

## COMPREHENSIVE SECURITY: GOING BEYOND THE FIRST LINES OF DEFENSE

Senior retail managers who have relegated PCI compliance responsibility to lower levels of the organization may be missing a critical opportunity to protect and even grow the business. Evidence is ample that, even after a months-long audit, attaining PCI-DSS compliance certification does not even guarantee that the enterprise was completely compliant at that moment. Retailers must adopt the mindset that data security is a critical and constantly moving target, and devote sufficient resources to developing a comprehensive framework to continually assess and address risk. A well-thought-out, comprehensive security plan can not only protect the enterprise from risk, but also reduce costs by abandoning a patchwork approach and enable innovation by providing a secure environment in which to develop new initiatives.

Sponsored By:



**MOTOROLA**

### › INSIDE

- 2 RISK IS EXPANDING
- 3 PCI: A PART OF THE PLAN
- 4 SECURING THE ENTIRE RETAILER ECO-SYSTEM
- 8 THINK BIGGER: SECURITY BEYOND PCI
- 9 DON'T THINK COMPLIANCE, THINK SECURITY

Personal financial identity ranks right up there with medical records when it comes to sensitive data. So you would think rules designed to safeguard that data, such as PCI DSS, would be so robust that they'd serve as the model for data protection done right.

Unfortunately, the reverse is true. The PCI standards body needs to learn a thing or two from those actually involved with implementing comprehensive, high-quality data security systems and procedures.

So retailers that think PCI compliance equals full data protection need to think again.

The intent behind PCI DSS is to protect highly sensitive cardholder data, specifically in the transaction process. That's a good start. But when we read stories about PCI-certified retailers suffering massive data breaches, it's clear that PCI DSS is not a roadmap to true security. Instead, compliance with PCI must be regarded as one often-revisited milestone on the journey to a comprehensive, evolving approach to securing all of a retailer's sensitive data and networks. In fact, it is possible to create a security infrastructure that is both comprehensive and cost-efficient AND which provides competitive advantage to a retail business.

For example, In Aberdeen's *Data Loss Prevention* report, June 2008, Best-in-Class organizations had experienced one data loss event in the last 12 months compared with eight for laggards, with an average cost of \$640,000 per incident. That adds up to \$4.5 million in cost avoidance for the Best-in-Class organizations.

**[TAKEAWAY]**  
**> COMPLICATING DATA SECURITY IS THE GROWING COMPLEXITY OF RETAIL NETWORKS. AS CUSTOMER TOUCHPOINTS EXPAND, SO DOES THE RISK.**

## RISK IS EXPANDING

Complicating data security is the growing complexity of retail networks. As customer touchpoints expand, so does the risk. The proliferation of channels includes e-commerce sites, social networking sites and physical locations including offices, call centers, distribution facilities and stores. These often feature both wired and wireless networks (intentional or rogue) supporting a proliferating number and variety of associate-facing and customer-facing devices. Integration of previously separate applications is also creating more pathways for data, both within retail organizations as well as through linkages with suppliers, distributors, service providers, financial partners and other third parties. IT trends including virtualization and cloud computing further deepen the complexity. The very technologies enabling twenty-first century retailing are those that are substantially broadening retailers' exposure.

Unfortunately, many retailers have devoted disproportionate resources to PCI to the detriment of other security priorities, or assembled an array of point solutions that leave dangerous gaps in coverage. According to a recent survey from Imperva and the Ponemon Institute, 71% of companies surveyed admit to not making data security a top strategic initiative, and 55% say they are only securing credit card information and not sensitive information such as Social Security numbers, driver's license numbers, and bank account details. A particularly troubling finding is that 60% of respondents don't think they have sufficient resources to comply with PCI and bring about a necessary level of cardholder security.

