



Safe without Wires:

The Value of Securing Wireless Technologies Report

Written by:
Steve Rowen, Partner



Sponsored by:



Table of Contents

- Executive Summary iii
- “Bootstrap” Recommendations – Elevate the Conversation iii
- Overview 4
- Why The Study Was Conducted 4
- Defining Retail Winners 4
- The Business Challenge 4
- Opportunities 5
- Organizational Inhibitors 5
- Technology Enablers 5
- Case Study Characteristics..... 6
- Case Study 1 – Grocery Retailer 7
- Business Challenges..... 7
- Wireless is Everywhere..... 7
- Manage the Human Factor..... 7
- Business in the Driver’s Seat 8
- PCI: Proactive? 8
- Opportunities 9
- Make Legacy Hardware History..... 9
- Beyond Customer Data..... 10
- An Issue of Customer Service..... 10
- Organizational Inhibitors 10
- Raise the Conversation..... 10
- Fuzzy Math 11
- Technology Enablers and Lessons Learned 11
- Strength in Numbers 11
- Avoid the Brick Wall 11
- Case Study 2 – Specialty Merchandise Retailer..... 13
- Business Challenges..... 13
- Pervasive Use..... 13
- The Hardware Headache 13
- Secure What’s Already in Use 14
- PCI: Necessary Evil 14
- Opportunities 15
- Bleeding Edge: More than Toys 15
- Organizational Inhibitors 15
- A Conversation worth Having..... 15
- Outline Success 16
- Technology Enablers and Lessons Learned 16
- The Power of Self-Healing 16
- Work in Pieces..... 16
- Appendix A: RSR’s BOOT Methodology..... 18
- Appendix B: About our Sponsors 19
- Appendix C: About RSR..... 20



EXECUTIVE SUMMARY

The value of wireless technologies is extraordinary. Steadily, ours is becoming a world without wires. Yet as today's retailer operates within an increasingly polarized paradox., the pull from one side to provide enhanced customer service is challenged by the need to cut costs. In order to differentiate themselves from competitors, retailers are also challenged to provide a heightened shopping experience to the time-starved, tech savvy 21st century customer, while also satisfying shareholders. All of this is to be achieved with a perennially limited technology budget.

As a result, retailers have shifted focus from technologies that only streamline efficiency to those that additionally address a higher order of needs. Wireless is an ideal solution to meet such needs, and increasingly becoming a means to do so at a manageable price point.

Yet the risk of operating such technologies is equally extraordinary. Retail's largest data breach to-date resulted from unsecured wireless data streaming in-store. Criminals with even the most limited technological backgrounds have targeted this free flowing signal of unfettered customer data as a highly profitable purse worth snatching from the air. Worse yet, those with motive and more realized technological savvy have identified retailers' lackadaisical treatment of data flow as a viable opportunity, extending well within the reach of highly organized crime factions. Theft of retailers' customer data is no longer just for "hacks;" it has become very big business.

The conundrum is only compounded by the hard fact that retailers, with best intentions at heart, have been leveraging the value that their new wireless technologies afford without much precaution to security. Until now.

For many, the Payment Card Industry's Data Security Standard has forced a hand of action. Whereas most were previously content to adopt a "wait and see" approach to security, the option to wait with held breath and crossed fingers that a breach would not occur has expired. At the time of this report, the majority of retailers – of all merchant tiers - are scrambling to meet their recently-extended PCI Compliance deadline.

Further, as recent breaches have shown, *customer payment data is not the only information that needs to be secure while in state.* Criminals with access to non-payment data have proven the ability to extract proprietary "security" methodologies, and with a small bit of effort, de-code a retailer's security protocol to obtain payment data.

Winning retailers' can clearly articulate the risks inherent in a future of non-compliance – **the expense far outweighs that of proactive investment.** Yet for those retailers whose security programs are lagging, while the game of catch-up can be frustrating, many valuable lessons can be extracted from retailers' whose compliance efforts are further along.

“BOOTSTRAP” RECOMMENDATIONS – ELEVATE THE CONVERSATION

From the retailers we spoke to in this case study-based report, RSR provides the following key takeaways. Not surprisingly, these suggestions are very much in line with experiences shared by winning retailers in other endeavors in customer data security research.

