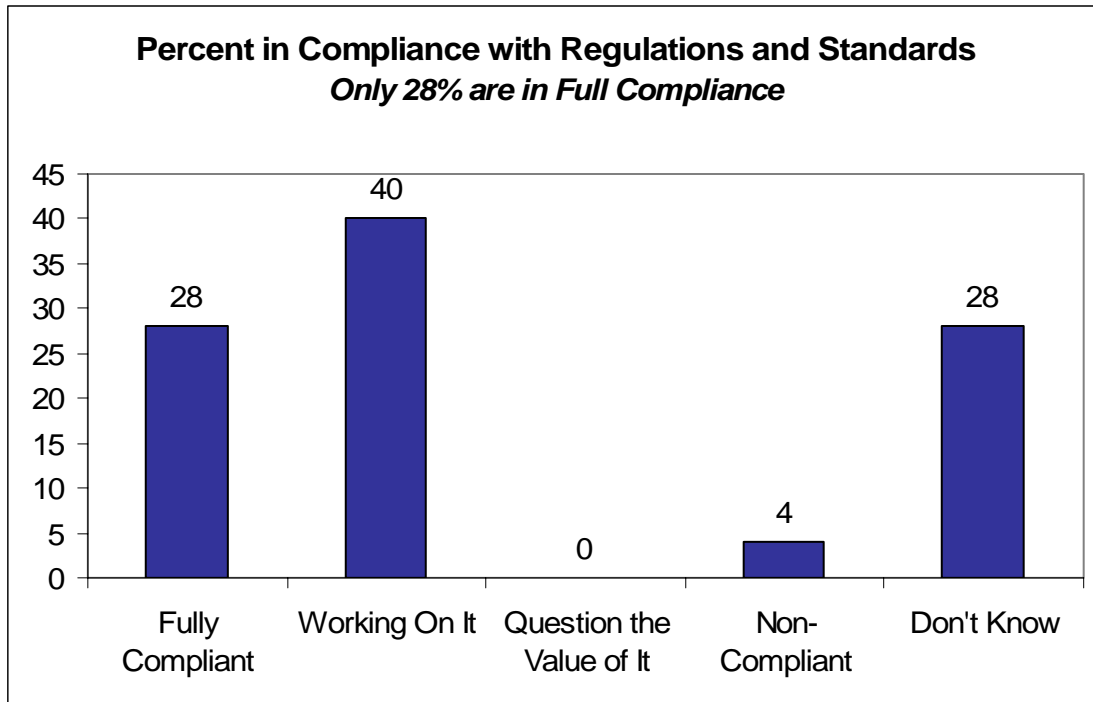
Recently publicized security breaches within the retail industry have shown that companies can suffer significant brand damage if/when breaches occur. On the other hand, companies have a tremendous opportunity to build loyalty if they successfully convey to customers that they are good custodians of consumer-specific data. It is surprising then that only 23.5 percent of survey respondents reported that their consumers have the opportunity to find out how data specific to them is being used.

SECTION IV: ORGANIZATIONAL BARRIERS

WHILE STEPS ARE BEING TAKEN TO ESTABLISH ORGANIZATIONAL ACCOUNTABILITY, RETAILERS ARE REACTING SLOWLY

For companies to avoid the nightmare of a public breach of customer privacy, organizational accountability must be established and supported by policies and processes that enforce compliance to standards and regulations. Many states in the U.S. have adopted rigid regulations about disclosure of consumer data security breaches, and financial networks such as VISA and MasterCard will impose harsh financial consequences if a breach occurs. Sixty-eight percent of survey respondents said they are either “fully compliant” or “working on it,” when it comes to standards and regulations such as the PCI standard (*figure 6*). But 78 percent of respondents indicated that they are either “highly concerned” or “concerned” that standards and proposed regulations will affect their businesses, indicating perhaps that many retailers view compliance as more of an interruption than an imperative. Retailers are also concerned that their views on the subject of *reasonable* standards and regulations may not be heard; only 26.5 percent of respondents think that retail trade associations are adequately representing retailer issues to state and Federal regulators.

