

---

# *Protecting the Enterprise's Information*



## *Centralized Security Report 2007*

WRITTEN BY  
STEVE ROWEN  
RESEARCH ANALYST



SPONSORED BY



# Table of Contents

Executive Summary .....	i
“Bootstrap” Recommendations – A Board Room Discussion .....	i
SECTION I: Overview .....	2
Why The Study Was Conducted .....	2
Defining Retail Winners .....	2
The Business Challenge .....	2
Opportunities .....	4
Organizational Inhibitors .....	4
Technology Enablers .....	5
Case Study Characteristics .....	5
Case Study 1 – Restaurant Retailer .....	6
Business Challenges .....	6
Opportunities .....	7
Making Lemonade of Lemons .....	7
In the Court of Public Opinion .....	7
Organizational Inhibitors .....	8
Separating Hype from Value .....	8
Technology Enablers And Lessons Learned .....	9
PCI: A Heavier Load Than SOX .....	9
CASE Study 2 – General Merchandise RETailer .....	11
Business Challenges .....	11
Opportunities .....	12
Reputations on the Line .....	12
Organizational Inhibitors .....	12
Exemplifying the Pain of Non-Compliance .....	12
Technology Enablers And Lessons Learned .....	13
No Time to Spare .....	13
CASE Study 3 – Specialty Apparel Retailer .....	14
Business Challenges .....	14
Opportunities .....	15
Keep Your Brand Out of The News .....	15
Organizational Inhibitors .....	15
Buy-in Is Everything .....	15
Technology Enablers And Lessons Learned .....	16
Keep Asking Questions .....	16
Appendix A: RSAG’s BOOT Methodology .....	18
Report Sponsor .....	19
ABOUT THE SPONSOR .....	19
ABOUT THE PUBLISHER .....	20

# Figures

Figure 1: Retailers Increasingly Capture Customer-specific Data .....	3
Figure 2: ...And Link Sales Transactions to Those Customers.....	3
Figure 3: Merchants Having Trouble with Their Twelve-Step Programs .....	6



## EXECUTIVE SUMMARY

The Payment Card Industry's DSS (Data Security Standards) regulations are a comprehensive set of mandatory regulations that all merchants must heed, to claim compliance. By design, these regulations force retailers to protect the customer's trusted information. And while this 12-step standard is thorough, leaving little room for interpretative or scalable deviation, getting to compliance has become one of the most challenging – and expensive – endeavors retailers face today. Retailers are still well behind in their efforts to protect themselves – and their customers.

Last year, the Payment Card Industry predicted that by the advent of 2007 more than two-thirds of Level 1 merchants (those processing more than 6 million credit/debit card transactions annually) would be fully PCI compliant. **This simply hasn't happened.** While our quantitative benchmark research puts the level of fully compliant retailers at only 28 percent (regardless of transaction level), there is new reason to believe that even these numbers are overstated. PCI compliance is currently overwhelming retailers seeking to leverage value from customer-specific data. However, retail winners are discovering ways to overcome the difficult and time consuming compliance challenge at the enterprise level. And while their individual needs and methodologies may vary, they share common experiences from which all retailers can learn.

**Most importantly, winners have successfully educated C-level executives and made them data security proponents.** This is no small feat, as compliance brings little apparent ROI and steep implementation costs. However, as evidenced by the experts in this report, by clearly demonstrating the risk retailers take in NOT taking these steps, a seemingly IT-driven presentation to the Board of Directors can still hit home. *This ability to transform data security into a Board Room issue is a baseline requirement for any successful overhaul of existing practices.*

Another key differentiator in these winning retailers' approach is the ability to “bundle” the benefit of secure technologies into legacy technologies already in need of update. Migrating from risk-prone to more responsible data handling practices is in no way a turn-key event. On the contrary, many of the practices that are in most need of overhaul rely far less on technology than they do on training, and present a prime opportunity to bring about significant organizational change for the betterment of the enterprise as a whole.

Winning retailers' can clearly articulate the risks inherent in a future of non-compliance – **the expense far outweighs that of proactive investment. Non-compliance and the threats it brings can damage a retailer's brand, almost irrevocably.**

## “BOOTSTRAP” RECOMMENDATIONS – A BOARD ROOM DISCUSSION

Our first and most important recommendation is to elevate the conversation. *Insist on Board Room Visibility.* Non-compliance represents not only significant fiduciary risk, but also threatens the company's *Brand* value to its customers. These issues directly affect shareholder value. *Winners* insist that regular progress reports are given to the Board of Directors, often as part of the efforts of the Audit sub-committee of the Board. Once this is attained, only then can an organization go on to follow these recommendations:

*Know where your data is.* This includes any type of information that the Payment Card Industry has defined as cardholder and sensitive authentication data, as well as customer and associate data that is commonly viewed as trusted information. The siloed nature of most retailers is bound to create shock and awe at the omnipresence of this valued resource once evaluated.

*Keep only the data you need.* This is an area in which retailers have become sinfully negligent. When pertaining to customer data, keep only that data which is absolutely necessary to complete a transaction/return. For employee and associate data, further stringent controls are required than most currently use.

*Enact strict guidelines for data access.* The key to securing data practices resides not only in the training of associates and outside trading partners of a predetermined access and usage policy, but also in corresponding accountability and clearly defined repercussions for any violation.