There are hopeful signs, however. According to AMR Research's *Get Thyself PCI Compliant: The Latest Approaches and Recommendations*, March 2009, "organizations are combining PCI compliance and management efforts into their overall corporate governance, risk management and compliance (GRC) organizations." However, as of January 2009, just 25% of those surveyed were using GRC as a strategic approach to compliance and risk management, according to *Cost-Effective Compliance*, a presentation to the National Retail Federation CIO Council by PCI Knowledge Base. In RIS News' *Store Systems Study 2009*, PCI compliance equipment/software updates was tied for #1 in retailer's top priorities for 2009, selected by 58% of respondents along with providing associates with better tools.

The bottom line is this: PCI DSS has proven itself unsuited to the task of ensuring complete data protection. To prepare for a secure 2010 and beyond, retailers must engage in industry best practices and prioritize data security not only to attain compliance, but to minimize risk across the enterprise.

Retailers must understand their unique security needs and develop a comprehensive framework for addressing today's vulnerabilities as well as setting up mechanisms to evolve security protections as the threats evolve.

### PCI: A PART OF THE PLAN

To date, many retailers have prioritized PCI compliance over other types of data security and used PCI requirements as a framework guiding their data security project planning. But this approach creates an overreliance on a generic roadmap that doesn't account for non-transactional data security or unique aspects of each retailer's business. Also, most importantly of all, it draws attention away from the primary goal – keeping your most valuable asset (your customers) safe from data theft.

*Continued on page 6*

### IN 2008'S DATA BREACHES...

74% resulted from external sources

20% were caused by insiders

32% implicated business partners

39% involved multiple parties

67% were aided by significant errors

64% resulted from hacking

38% utilized malware

22% involved privilege misuse

9% occurred via physical attacks

SOURCE: 2009 VERIZON BUSINESS DATA BREACH INVESTIGATION REPORT

**[INDUSTRY INSIGHT]****SECURING THE ENTIRE RETAILER ECO-SYSTEM**

A secure, reliable network is one that offers availability, integrity and confidentiality. Motorola offers a holistic approach to help retailers secure their entire network, whether it's wired or wireless. RIS News talked to Richard Rushing, Chief Security Officer for Motorola's Mobile Device Business, about the company's approach to network and data security.

**Q: WHAT DO YOU SEE AS RETAILERS' TOP CHALLENGES RIGHT NOW IN SECURING THEIR DATA AND NETWORKS?**

**A:** There are so many that it is difficult to boil it down to a single answer, but certainly one of the biggest is balancing the consumer's desire for speed and efficiency with the need to protect sensitive data. In their efforts to make the shopping and check-out experience as pleasant as possible, retailers have deployed very sophisticated wireless networks and equipped their employees with mobile devices. Combining this with their extensive supply-chain networks and extranets creates a lot of complexity and vulnerability that can be difficult to manage.

**Q: TELL US ABOUT MOTOROLA'S INVOLVEMENT IN RETAILER DATA SECURITY.**

**A:** We take a holistic approach, from designing mobile devices and wireless switches with PCI-compliant encryption and firewalls, to delivering a full suite of security services to help retailers manage the complexity and defend themselves from attacks. But we also know from scores of security engagements as well as our own in-house experience that technology is only part of the answer, so once we "secure the perimeter" or address specific compliance requirements, we work with retailers to make security part of their everyday business processes. This allows the security program to be more responsive to the dynamic needs of the retail business.

**Q: DO YOU HELP RETAILERS ADDRESS WIRELESS NETWORK SECURITY ONLY, OR WIRED AS WELL?**

**A:** Certainly wireless security is a big part of our value proposition and a differentiating core competency, but we recognize that information has to be protected through its entire lifecycle. The need for protection doesn't change with the conduit and it doesn't end at the firewall. Our goal is to provide security solutions from the point of data capture to the place of data storage. Our focus is on helping retailers operationalize security and extend it throughout the network of suppliers and partners. That means we have to concern ourselves with the wired network as well as wireless.