Figure 6: Retailers’ Level of Compliance



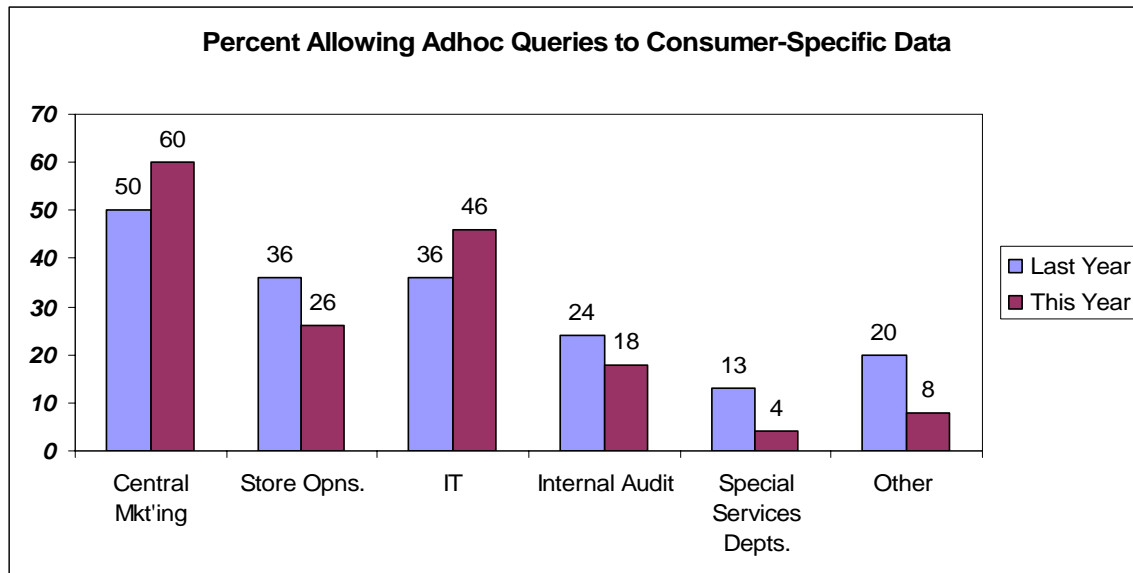
Retailers are moving begrudgingly towards compliance.

A full two-thirds (66.7 percent) of survey respondents have established a single security program coordinator to address internal and external risks to the security, confidentiality,



and integrity of consumer-specific data (up from 56.6 percent last year). However, in spite of that positive direction, unfettered access is still allowed to consumer-specific information in many cases, particularly by Central Marketing and IT personnel (*figure 7*). Adhoc queries create the potential for a security breach, especially in those cases where retailers are storing payment information for future use (47 percent, see *figure 2*). In fact, such practices could be a violation of the Payment Card Industry (PCI) Data Security Standard 7.2, which states that merchants must “Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know, and is set to ‘deny all’ unless specifically allowed.”¹ This issue takes on special importance when considering survey responses from retailers who have “knowingly been breached” (14 percent). Almost 30 percent of those respondents said that the threat came from internal staff. In spite of this, less than one-half of retailers (47 percent) have taken steps to train their employees about policies related to the confidentiality of consumer-specific data. This response is actually down from the *2005 Benchmark*, where 56.6 percent said that they provided training to employees.

Figure 7: Adhoc Queries to Consumer-specific Data



Despite its sensitivity, access consumer-specific data is not well controlled.

Adhoc queries aside, the frequency of control audits appears to be on the rise, compared to the *2005 Benchmark* results. Controls associated with consumer-specific information are audited on a scheduled basis “annually” or “more frequently” than annually by 30.6 percent of respondents, and “on demand” by 38.8 percent. Controls associated with information that is shared with business partners are audited “on demand” by 46.1 percent of retailers, and on a scheduled basis at least annually by 20.5 percent.

¹ Payment Card Industry Data Security Standard, Version 1.0 December 15, 2004, © 2004 Visa U.S.A. Inc.