First, elevate the conversation. The most successful security programs are those which gain the interest of C-level executives - early on. This process will slightly vary from one retailer to another, but is commonly bound by a joint presentation of the company's current – and needed – security status to the Board of Directors.

Next, speak the right language. While compliance is the goal on which most retailers currently focus, decision makers and LOB personnel do not care about technology. By focusing on business drivers, wireless proponents can speak the language needed to realize the benefits of secure wireless solutions. This can be accomplished by addressing benefits in productivity, benefits in customer service, benefits in marketing – a language based more on revenue generation than purely cost avoidance. The ability to attain a higher level of customer centricity will always be viewed with greater interest, and by speaking directly to this point, enables foresight beyond the technological or compliance goal line.

Lastly, set clear objectives in realistically achievable pieces. Lou Holtz, Notre Dame's most winning football coach, once quoted that "When all is said and done, much more is said than done." Due to the need-based urgency to sure up existing technologies and meet industry mandate deadlines, there is no shortage of conversation and "quick fix" solutions to the customer data security dilemma facing our industry. However, winning retailers consistently demonstrate a calm and calculated approach, avoiding the fruitless hair-on-fire trap, steadily tackling one attainable goal at a time.



OVERVIEW

WHY THE STUDY WAS CONDUCTED

The goal of RSR Research’s “Safe without Wires: The Value of Securing Wireless Technologies” Report is to better understand how winning retailers are able to mitigate the challenges of operating wireless technologies – enterprise wide – more securely. Additionally, we set out to uncover how these retailers utilize technology and processes to conquer internal inhibitors and generate new revenue opportunities.

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 RSR 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

Put bluntly, retailers are currently engaged in a dangerous and expensive game of catch-up. The early generation wireless technologies they’ve been leveraging for years have brought tremendous opportunity, but were not designed with the required security measures of today in mind.

In the store, wireless technologies provide a cost-effective manner to bring store associates a higher level of efficiency. Inventory management may be completed faster and with more accuracy, while communication among store staff is greatly improved. Associates armed with wireless devices may also provide enhanced service and information to customers, many of whom already have a high-knowledge base in-store due to research performed online prior to entering the store. Customer-facing wireless technologies also shorten wait times, increase “shoppability,” generate exciting new ways to obtain product information and perform specialty functions such as gift registries, direct-shipments, and special orders of merchandise. Wireless is also becoming a common platform for myriad systems that were previously hardline-based, including replenishment and Point-of-Sale systems. The savings retailers experience by eliminating the need for cabling new and updated stores is tremendous.

In the Distribution Center (DC), wireless represents the cutting edge of efficiency and speed. The cost of operating a whirling DC can be drastically mitigated when enacting wire-free technologies, while precision can be significantly enhanced.

And in retailers’ corporate office environment, the advantages of wireless are being leveraged at a breakneck pace. This new and truly mobile workforce has become steadily more reliant on wireless tools and technologies.

Yet when not secured properly, these technologies are an open gateway to criminal activity.

As a result, retailers, faced with a consequence-driven mandate for non-compliance, are staggering to both shore up existing wireless technologies and, in some cases, replace legacy equipment with newer, more-security friendly devices. This, as with any security upgrade, presents a significant cost/ROI pain point for many retailers.

OPPORTUNITIES

While it is true that wireless technologies are helping retailers to create value in ways previously unavailable, winning retailers are viewing the move to secure these devices – and their overarching security programs - as a necessary means to much larger end.

While the industry focuses in on meeting its goals of PCI Compliance, winning retailers see compliance as part of a larger set of issues – the ability to protect and ultimately please the customer. Therefore, as PCI Compliance essentially forces the organization to reinvest in technology and processes that might otherwise have gone overlooked, it is well advised to find the tertiary benefits of such mandated change.

Our retail winners reinforce this notion, citing that the effort to become compliant has essentially shifted the organization to a proactive stance. To quote one retailer, **“We’re now proactively fixing potentially harmful errors, rather than being bitten by them.”**

ORGANIZATIONAL INHIBITORS

As with any security initiative, organizational inhibitors abound. Yet retail winners are finding ways to not only combat inhibitive factors, but actually *convert* those obstacles into proponents.