*Foster an understanding that PCI DSS Standards compliance is part of a larger set of issues.* Companies are bound by related laws and regulations such as Sarbanes-Oxley and HIPAA, as well as industry standards like PCI DSS. *Winners* recommend an integrated approach.

# SECTION I: OVERVIEW

## WHY THE STUDY WAS CONDUCTED

The goal of RSAG’s Retail Data Security series is to both gain a comprehensive understanding of the state of data security in retail AND provide valuable information for those yet to act. We seek to educate by way of example – by understanding what winning retailers are doing to secure their customer information from harm.

In this report, we set out to determine what’s working for winning retailers at the enterprise level.

## DEFINING RETAIL WINNERS

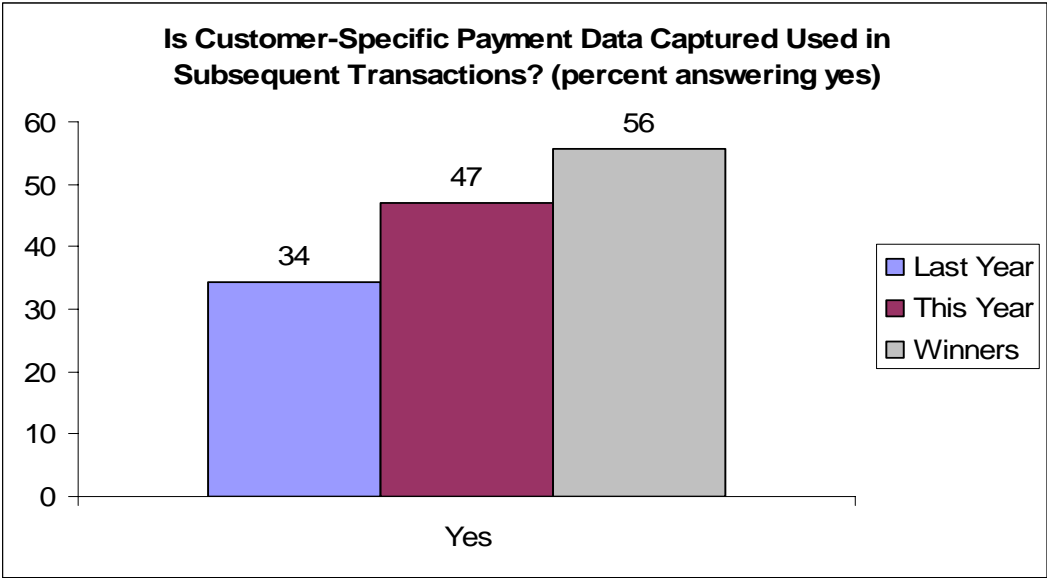
Our definition of retail winners is straightforward. We choose to follow Wall Street. Wall Street judges retailers by year-over-year comparable store sales improvements, and RSAG does the same. Assuming industry average comparable store sales growth of three percent, we define retailers with sales above this hurdle as “winners.”

Yet for the purposes of this report, we additionally require winners to be in the advanced stages of pursuit to comply with the Payment Card Industry’s Data Security Standard. Compliance to this mandate is the most clear-cut measure of a retailer’s commitment to protect its brand, its operations, and its customers.

## THE BUSINESS CHALLENGE

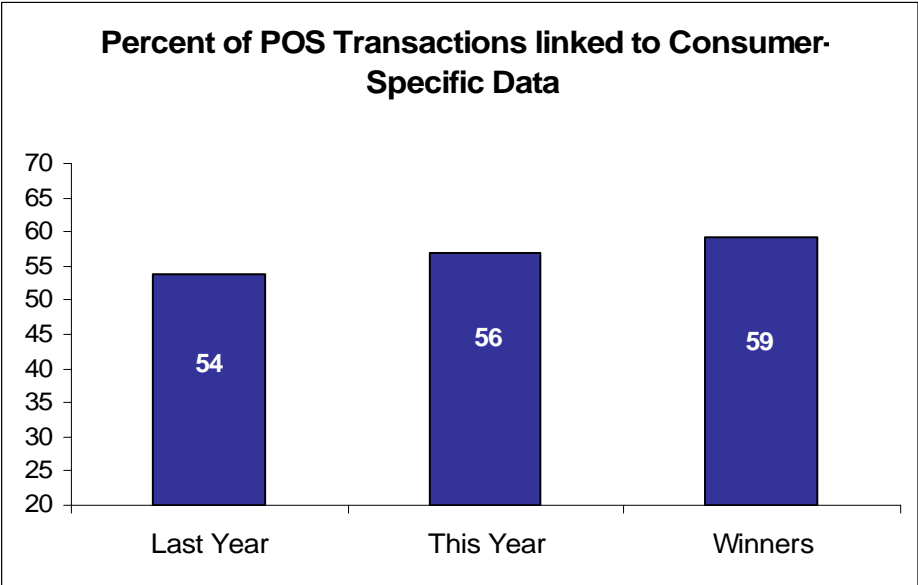
For years, retailers have taken the opportunity to gain “strategic customer intelligence” as a direct result of the consumer’s tendency to carry less cash. The detailed data captured through cashless transactions has steadily been used with more frequency by retailers – most clearly exemplified in the facts that increasing numbers of retailers use this data for subsequent marketing and merchandising purposes (Figure 1) and then link that data to identify the customer (Figure 2). This has caused issues with privacy advocates like CASPIAN. It also has created security issues for retailers, who once cared about security only as it relates to nightly cash deposits. Additional fallout can be viewed all too frequently on the nightly news as the treasures within data repositories have become more attractive to criminals than were poorly guarded bank vaults of old.