The number of retailers who have developed a formal incident response plan has improved since the 2005 study. Although those that do not have such a plan continues to hover near 45 percent (43 percent compared to 45 percent last year), 52.9 percent of survey respondents said that they have a plan in place compared to 41 percent last year. And 65.8 percent of those that have a plan test it at least annually.

Not much has changed since last year's results as relates to change control for computer applications that use consumer-specific information; according to this year's benchmark, 47 percent certify changes to applications that access consumer-related information compared to 44.7 percent in 2005.



SECTION V: TECHNOLOGY ENABLERS

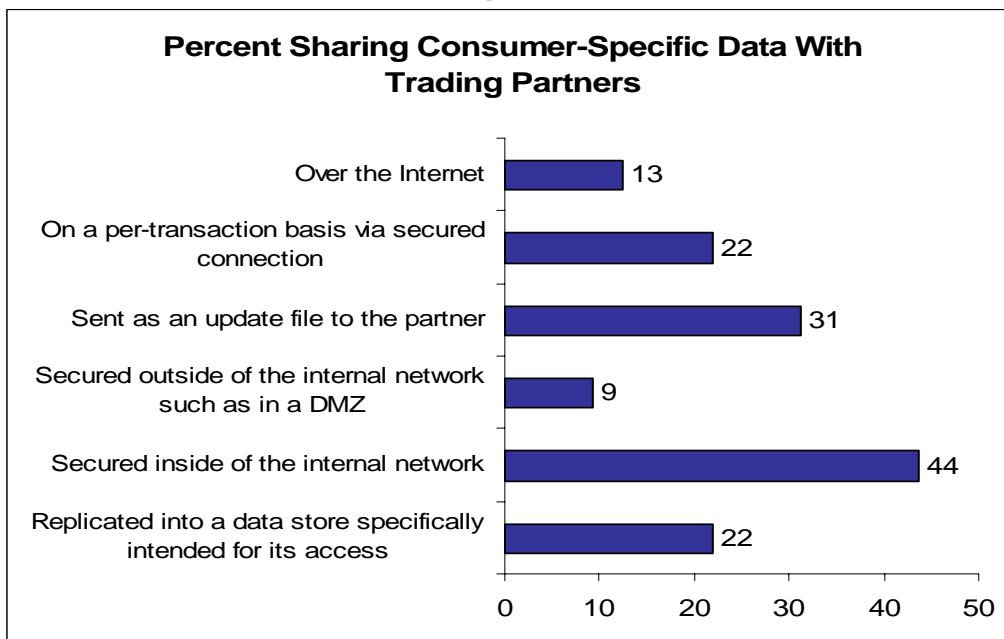
THE GOOD NEWS: TECHNOLOGIES WILL HELP MITIGATE RISK – IF THEY ARE USED

Although retailers are moving aggressively to use the Customer dimension to fine tune their merchandising strategies, they are moving much less aggressively to utilize the technologies available to them to mitigate risks associated with the use of that data. This is not for want of technology answers, however. Technologies such as data encryption, access logging and proactive forensic analysis, penetration testing tools and services, and other techniques are available now.

This year's study shows that 61 percent have established a central "customer master" database that can be accessed at the point-of-sale in "real time" (as opposed to older techniques, such as store-specific customer databases or centralized points databases). However, less than one-half (47 percent) of survey respondents indicated that they encrypt consumer-specific data. Most of those, 75 percent, encrypt the data within the database itself (the remainder encrypting it only as it goes through the VPN). This represents very little change from the 2005 study results, when 31 percent reported that they were encrypting the data within the database itself.

When it comes to sharing data with partners, retailers show no consistent pattern (*figure 8*). 53 percent of survey respondents send updates to their partners either on a per-transaction basis or as a batch file update; by so doing, these retailers potentially lose control of the security of that data, and must depend on their partners' capabilities.

Figure 8: How Data is Shared with Trading Partners



Many retailers send consumer-specific data updates to trading partners.

The number of retailers who enable secured access to their internal network has increased however, since the *2005 Benchmark*, when only 23 percent reported having provided secured access to the data.