This is most successfully achieved when the conversation can be escalated beyond the IT department, and is echoed in the words of our case study respondents. However, even after the conversation has successfully been had at the highest levels, by virtue of human nature, people involved in established processes will lay ownership to certain aspects of pre-existing methods of operation. However, with a mindful (and somewhat time-consuming) effort to educate all involved as to the benefits of enhanced wireless security practices, winning retailers insist that rollout and day-to-day operations are eased tremendously – and well worth the time.

TECHNOLOGY ENABLERS

The price-point in wireless security has dropped significantly in recent years, although anxiety remains high among retailers whenever the concept of any change to the network is mentioned. It is important to note, that while bandwidth and infrastructure costs are still significant, multiple new vendors have emerged with alternative solutions to a full-scale network refresh. This pattern is highly attractive to retailers who prefer vendors who fold security and functionality into one unit, mitigating the need to purchase multiple components from multiple vendors.

In light of this, RSR highly recommends that retailers grappling with their own wireless security shortcomings roadmap exactly what goals they wish to attain, assigning realistic time and attainable time frames up front. By doing so, not only will the process of technology refresh inevitably flow smoother, but the danger of purchasing the wrong technology for its individual needs may be eliminated.

CASE STUDY CHARACTERISTICS

RSR conducted interviews with two retailers between June and August of 2007. Both 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 – GROCERY RETAILER

The first case study is a US-based grocery retailer. The company operates at the Level 1 merchant base, conducting more than six million cashless transactions a year.

BUSINESS CHALLENGES

Wireless is Everywhere

When asked which wireless technologies it is using in store, DC and back office environments, Retailer One indicates the omnipresence of wireless technology across the enterprise. “We have a wireless POS platform in our lab environment right now, and are planning to roll out to a single store for proof of concept directly. We have a number of wireless computers, the majority of which are in our back office environment. Also, in stores, we have a tremendous number of wireless handhelds in our stores, approximately 10,000, and then another 10,000 in our warehouses and distribution centers.”

He continues, “We use data encryption over some of our wireless networks, and also a significant number of cellular communications via PDAs and Blackberries, most notably in the back office environment, but these are starting to make their way into our retail locations via store managers.”

“We have wireless routers and access points in both the back office as well as stores, and several wireless customer facing technologies in the form of kiosks,” says the retailer.

Clearly the value of wireless technologies has afforded this retailer great success, as it someday plans to invest further in cutting-edge wireless solutions: “Over the last couple of years we’ve run some proof of practice implementations with RFID, but are still struggling from a warehouse and DC perspective to justify further RFID technologies. There is significant opportunity, but the cost is still too high.”

Manage the Human Factor

When asked were the biggest security challenges lie with wireless technologies in the store, the retailer lists the following:

1. User password management
2. Separating/segregating wireless traffic from the rest of the network
3. Hacks

“Password management and separation/segregation of wireless traffic from the rest of the network are far and away the most challenging aspects. Further down the line, hacks are a significant concern, but to date, our real concern is password management.”

The retailer also indicated that similarities, regardless of the environment, exist. “From a business perspective, despite a few specific technical differences, the challenges we face at the store level are identical to those in the distribution center.”

When asked about its current methodology for enforcing and enacting security procedures regarding wireless technologies, the retailer opens up to offer the following: “Enforcing policy-based procedures for legacy technologies is difficult. We don’t have current technology that helps automate key rotation, nor any that help identify rogue access. So much of what we do is based on our frequent audits – a trust but verify approach.”

He continues, “We struggle with encryption, for example, as much of our wireless encryption is isolated to areas where payment is moving across the network. We encrypt our payload, but non-payment related data is still not encrypted. Because much of what we’re working with is legacy infrastructure, it doesn’t lend itself well to the management of encryption, so we’ve had to implement a solution for a component of our environment to secure the payment while we work to uplift the entire infrastructure.”

And while the retailer’s payment system is on a separate VLAN, “We’re in a Catch 22 in terms of logging some of our payment data. We’re currently monitoring IOS logs, sending them to a central location, mining that data, and correlating it abnormal events. It’s not perfect, but at this time is the most logical and cost-effective solution.”