Figure 1:  
*Retailers Increasingly Capture Customer-specific Data*



For retailers, the real challenge at hand is playing a very expensive game of catch-up. In our ROI focused age, most are having a difficult time rationalizing major investments to secure the data and processes they already use.

Figure 2:  
*...And Link Sales Transactions to Those Customers*



In addition, while emerging privacy and security technologies consistently become stronger, the cost of re-training employees is sizeable. While associates in the merchandising department may believe that an ad-hoc query of customer data resulting in a spreadsheet downloaded to their laptop will be leveraged to benefit the company, they rarely think of the implications if their laptops are hacked when next used at a wireless café or stolen at the next major retail conference. Strict corporate access controls must accompany the growing number of devices being granted to today's retail workforce – particularly those that are portable.

## OPPORTUNITIES

Unlike physical security, data security holds little opportunity to generate immediate ROI metrics. For example, a risk-prone network will have few “before and after” analytics showing reduction in shrink the way a solution such as Digital Video Surveillance would.

However, winning retailers view the prospect of becoming PCI compliant as a tremendous opportunity for their business to genuinely thrive. Though the standard is often seen as unwelcome, it forces retailers to enact good business practices. These practices, in turn will give them the ability to operate with more security and confidence, proactively avoid brand damage and loss of customers due to a security breach, bringing about operational change that benefits all aspects of the business.

One of the most clear-cut supporting factors of this notion is echoed by each of the winning retailers we spoke with. Each discovered horrifying realities when first diving deeply into their existing data practices. Not only were controls unregulated, disparate, and disorganized, but the very location of data silos and usage throughout the corporation was actually counter-productive to profitable practice. By accepting this reality and working to get past it, the culture of the organization has become more regulated, productive, and profitable.

But the most defined opportunity that enterprise-level data security technology and process affords is, for better or worse, to **significantly reduce or eliminate the cost of non-compliance**. As evidenced in our benchmark numbers, the majority of retailers still do not view non-compliance as a serious threat to their business model. The cautionary words of our final case study interviewee should serve as a wake-up call for those laggards.

## ORGANIZATIONAL INHIBITORS

A lack of immediate ROI continues to be the strongest inhibitor of retailers enacting stronger data security practices.

Cultural resistance to change should no longer remain a dominant factor, as winning retailers are laying out the framework for successful co-ordination of internal support driven by the organization's highest levels. Though time and research intensive, educating the executive level of the organization to the guaranteed cost of continued negligence is a highly successful model, aiding to set proactive thought leadership in motion. The number of high profile disasters continues to rise. A laundry list of the financial and public relations fiascos is a splash of cold water on any senior executive.

## TECHNOLOGY ENABLERS

Regardless of your organization’s viewpoint of the Payment Card Industry’s Data Security Standard, it has proven to be a mandate that is bringing about change in an otherwise stagnant area of an already slow-moving industry. Those who have started working toward compliance already see the value in the networking, encryption, and organization infrastructure requirements it has brought about.

For those slow to act, technology providers are continually offering a host of solutions at friendlier price points targeted at smaller merchants with limited budgets. Meanwhile, winning retailers insist that a pre-established knowledge base of what an organization needs most will aid greatly in all stages – and cost – of working toward compliance.

However, a word of warning from our *Winners*: there is no magical “one” solution that brings a company into compliance. Since most retailers have a mix of legacy and package applications in their application portfolio spanning many technology “generations”, each exchange of sensitive data between applications and technologies must be examined for compliance. This starts with the origin of much of the sensitive data – the store-level Point of Sale system, which is often the oldest and most proprietary application in a company’s portfolio.

## CASE STUDY CHARACTERISTICS

RSAG conducted interviews with three retailers between February and March of 2007. All are retail “winners,” and operate a well known brand on a domestic level. In the interest of providing quality information that may be sensitive in nature, each will remain anonymous throughout this report.