According to the Payment Card Industry Data Security Standard²:

“Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.”

The percentage of retailers who are capturing and maintaining forensic data (source, destination, time stamps, ports etc.) has increased; Forty-nine percent now report that they do so, compared to 35.5 percent in last year’s study.

Finally, a number of proven solutions and services exist to test the penetrability of internal networks. Fifty-one percent of survey respondents indicate that they use penetration testing tools and services, and 86.7 percent report being satisfied with test results.

² © 2005 MasterCard International Incorporated
Payment Card Industry Data Security Standard • January 2005



SECTION VI: BOOTSTRAP RECOMMENDATIONS

DO IT NOW

Retailers today have the ability to use information captured from points-of-sale to be able to deliver compelling value to consumers, either as individuals or as members of communities. In many ways, this is a return to a pre-mass merchandising concept, before consumers began to be treated as an amalgam of many different demographics, lifestyles, and buying preferences. The difference today is that retailers can achieve a level of *intimacy* and still perform as a large scale enterprise. Information technology makes this possible, and winners are using information and technology to better understand customer preferences and to plan their merchandising strategies accordingly. However, such strategies do not come without risk. A climate of distrust exists; according to some studies, 90 percent of the American public care strongly about privacy, and most feel that they have lost control over the privacy of their personal information³. It is in this climate that retailers and their partners in the Extended Retail Industry are capturing and using consumer-specific data.

Based on the results of this 2nd *Annual Retail Data Security Benchmark 2006-2007*, we believe the evidence is clear: **Now** is the time to address the organizational and technical issues surrounding the effective use and security of consumer-specific information. Those companies that effectively use this information to drive customer value while at the same time ensuring its privacy and integrity, will be rewarded with increased customer loyalty and improved earnings. Failure to secure consumer-specific data will result in brand erosion and crippling scrutiny from regulatory agencies and financial networks.

“BOOTSTRAP” RECOMMENDATIONS

- Assign organizational responsibility, and support it from the top. The privacy of consumer-specific data is a boardroom concern, not merely an IT governance issue. Failure to ensure the privacy of customers’ data creates tremendous fiduciary risks.
- Retailers must develop a technical and process roadmap for compliance to industry standards, particularly the PCI DSS standard (www.visa.com).
- Keep only that data which is necessary to meet operational objectives, and only as long as necessary. Follow the standards in regards to what data should and should not be kept.
- Convey your commitment to consumer privacy to your customers via every channel (stores, Internet, catalog).
- Train your employees about the company’s policies with regards to consumer privacy.

³ Robert Belair, Current Trends and Policies in Consumer Data Security, 11/2005, RSAG Retail Data Security Forum

- Develop a security breach response plan that includes communicating to the appropriate regulatory and law enforcement agencies, financial networks, and to consumers themselves.
- Seek active partnerships with solutions companies such as network technology providers to understand and implement best practices.



REPORT SPONSORS

.....

ABOUT CISCO SYSTEMS

The Cisco Intelligent Retail Network is a secure platform for retailers to build upon in order to improve the customer experience and strengthen retailers' competitive advantage. The Cisco Intelligent Retail Network allows retailers to comply with payment card industry requirement, simplify business operations, improve supply-chain visibility, and accelerate decision making through the convergence of data, voice, video, and mobile communications. To learn more, visit www.cisco.com/go/retail.



.....

ABOUT RETAIL SYSTEMS ALERT GROUP

Retail Systems Alert Group is the leading provider of objective, high-quality information resources for the Extended Retail Industry (ERI). We have followed the advancements of technology and business process innovation in this industry for almost two decades, and we deliver our insights and analysis through high-value conferences and tradeshows, publications, research, training, and Web-based services.

For more information, visit www.retailsystems.com

Retail Systems Alert Group services the Extended Retail Industry (ERI). This term, coined by Retail Systems Alert Group, describes a broader consumer-focused ecosystem encompassing retail, manufacturing, transportation, distribution, logistics, warehousing, solution providers, and other supporting organizations.



.....