Business in the Driver’s Seat

When asked why this is becoming a more important issue to the organization, the retailer points to business drivers. “Wireless has the ability to help what the business wants to do from a customer centricity perspective, from a supply chain perspective, from a pricing and merchandising perspective. And we’re still struggling to support a lot of uses of wireless technologies today, due to a dated wireless infrastructure. So in addition to the more obvious compliance drivers, business drivers are really pushing us to expand our wireless infrastructure.”

He continues, “For example, we have an interest in wirelessly scanning what’s on our shelf and having that information wirelessly transmitted back to our ordering and replenishment systems. That would cut down the labor involved simply in ordering.”

The challenge also extends to the back office environment. “Everyone is clamoring for productivity and collaboration, but we only have pockets of wireless deployed.” He also addresses a common issue pertaining to distribution center and warehouse facilities. “To attain coverage in buildings of this size without dead spots - or bleed out – is still a real challenge.”

PCI: Proactive?

When asked how important it is to secure non-POS data, the retailer points to additional areas of tremendous responsibility and liability. “PCI has really turned up the heat on payment related data, but for us, there are two other categories of data that are just as important – even though they don’t receive an abundance of media attention. Because we have a health department, and also offer self-insured health care, we have a tremendous amount of patient health related information.”

This point furthers the notion that winning retailers, whenever possible, bundle their PCI Compliance efforts with a greater set of regulatory and aspirational goals.

The retailer continues, “Also, to attain our level of customer centricity, we have an unbelievable amount of customer information. We use this from a marketing perspective, and were we ever to lose that information, all of the marketing and customer centricity that we’ve excelled at would be dramatically impacted. As a result, these repositories have to be protected – this information simply can never leak out and end up on someone’s mailing list.”

The retailer also confides some effect of very recent data breaches on its security policy, but that risk assessment of its sensitive data had already been performed. “We already had the controls around this data and were fully aware of the risks, so the media attention to some other retailers’ unfortunate breaches has resulted in senior management asking the question, ‘How are we?’ Fortunately, due to our proactive nature, it was an easy question for us to answer.”

OPPORTUNITIES

Make Legacy Hardware History

When asked to identify opportunities to positively affect and reduce business challenges in the store, the retailer lists the following in order of priority:

1. Hacks
2. User password management
3. Separating/segregating wireless traffic from the rest of the network

“Because much of our infrastructure is several years old, there is a lot of opportunity to address several issues. For example, authentication into our network is fairly weak, so there is significant opportunity there. But the main concern we have today in the store is hacks. We know that wireless networks bring risk, and we’ve done some fairly exhaustive investigation to mitigate risk through the use of such controls as firewalls and ACLs, to try to segment risk from the payment environment.”

The retailer also points to the differences in securing DCs and stores. “The one major difference is that the physical controls around our distribution center data are greater than those in our store environment. Within the store, due to the nature of people coming and going, associates moving freely into the back office environment, there is much more of a challenge. Should someone walk away with an access point from a retail store – that’s not beyond the realm of possibility.”

The retailer continues, “We are also still using generic role-based account. We are in our second year of an identity access and management rollout, and the by the end of this Fall, we’ll have individual unique accounts available at the store level.”

How about employee record forms – are they fast enough?

Beyond Customer Data

When asked about opportunities existing beyond mere compliance, the retailer immediately points to information beyond payment data. Pertaining to employee record forms, “The bottom boarding process is the one thing that delays the process more than anything else. Once in the HR system, the solution has the connection and can auto-generate the accounts, but the delay is still with the paperwork aspect. So the more we can automate that through kiosk solutions in our stores, or in our HR offices, where employees and potential employees key in information, rather than writing on a piece of paper, that’s what cuts the process down.”

An Issue of Customer Service

When asked to identify additional opportunities, “There’s cost avoidance, for certain. Enacting a wireless kiosk is dramatically more cost effective than a wired kiosk, so it allows us to do a lot of things better, both from a capital perspective and a time perspective. But the majority of the business drivers are not merely cost-avoidance, but actually revenue generating. Productivity benefits, customer service benefits, marketing benefits. This is all about customer centricity, and that’s always revenue generating. We’re more focused on revenue generation than we are on cost-avoidance, and that is one of the clearest indicators that we’re in a growth mode.”