# CASE STUDY 1 – RESTAURANT RETAILER

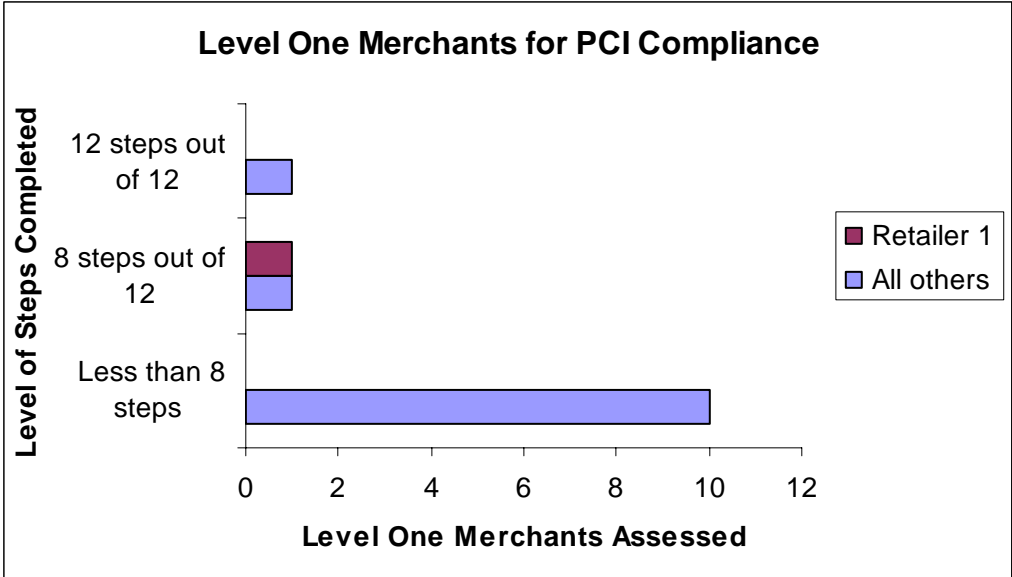
The first case study is a US-based restaurant chain. The company operates at the Level 1 merchant base, conducting more than 6 million cashless transactions a year, and is currently in the process of migrating from a legacy SCO/Unix environment to a Wintel platform.

## BUSINESS CHALLENGES

*When asked about its level of compliance with the Payment Card Industry’s Data Security Standard, “We’re currently compliant with eight of the 12 high-level standards. We’re diligently working toward the other four, but are not committing to anything prior to December 31<sup>st</sup>, 2008.”*

Also of note, the retailer has recently asked to be benchmarked against its peers (Figure 2). “We’ve asked our assessment company to rate us against 12 other Level 1 merchants, and we rate at eight of the 12 required for high level compliance. Of the remaining 12 retailers assessed, all of which are comparable merchants, only one was fully compliant, and only one other was as high as we are. And these are all Level 1 card-present merchants.”

*Figure 3:  
Merchants Having Trouble with Their Twelve-Step Programs*



*When asked about its data response team, retailer one states, “We have the plan and the individuals identified, the communications plan built as well as contacts established, both at the US Secret Service as well as a certified forensic analysis team. We actually have pre-paid hours with forensic analysis, which is nice to have.”*

The retailer also indicated that it has an appointed a **Chief Information Security Officer**, who reports directly to the CIO. **Both of these individuals are responsible for presenting data security and risk management issues to the Board of Directors.**

*When asked about the organization’s awareness of device connectivity (and the ensuing ability to keep track of how many sessions are open, and which computers are attempting which tasks),* the retailer quickly points to its lack of a centralized point of aggregation for all transactions. “We resolve every transaction directly from the store to the acquiring bank. This has some pros to it, but making changes becomes more difficult.”

*When asked about its methodology for user/password procedures,* the retailer states, “We have an established proposed process for the new environment we’re rolling out, and that’s one of the areas we’re working on. It’s going to be **a unique user and password per session**, which will be spawned as needed, eliminating administrative accounts in the local boxes. And we have a centralized management console that will produce that account on the needed system on-demand, and then destroy that account once it is no longer needed. No one has the root password, and we have two levels of administrator access – one runs scripts while the other can actually perform maintenance on the system.

“We’ve changed the password on an every-30-day basis. We have an algorithm that runs in the background that changes to a pre-known password, but we’re not even able to generate those until the month preceding when those will be accessed. They’re based on store crew or store manager, then there’s help-desk and above (administrator). The end-user access is created within the application.”

“If I’m a store manager, I know my own password to get into the application; I know no password to get further into the system. Each user of the application has a unique password. Store-level operations people only have an application-level password. They are presented with a user interface and can’t get to the OS.”

## **OPPORTUNITIES**

### **Making Lemonade of Lemons**

*When asked about immediate opportunities beyond PCI compliance from strengthening the network,* the retailer says, “Prior to cashless transactions our stores were disconnected islands with no internet connectivity, no real risk from an IT perspective [recent upgrades have changed that scenario]. So in general, it’s a good thing for us – we don’t point at PCI and say their making us do this, it’s given us great leverage to bring about real change.”

### **In the Court of Public Opinion**

*When asked how the investment in more secure customer data can be leveraged to create competitive advantage, win new customers, or convey a message of loyalty to the consumer,* the retailer explains, “The end user doesn’t know anything about PCI compliance – nor do they care. We frown on companies that tout their level of security as a method to gain new customers. A case in point, one of our competitors recently issued a statement of a date when all of its stores will

be PCI compliant, and that's just an invitation to a hacker. **The moment you start bragging about your security is the moment you've laid down the gauntlet for criminals to come and prove you wrong.**"

He continues, "The public is certainly getting inundated with [information about] breaches – and if you haven't had to cancel a credit card as the result of a breach yet, you're in the minority. Most people have either gone through this or had someone close to them go through it. I've had to go through it twice now. And I think in the end the consumer tends to blame the criminal more than the merchant."

*When asked about the opportunity to reduce risk (which is fundamentally a cost),* he explains, "We're redesigning our entire network at the store level to support PCI. The proposal we have right now is indeed expensive, but comes as a one time fee. Our other option, to make every network in our system of stores compliant would have cost \$500 million over a 10 year span. So from a protection of data classification, confidential or business-critical data simply has to have these controls. And that's really a good thing."