When asked which business challenges solution providers should be addressing further in their product designs, the retailer offers an interesting point of view. “Currently, most solution providers seem focused on hack detection, password management, segregation - whether by rogue detection or wireless firewalls – a lot of those simulation functions are coming into 3rd generation products, but I don’t see enough focus on outside interference.”

ORGANIZATIONAL INHIBITORS

Raise the Conversation

When asked which is the primary inhibitor to further securing the wireless technologies used, pragmatism takes hold. “Nothing more than price tag. With 1800 stores, 200 offices, warehouses and distribution centers, the price tag is daunting. With that, we’ve been working in piecemeal, and we’re going to start targeting areas where we launch any of three new technologies we’ve purchased. This means we won’t be having one massive rollout across the organization, due only to the cost factor.”

Within your organization, do you need ONE key decision maker who must understand the value of such solutions? “We have multiple decision makers in our organization, and different levels of management have different signing authority. That said, when we start evaluating large technology purchases, the CFO and CEO must be educated to the business need and the value. That means all the technical buy-in and strategy buy-in must be attained by the IT management team, conveyed to the CIO, and then presented to the CFO and CEO for any large-ticket security item.”

Fuzzy Math

When asked which are the easiest/hardest justifications to overcome and describe its strategy for gaining internal support, Retailer one speaks directly to ROI justification. “The ROI aspect is a lot easier to address from a business perspective than it is from a technology perspective because the numbers available just aren’t concrete. We can talk about the benefits, and the Gartner’s and Forrester’s of the world put out pieces identifying total cost per lost record, but until that actually happens to you, those figures are still very fuzzy. They’re not as dramatic and concrete as if we examine the investment of dollars and the X number of dollars returned through increased sales, increased productivity, or improved labor costs. That is a business decision, and that is black and white when you’ve enacted the business drivers to support the infrastructure investment.”

When asked how inhibitive the conception that a wireless security upgrade will require enormous network upgrade costs is, “This is an eight figure price tag. So, it’s pretty significant.”

TECHNOLOGY ENABLERS AND LESSONS LEARNED

Strength in Numbers

When asked to rate the existing solution community’s response to these challenges, the retailer insists that not all vendors are created equal. “I think it depends an awful lot on the vendor. There are some that are trying to be a one stop shop, and that’s much more advantageous to us. We like vendors that fold the security and functionality together into one unit, so that we don’t have to purchase multiple components from each vendor.”

When asked which existing technologies help move the organization further toward its PCI compliance goal most realistically, “Those which don’t require multiple partners. Moving toward the PCI goal, there are many ways to get there. Compensating controls allow a retailer to do a lot - you can have a very insecure wireless network next to a very secure payment network, and according to the auditors, that’s acceptable. But from a security perspective, I still have heartburn over knowing that the credentials from a wireless network could be compromised and used on a wired network. I don’t think PCI is the driver that many make it out to be, since you can get compliant without having to really completely address the risk.”

Avoid the Brick Wall

When asked for recommendations to others in a similar situation, “Focus on the business decision, not the technical one. If I’m talking to the CEO or CFO about the technical reasons to upgrade wireless, it will always fall on deaf ears. But if I’m able to talk to the business opportunities or in some cases, such as PCI Compliance, the cost effectiveness, that’s when it will resonate. The financial viability is always what brings about buy-in and change when dealing with security issues. That’s when the question comes down, ‘Why would we not spend money to get all of this additional revenue?’”

When asked what pitfalls to avoid based on its experience, Retailer One points to the importance of elevating the conversation. “This cannot be looked at as a technical or security problem. That approach will only guarantee running into a brick wall when the discussion invariably

elevates to those who are coming from a business background. So make sure you look at wireless security as a business solution to a business problem. What enhanced capabilities will increase productivity? What will a wireless solution provide beyond PCI Compliance? If you can have those business drivers it moves a lot better.”

CASE STUDY 2 – SPECIALTY MERCHANDISE RETAILER

The second case study was conducted with a specialty 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

Pervasive Use

When asked which wireless technologies it is currently using, the retailer indicates a plethora of devices. “In the store, we’re using wireless PCs, wireless handhelds, 802.11 a, b, and g, access points, and on the horizon we’ve identified wireless digital video surveillance as something we’re very interested in.”

“In the distribution center we’re using wireless VOIP phones, Blackberries and wireless PCs as well, wireless handhelds, and we’re currently discussing some RFID options with several of our manufacturers. Whether we will go full RFID or just high-ticket items is still being discussed.”

He continues, “In our back offices we’re using all types of wireless and cellular communication devices, including PCs, PDA’s, and Blackberries for both our stationary and traveling IT department.”

The Hardware Headache

When asked to define the biggest security challenge it currently faces, the retailer immediately points to legacy equipment. “This is admittedly more of a budgetary issue than a technical one, but we have so much legacy equipment in our distribution centers and our stores that requires us to stay with WEP. We’re in the process of getting rid of all of it, but swapping thousands of devices at a time has been a real challenge.”

He continues, “From a technological standpoint, wireless has been fairly straightforward for us, but authentication has been an issue. Trying to protect devices that we don’t have control over, for example, making sure that our wireless PCs in our stores remain ours. We’ve worked closely with our active directory team to build machine counts and active user accounts, so if a machine and its user aren’t both in a specified wireless user group, access is denied. We started this by Mac filtering, but quickly transitioned into these user groups, essentially enabling any authorized wireless user to access any authorized wireless device.”

Retailer Two also identifies some future challenges it is seeking to eradicate today. “In addition, mobile users VPN to get to corporate systems via a SSL VPN portal, but we are in

the process of building parallel wireless LAN segments at stores - a guest network for mobile workers - that are completely segmented from the rest of the network.”

Secure What’s Already in Use

Retailer Two is also in the process of learning more about interference and hacks pertaining to its pre-existing wireless solutions. “As far as signal theft and hacks, in both our stores and DCs, we are currently piloting a system to monitor signals and notify us of any unauthorized users attaching to our access points. We’ve already had great success with it in the corporate environment, and we currently get alerts if someone is trying to connect. So far, what we’ve found is that 90 percent of these attempts have been employees trying to access our wireless with devices they’ve brought in from home, but we want to know more about bleed-out and attempted hacks, so that’s why we’re piloting right now.”

When asked to describe its current methodology for enforcing/enacting security procedures regarding wireless technologies, the retailer points to the importance of further – and specific – consideration for wireless applications. “Our security policy is really about access, and is not specific to wireless. But this is changing. For example, currently, payment card transactions do not traverse our wireless network in any way, but as we move to a new POS system, we’re forced to adopt further segmentation, VLANs, switches, and other lock-down technologies.”

When asked about ways to improve the above methodologies for enforcing/enacting security related procedures and practices, forensic data capture tops the list. “We’re currently looking to improve our forensic data capture. Currently, the alert program we’ve been running at the corporate level for a few months has provided us with an enhanced comfort level, and we’re eager to obtain that feeling for what transpires in our stores.”

PCI: Necessary Evil

When asked how large of an influence the PCI mandate is on its current and intended course of action, the retailer pulls no punches. “PCI is a nightmare. It’s been a tremendous factor in the consideration of a new POS, and it’s partly eradicated additional wireless applications we were considering.”

Interestingly, the retailer’s motivation to become compliant is more focused on the customer’s security than that of brand damage or non compliance. “No one wants to be the company in the news, but we’ve had so many changes to applications, servers, and processes that we’ve had to enact a separate testing room at corporate to test all devices and applications for their ability to help us stay PCI compliant. The net, of course, is that PCI has become far more expensive than SOX 404. We didn’t like Sarbanes, but we actually hate PCI. The thing is, we’re all customers somewhere, so even though we hate it, we know it has to be done”

He continues, “We meet 2-3 times a week in different departments to discuss PCI Compliance. We’re being extra cautious, we’re doing all the diligence, we don’t want to leave anything unchecked.”

When asked how much of a challenge incorporating new security technologies with legacy hardware poses, “We used to have five to six individually managed access points at every store, and at the time, we had 130 stores. When a disgruntled employee left, we realized we were wide open to risk, and had to immediately change every store. At the store level, we had to install a centrally managed system, while at the DC, we enacted finger-pointer scanners, which only work with a certain level of WEB encryption. So for a few years we’ve been trying to gain funding to replace some of this legacy equipment, and that’s one area where PCI has been a tremendous help. As a result of the challenge to make these devices work with new radios and new systems, we’ve decided to literally pull all of it. We’ll be entirely WEP free by October.”