He continues, "There are a few components of trust in the customer relationship. For us, the first is a food safety issue, but the other is one the customer doesn't even realize they've given to us - and that is trust with their financial instrument."

"If we had food that became a safety issue, it would happen immediately, hit the news, and would create a brand issue. But if we had a financial issue it would generate even more damage from a brand perspective. And though that seems contradictory to the news of promoting security as a method to gain customers – what we're doing is preventative, not grandstanding. Because when financial damage hits the media it lasts for quite some time, and is reflected in stock prices."

He adds, "If anything were to happen to us, we believe it would be a skimming incident at a remote location. Since we don't centrally aggregate any data, the likelihood of us having a mass breach is not very high. And because we don't store any of that data, resolving whose data was lost would be nearly impossible. We don't even have the data to mail out the informative letter to the customer, but by the same token, we don't even have that data to be stolen. It's a better model because we're not using data to identify the customer. It's safer."

## ORGANIZATIONAL INHIBITORS

### Separating Hype from Value

*When asked what (technology, culture) keeps the organization from implementing stronger security of internal data-handling procedures/systems,* the retailer points to technology first. "Take IKEA's wireless linebusting technology. As security professionals, we see this in the news, and our management is seeing it too. As a result of this type of media buzz, projects get built, and are 90 percent completed just before rollout and only then are we asked about the solution from a security prospective. As much as that technology helps you get to your customers faster, the risks are just too high for us – we'd never accept that level of risk."

“With PCI, which has been the driving force behind our network redesign, we have to evaluate the existing technologies based on their risk. We need to get our business processes away from the cash flow. We can continue to do business and bring in devices that may not have to be as secure as cashless data, because it’s really expensive to secure that data”

*When asked about internal buy-in*, retailer one says, “We had our ‘come-to-Jesus’ moment over a month ago. It was a long time coming, but getting the right message to the right ears was really worth it. We had a meeting with the CISO, the director of technology assurance, a senior VP and two of his direct reports with regards to security in-store. Our goal was simply to educate about the existing problem. We held a full-day PCI workshop with application developers, the treasury department and walked through the standard. We also armed ourselves with some great data from our assessor, and explained the risk from a company perspective outlining risk, and who, based on connectivity, is most likely to be hacked. Then we showed the current network diagram, and explained what we now have to secure. Little red lights went off in everyone’s head, and after that awakening moment, we’ve seen things roll very quickly – once that whole issue was properly conveyed to management.”

*When asked about the best way to sensitize the Board of Directors to the issue*, he explains, “The Board of Directors presentation from a security perspective was 60 percent devoted to PCI compliance. We have an annual meeting for the board, but at last year’s our CFO and CIO acknowledged that PCI compliance was the greatest risk that technology posed to our business – above and beyond SOX.”

## TECHNOLOGY ENABLERS AND LESSONS LEARNED

### PCI: A Heavier Load Than SOX

*When asked about the extra pains endured to protect itself while operating a hacker-prone OS*, the retailer points to penetration testing. “We have to harden the OS, and are diligent about full penetration testing by a third party to evaluate the system level security prior to rolling out. We’re also very diligent about patching and we do a full re-test at any system-level change of the system. We invite the penetration tester to sit at the console, give him full access to the box and say ‘You’re in a store, you’re an employee, get to the cashless session. Get to my cashless data.’ If they can’t, only then do we sign off on it.”

The retailer adds, “We’re being very aggressive, and this is not an easy process. We have to add another cable to every register, we have to add a router to every store, and we have to manage those configurations. Theoretically we’re disconnecting the pin-pad from the register. As a result, data would have to route over the network, and the credit card number would never be seen by the POS [system].”

*When asked about impending legislation (ala SOX 404)*, he states, “SOX has been easier to comply with than has PCI, due entirely to one fundamental difference. SOX says you must

have a control in place, and then leaves it to the company to decide with an independent auditor what the appropriate control is.

“Yet PCI says you must do this – regardless of the scope of your environment, how much data you have: whether or not it’s encrypted, you have to do everything. There is no margin for fudge factor. And the compensating controls that are allowed today are subject to be held returned in following years. It’s a much more rigorous scrutiny that occurs. Granted, SOX goes further into the corporation and can be more challenging from a scope perspective, but from the level of granularity and complexity – PCI’s much tougher.”

*When asked which technologies are the most mature at this point for operating a secure data infrastructure,* he states, “People have focused more on the gateway traditionally, and I agree that that is number one – you have to have good gateway security – and historically security administrators have considered the internal network as a secure and trusted network. But with the portability of devices right now, establishing VPNs and the connectivity between companies, you really have to treat it as a hostile environment. And that means you have to be proactive about endpoint security as well. Either you have rigorous intrusion prevention mechanisms at the gateway or you must secure every endpoint as if it were on the open network.”

*When asked to provide recommendations for others,* he advocates, “The message I would give to anybody is to get your cashless data on a separate network, and don’t put anything else on it. Communicate only outbound on the necessary ports – it will make life so much easier. It’s one of those tough pills to swallow initially, but in the long term it is really much easier to manage.”

*When asked about pitfalls to avoid,* the retailer warns, “Don’t store data, segment your cashless data, and secure your endpoints – don’t ignore them. And that’s terribly difficult in retail. In an office building where you’ve got an IT staff it is easy. But you don’t have IT in your stores to fix things, manually install patches – it’s very difficult.”