OPPORTUNITIES

Bleeding Edge: More than Toys

When asked what additional business benefit result from addressing these challenges (cost avoidance vs. ROI, consumer trust, value, competitive advantage), “We get to do some fantastic stuff. We’ve never been a large proponent of bleeding edge, but in the area of wireless and security, our organization realizes the advantage of being 10 steps ahead.”

The retailer goes on to describe some of the tertiary benefit of the mandate. “From a non-technology side, PCI has given us the opportunity to set up processes we never had in place: this week we’ll log into every firewall, we’ll check every user account, we’ll check every log in, we’ll check that we’re sending all our data according to SOP. It’s given us a reason to refresh on a configuration level, not just a technological level. **We’re now proactively fixing potentially harmful errors, rather than being bitten by them.** We’re no longer reactive.”

ORGANIZATIONAL INHIBITORS

A Conversation worth Having

When asked to identify a primary inhibitor to further secure wireless technologies, the retailer offers up a highly pragmatic reply. “Time. PCI Compliance doesn’t wait. Staff budget is far harder to obtain than gear budget for us. And in our team, there are several ‘this is the way we’ve always done it’ people, who’ve been resistant to process change. This mandate is very specific, and for those who don’t want to change the way they’ve operated, those who’ve always had access to a device that now, due to specific rules and regulations, no longer have access – overcoming that pushback is inhibitive.”

He also reinforces the notion that there is far more to a successful compliance program than technology. “What this really gets down to is people. The security and compliance team can often be viewed as smug, arrogant and high handed. For example, many of our store users want to use Apple AirPort devices, and it is our responsibility to refute these requests. We’ve come to the conclusion that it is not necessary for us to demonstrate to our store associates how vulnerable certain wireless technologies – technologies we sell in store – really are. And this often results in a crossing of swords with a store or DC operations employee. Another example, we have a group that thought sites would work better with dedicated T1 lines. We

did the proof of concept, and showed the gain as 1.5 seconds every 15 minutes. This is clearly not worth the \$1000 a month upgrade to a T1, so these are conversations that we're having quite often."

Retailer Two goes on to describe the benefit of unified internal communication. "As a result, one of the things we've found is that having these conversations is very beneficial. Most people tend to better understand once we've taken time and made the effort to explain why our wireless and security policies require change – but again, that takes time."

In summary, "The issue of bandwidth vs. latency is a difficult conversation to have, but it is important to drive home to users that the slowest link in the chain is always the human interface."

Outline Success

When asked who within the organization is the key decision maker to must understand the value of such solutions, Retailer Two offers the following: "We have a new CIO, and we're going through a series of changes. He comes from a highly technical background, so that is a large value-add. But we still had to make a presentation outlining where we are today, and what steps we'd like to take next. And one of the things that we have that makes our efforts more bearable is the fact that our direct networking team has given me, the spearhead of this project, 100 percent support."

TECHNOLOGY ENABLERS AND LESSONS LEARNED

The Power of Self-Healing

When asked which existing technologies help move the organization further toward its PCI compliance goal most realistically, "We've had to pre-build a system for a new DC facility. Until recently, all of our networks were pretty flat and all touched each other. Today, it's set up in an appropriately segmented fashion. Our LAN infrastructure and our new wireless security technology allow us the freedom to move forward without any downtime or outage."

"In addition, we're migrating from a case-by-case management of each individual AP at the switch to a centralized management system, giving us multiple redundant controllers at corporate that take over should any local controller fail. So the ability to centrally manage security from a single location has been a key enabler. It's changed the way we look at technology – going forward, if a product doesn't give us central management we're not interested in its potential functionality."

"We're also experimenting with self-healing and self-blocking technologies, which can automatically take themselves offline should an event occur."

Work in Pieces

When asked for recommendations to others in a similar situation, the retailer stresses the importance of not allowing scope to overwhelm. "When we first started, we were stabbing at everything all at once. Until we sat back and roadmapped our PCI and wireless goal, we didn't have great progress. Once we had gone through and identified our devices, identified who had

access to each and assigned responsibility, and verified configurations – the basics – we found that we’d knocked out the first third of our PCI Compliance initiative. After that, it became systematic, but it was entirely dependent on roadmapping what we had and what we’d need to do”

When asked to share pitfalls should others avoid based on its experience, Retailer Two warns of the dangers of trying to boil the ocean. “It is very easy to become overwhelmed, especially when you first start examining your data in state. In addition to all of the other things we were on the hook for, once we started to examine our data structure, panic set in for about a week. Only when we settled down and broke the initiative down into manageable chunks, were we able to make real headway.”

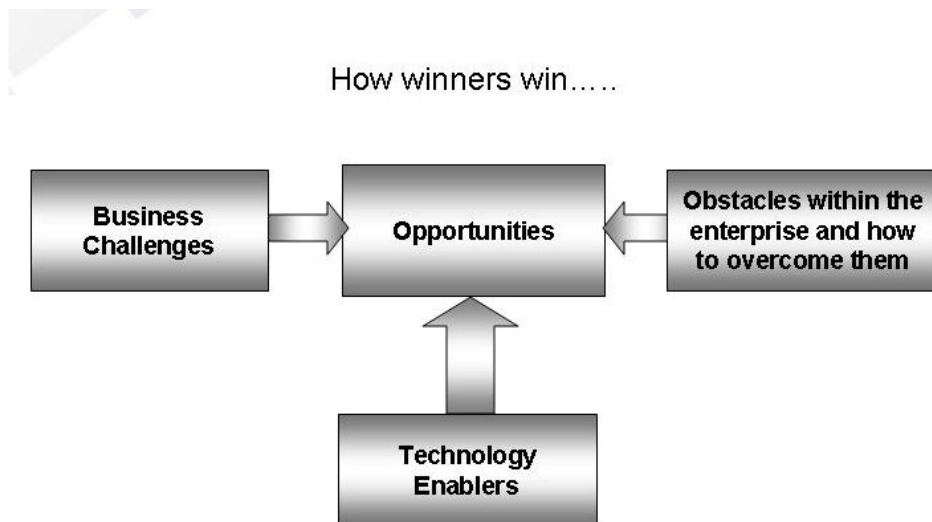
The retailer also points to the importance of action. “There are dozens of companies that will come in and perform a PCI audit, and that’s great. But while they are working, we’re not. The report does not fix the problem, it’s very important to avoid analysis paralysis.”

APPENDIX A: RSR'S BOOT METHODOLOGY

RSR 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** – RSR 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. RSR’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. RSR’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. RSR surveys question retailers about the technologies they employ to solve their business challenges.

RSR believes winning is not an accident in the retail industry. 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.



APPENDIX B: ABOUT OUR SPONSORS



AirTight[®]
NETWORKS

AirTight[®] Networks enables enterprises and service providers to maintain network and mobile client integrity from wireless security vulnerabilities whether or not they deploy a wireless network. AirTight Networks offers the industry's first wireless IPS (WIPS) that delivers around-the-clock wireless monitoring and automatic intrusion prevention as well as manages wireless network performance for maximum capacity and uptime. For more information, visit our website www.airtightnetworks.net.



Aruba Networks enables cost-effective and painless PCI compliance with one integrated platform for security, wireless LANs, mesh and remote access. Aruba offers built-in Wireless IPS capabilities to be used as an overlay to protect an existing wireless LANs or as an integrated part of a secure wireless LAN that protects legacy WEP-only devices and enables new mobile applications. Aruba's centrally managed platform is designed to easily fit on top of existing wired and wireless networks to prevent unnecessary network redesigns and upgrades. For more information, please visit www.arubanetworks.com/pci.



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, and thought leadership and advice on navigating these challenges for specific companies and the industry at large. RSR’s services include benchmark reports covering the state of retailer technology adoption for topics ranging from merchandising and supply chain, store operations and workforce management, to customer-facing and multi-channel technologies. Custom research reports provide more in-depth views into topics of industry interest, and advisory services help retailers and technology vendors make the most of the insights RSR provides. To learn more about RSR, visit www.rsresearch.com.