## CASE STUDY 2 – GENERAL MERCHANDISE RETAILER

The second case study was conducted with a membership general merchandise chain. The company also operates at the Level 1, and is aggressively pursuing its goal of complying to the PCI's Data Security Standard.

### BUSINESS CHALLENGES

*When asked about its level of PCI compliance,* retailer two states, “We anticipate being compliant by the end of September, 2007. We’ve been through various iterations of assessment at this point, and would currently gauge our progress as 70 percent complete. Of course there is no static endpoint, as this will forever be an ongoing process.

*When asked which components have been most difficult,* he explains, “Single sign-on has been something we’ve identified as a long-term goal. I can recall conversations within our organization 15 years ago when we were discussing its advantages, but it’s been a very difficult functionality to attain. It is not easy.”

The retailer also points to the processes of data encryption and decryption as significant challenges. “We likely have allotted the most resources to our network. It was previously very flat, so it’s taken quite a bit to get the network to where we wanted it to be. Encryption/decryption has been a huge component of that issue, as the POS data flowing upstream onto the network was a real challenge, as well.”

*When asked about its data response team,* the retailer says, “This is something that we’ve already completed. We’ve always had a crisis communication plan in place via our Emergency Response Team, so our response team as it relates to the requirement of PCI compliance was easily attainable just by tweaking one little component of that structure. The plan completely spells out how to inform law enforcement, the consumers, and the press.

*When asked who is responsible for educating the Board,* he explains, “Our data security team has not met with the Board of Directors in quite some time. We regularly meet with senior leadership team to provide this information, and our CFO provides routine updates from the security team to the Board.”

The retailer continues, “Our audit subcommittee also is responsible for educating the Board to risk management and fiduciary risk, as this is an issue that they are highly sensitized to. As a result, we are also currently scheduling a near-term briefing to the Board by the data security team, itself. There is no such thing as too much education in this matter.”

*When asked about its methodology for user/password procedures,* he states, “This is another thing we’ve already completed. We can monitor and record every password reset that occurs. And we have role-based access established for our entire retail user-base. Every associate must

create a profile, is given a unique ID to logon, and must reset a new password every 90 days.”

## OPPORTUNITIES

### Reputations on the Line

*When asked about immediate opportunities beyond PCI compliance from strengthening the network, the retailer says, “It’s really all about protecting customer information. This is the thing that keeps us up at night, making sure that we’re doing all we can, because for our particular model in today’s marketplace, it is prerequisite to staying in business. Making sure that the customer’s personal data is kept confidential is the basis for our entire reputation.”*

*When asked how the investment in more secure customer data can be leveraged to create competitive advantage, win new customers, or convey a message of loyalty to the consumer, the retailer echoes the sentiment of our first case study interviewee. “This is really a zero-sum game. Of course it serves well to make known your privacy policy, and the logos of those vendors who are helping you achieve your goals can be prominently displayed online and in catalogs, but the only real incentives given are provided by VISA to such organizations as banks and clearing houses.”*

The retailer also goes on to state that its customers are highly privacy and security sensitive. “Our customers are very concerned, highly interactive, and actually police these matters for us. They are most certainly engaged.”

*When asked about the opportunity to reduce risk (which is fundamentally a cost), he explains, “We actually were just having this conversation internally the other day. Though everything that we’re working toward is preventative in nature, prevention really is cost-savings. Though it is often a difficult challenge to prove that point, we simply cannot slow our beating of this drum.”*

## ORGANIZATIONAL INHIBITORS

### Exemplifying the Pain of Non-Compliance

*When asked what keeps the organization from implementing stronger security of internal data-handling procedures/systems, he explains, “Corporate culture is the primary inhibitor. From a technology standpoint, I’d be remiss to not point out that the Windows format is a weak point. With such an operating system, we’re really enacting perimeter based controls, not so much protecting data as we are preventing access to it.*

“But again, the largest inhibitor is changing existing views and practices based on culture. It is imperative to start small when trying to alert the internal staff if you’ve not experienced a data-breach incident. What PCI has really done is exemplify the reality of fiduciary pain of non-compliance. It’s awoken so many executives, particularly in Tier 1 organizations, who consequently now want to boil the ocean. And while security was previously viewed as a bottle neck of naysayers, now we see that it is increasingly important to have the entire

organization realizing that security is everyone's job in order to protect our customers and their experience. This is a process, and it takes a long time."

## TECHNOLOGY ENABLERS AND LESSONS LEARNED

### No Time to Spare

*When asked to provide recommendations for other, retailer two advocates, "Patience is such a key component of a successful PCI Compliance initiative. Any attempt to hurry this process or take on too many components at one time will surely lead to failure. Our recommendation is to map out each of the mandate's steps individually, set realistic goals, and act accordingly within your staff's feasible bandwidth."*

*When asked about pitfalls to avoid, the retailer immediately points to the need to act now. "We feel as though we waited a bit too long to begin acting on this initiative, which has made the journey far more difficult as a result. Granted, we're almost there, but had we started a year and half earlier we'd most definitely have spent less money, experienced fewer frustrations, and had incurred much less of an overall struggle. I can't stress strongly enough how important is to act now."*

## CASE STUDY 3 – SPECIALTY APPAREL RETAILER

The final case study was conducted with another Level 1 merchant; a specialty apparel chain. What makes this study most interesting is the experiential vantage point the retailer is able to speak from, having been the victim of a major data breach itself.

### BUSINESS CHALLENGES

*When asked about its level of PCI compliance*, retailer three explains, “We are not 100 percent compliant, but I’d say we’re about 80 percent there. As a result of our particular situation, we actually have 177 requirements. The POS processing and the store systems are completely different. For 15 percent of the remaining needs we’ll be using Visa-sanctioned compensating controls, and the final five percent are projects that are in the works that simply have not yet been completed due to their technical complexity. We have a deadline of being completely compliant, including the compensating controls by August of 2007.”

*When asked which components have been most difficult*, “From a business perspective, justifying the multi-million dollar costs has been the most difficult aspect – the costs of hardware, resources, and people, none of which is generating one penny to our retail profit.”

The retailer also echoes the words of our first case study interviewee. “This entire process has been more difficult to undergo than was SOX 404. From a technical standpoint, encryption has definitely been the hardest component. If we operated one central database, the task would have been much simpler. But we’re a very siloed company, and as a result, figuring out the encryption handshake has been, by far, the most difficult aspect.”

*When asked about its data response team*, the retailer conveys, “Due to our specific situation, every aspect required of a response team is intact. There is a certain order that all of the notification requirements must be met, and not everyone needs to be notified immediately. The very first person to be notified is the executive committee, followed directly by the forensic attorney.”

*When asked who is responsible for educating the Board*, she explains, “We have an Information Security Officer who reports to the CIO who in turn, reports to the CTO. It is the CTO’s direct responsibility to report to the Board of Directors, and provides periodic updates every month to the audit committee (comprised of members of the Board of Directors).”

*When asked about its methodology for user/password procedures*, she says, “This is another area we’re currently working on. One of the misfortunes of a company caught in a breach situation is that everything becomes a number one priority. Everything must be done as quickly as possible, and you simply can’t boil the ocean. We can know who’s doing what on certain cardholder systems but at the present time, not all of them.

“Presently, we have a really good handle on our POS system, and that’s the one that generates the most risky data.”

The retailer adds, “Because of Sarbanes, we’ve done a really good job on dramatically reducing the number of people with root passwords. We don’t have single sign-on

application, so our root issues are with people that haven't been with the company for five or six years. Their company logon will be disabled as soon as they leave the company, so they'd never be able to access the system. We're working toward a single sign-on that gets updated every week."

## OPPORTUNITIES

### Keep Your Brand Out of The News

*When asked about immediate opportunities beyond PCI compliance from strengthening the network,* retailer three states, "PCI compliance is just part of the overall compliance obligation of an organization. If a company can be PCI compliant, it means they have a very good set of IT controls. If you're publicly traded, it definitely aids with Sarbanes Oxley auditing, as well as HIPPA. PCI compliance essentially really forces a very unregulated industry to straighten up."

*When asked how the investment in more secure customer data can be leveraged to create competitive advantage, win new customers, or convey a message of loyalty to the consumer,* she explains, "I think today's customers are very aware. The best way to have customer loyalty is for them to never ever hear your name on the news. It's kind of ironic, since there is no safer place to shop than a retailer who has incurred a breach, as such a retailer is forced to have some of the best retail systems in place. But to prevent a breach from happening is a far better model for your organization, your brand, and your customers."

*When asked about the opportunity to reduce risk (which is fundamentally a cost),* she says, "I do think that there is benefit. If you have an old network, there's a benefit to having a new network. Your systems run better, you'd likely need new desktops to go with it, enhanced technology – everything would be better. Newer is always better, smoother, you get better reporting, but it's still a cost. And there is no single source of technology that will make you PCI compliant. A comprehensive solution for end-to-end and provides complete data flow takes a lot of research. And though an IT group may have a significant amount of talent and skilled people, it doesn't have the expertise for a comprehensive view."

## ORGANIZATIONAL INHIBITORS

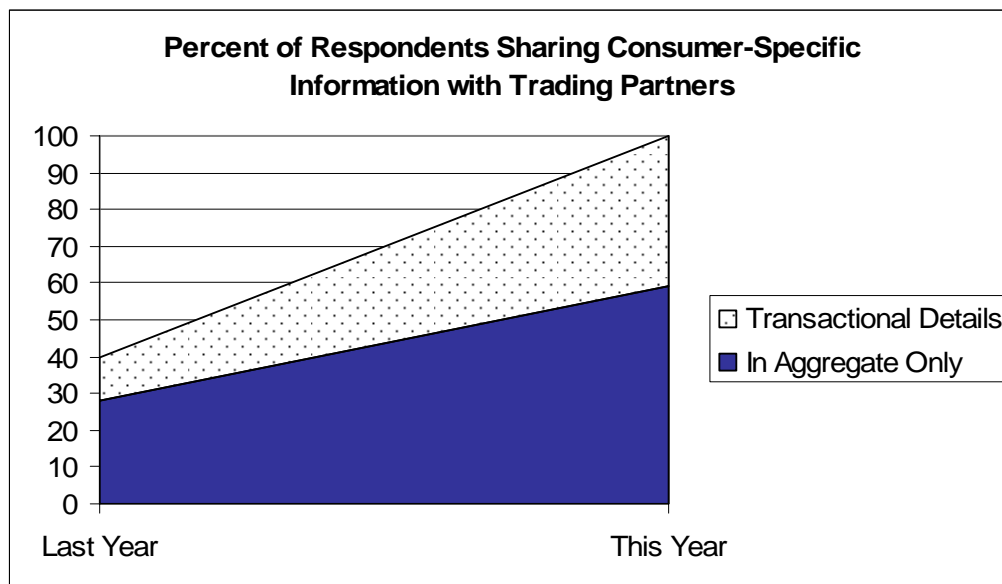
### Buy-in Is Everything

*When asked what keeps the organization from implementing stronger security of internal data-handling procedures/systems,* the retailer explains, "Your entire culture has to change. If IT controls are supported by business processes – that's when you get real change. Unless you have the business processes that are going to support successful auditing of a control – if nobody does anything to make that control passable when you audit – the control becomes useful."

*When asked about the best way to sensitize the Board,* she states, "With the lack of resources most retailers have available, something simply has to give. It has to be incorporated into something else. You can't just bring in consultants to do everything. Even though they may provide a lot, the culture change has to come from the process owners knowing what they

are supposed to do and that they're able to change how they do their jobs. You have to train people, support people, and then hold people accountable.”

The retailer continues, “We’re setting corporate policy limiting ad-hoc queries by employees, but there is still an X factor. And our biggest threat as a company is not credit card data – it’s associate and business data. VISA has done a very good job of crippling credit card information, and that’s great news for consumers. But HIPPA has not been enforced the way PCI has. It’s important to remember that Level 1 associate data could really harm you. Spouse information, child information, 401K and billing information - all of this data gets passed off to 3<sup>rd</sup> party vendors. It’s easy for us to encrypt all of our associates’ social security numbers, but we have to force that onto our vendors that manage all matters pertaining insurance, health care, etc.”



## TECHNOLOGY ENABLERS AND LESSONS LEARNED

### Keep Asking Questions

*When asked which technologies are the most mature at this point for operating a secure data infrastructure,* retailer three explains, “There is no single solution. It is a complex solution set for a complex problem. But your POS is going to be very different from your data warehousing system, which is very different from your credit card processing system. There may be solutions for each, but they must all work together.”

*When asked about impending legislation (ala SOX 404),* the retailer responds positively. “We’d welcome it. One national uniform law on customer privacy and notification would ease the difficulty of managing 50 individual sets of regulations. By default, retailers have to defer to the most stringent state in California. So we don’t want to see another unfunded mandate; a national uniform law would be ideal.”

*When asked to provide recommendations for other,* she advocates, “Corporations can help themselves if they know what they really need. IT tends to have the attitude that ‘we can keep all of this; we can capture all of this and hold onto it – just in case we need it for something later.’ So you have acres of stuff that you don’t really need, all of which needs a business justification, especially for level 1 and level 2 data. Once you’ve asked, ‘Why do I really need these credit card numbers?’ you’ll likely find that you need them for authorization and you need them for settlement, then for a certain period of time for chargeback management. That’s a legitimate business reason. But to know in your customer loyalty program what a customer spends on one card vs. another to send a targeted coupon; that’s not viable.

“Another thing is knowing where you have data. We are finding data all over: log files, trace files, troubleshooting tasks get moved to another server, power outages – the complexity is likened to Pandora’s Box. The breach has made us a better company. But we’d rather have found out proactively.”

For those who are not proactive, she states, “You’re going to have to do this. Ignoring PCI compliance will not make it go away. You need to have very good encryption methodology in place, very good access, very good authorization and the safeguarding of your company’s assets. VISA is requiring you to have these functions, and it will cost you millions in technology and resources. But the truth remains that if you don’t, you’ll have to pay those millions in VISA fines. At least by investing in technology you’re strengthening the infrastructure of your company, as well as the culture and the business processes. But retailers are not accustomed to regulations the way financial, health care and education institutions have become.”

To those with a cavalier attitude, the retailer offers the following: “People used to view VISA fines as an alternative to implementation costs. But now the payment card industry is promising to raise the interchange rate. And that puts a number on what this will cost your organization.”

*When asked about pitfalls to avoid,* she warns, “Don’t allow yourself to be seduced by what to hear. A little more research and time invested in finding someone you can trust that can guide you through the handshake of data flow is worth it. It may take longer, but it’s worth it. Keep asking questions until you get the same answer twice.”

## APPENDIX A: RSAG'S BOOT METHODOLOGY

RSAG uses its own model, called the “BOOT,” to analyze issues in the Extended Retail Industry. 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. We also identify opportunities missed – and describe leading edge models we believe can 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. 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 (ERI). 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.

## REPORT SPONSOR

### ABOUT THE SPONSOR

.....



Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government and home communications, and Cisco Internet Protocol-based (IP) networking solutions are the foundation of these networks. 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 <http://www.cisco.com>. For Cisco Retail news, please go to <http://www.cisco.com/go/retail>.

## ABOUT THE PUBLISHER

.....



RSAG 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 tradeshow, publications, research, training, and Web-based services. For more information, visit [www.retailsystems.com](http://www.retailsystems.com)

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



Copyright© 2006 by Retail Systems Alert Group, 377 Elliot Street, Newton Upper Falls, MA 02464 United States of America • (617) 527-4626.  
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.