**Q: WHAT AREAS DO RETAILERS TEND TO OVERLOOK OR UNDER-FUND IN THEIR DATA SECURITY PLANS?**

**A:** The retail environment is dynamic. Stores are always changing, with people moving in and out, new products, new technologies, and new business initiatives. We find that many retail organizations treat the environment as though it's static, designing a security solution for a particular point in time and then thinking that it will continue to work for them. However, that solution is often focused on the technical requirements rather than the broader view that security requires.

**THE NEED FOR PROTECTION DOESN'T CHANGE WITH THE CONDUIT; RETAILERS NEED TO ENSURE SECURITY THROUGHOUT THEIR ECO-SYSTEMS.**

But technology is not a silver bullet. It requires a holistic approach of people, process, policy and technology. The solution must consider how you manage risk in a sustaining way that also aligns with strategic business goals. It becomes robust when security is part of operational processes. It becomes agile and resilient when the security team is viewed as the advisor to the work of their internal business partners. As security professionals we must ask, “Do we have a policy foundation that defines our expectations? Do we have gaps within our policy and are the appropriate protections in place? Do we have an auditing or monitoring process for configurations and protections?” It’s the investment in those foundational capabilities that allows us to operationalize security. It’s the day-to-day hard work to operationalize that sometimes lacks the appropriate focus and funding.

**Q: HOW CAN THOSE RESPONSIBLE FOR RETAILER DATA SECURITY ENSURE C-LEVEL SPONSORSHIP FOR DATA SECURITY INITIATIVES?**

**A:** It starts with a focus on the real risks. Security professionals need to understand and align with the mission of the company. Once you understand the business goals and the risks to those goals and align your security program to them, the funding typically follows. As security professionals, we need to bring to management an understanding of the risk tied to the business goals and let them decide what is acceptable.

Another thing we need to develop is a roadmap with suggested areas of investment one, two, and three years out. We know this outlook can change, so if the risk drops we can move something out and if it increases we can pull things in. At Motorola we did that with some technical controls. The risk changed and we dropped the requirements. We were then able to bring that back to management to show we are realistic, in sync with business needs and build credibility as business partners.

Here’s another example. Right now it is important to communicate to management that wireless is a critical, deeply integrated part of the business. We need to update and incorporate wireless and mobility risk into the analysis and dialogue to protect and enable our business goals.

**Q: YOUR MESSAGING SUGGESTS THE STEPS NEEDED TO SECURE DATA CAN ALSO ENABLE INNOVATION AND HELP GENERATE REVENUE. CAN YOU EXPLAIN?**

**A:** Once you build a firm foundation of a properly applied holistic security program, you attain scalability, reliability and agility in your environment. You are better able to respond to and support the dynamic needs of the business. Conversely, an unsecured network is one where you’re not in control of who’s on the network and what they can access. You lack visibility, leading to slow response times, separation of systems, crashes, and so on. You don’t get the best of your technology investments if people stop using them due to limitations and performance issues.

With a secure network you can get the best out of the technology – wireless kiosks, queue-busting, and so on, and easily add new devices, with the reliability and bandwidth necessary to properly support them. That leads to significant productivity enhancements: associates can do their jobs more easily, they can help more people, customers complete their purchases, supply chains work properly. A secure network is a stable network, and a stable network enables innovation. ■

**ONCE YOU BUILD A FIRM FOUNDATION OF PROPERLY APPLIED SECURITY, YOU ATTAIN SCALABILITY, RELIABILITY AND FLEXIBILITY IN YOUR ENVIRONMENT.**

Continued from page 3

In some cases, the most obvious choice of a technology to address a specific PCI requirement may not be the best one; an alternate may address the requirement while delivering additional benefits. This concept was advocated by Avivah Litan, Vice President Distinguished Analyst with Gartner Research, in a May 2009 report, *Moving Beyond PC*, at Visa's Global Security Summit: "Many companies have implemented security technologies that aren't included in the PCI standards, but provide equal or greater levels of protection."

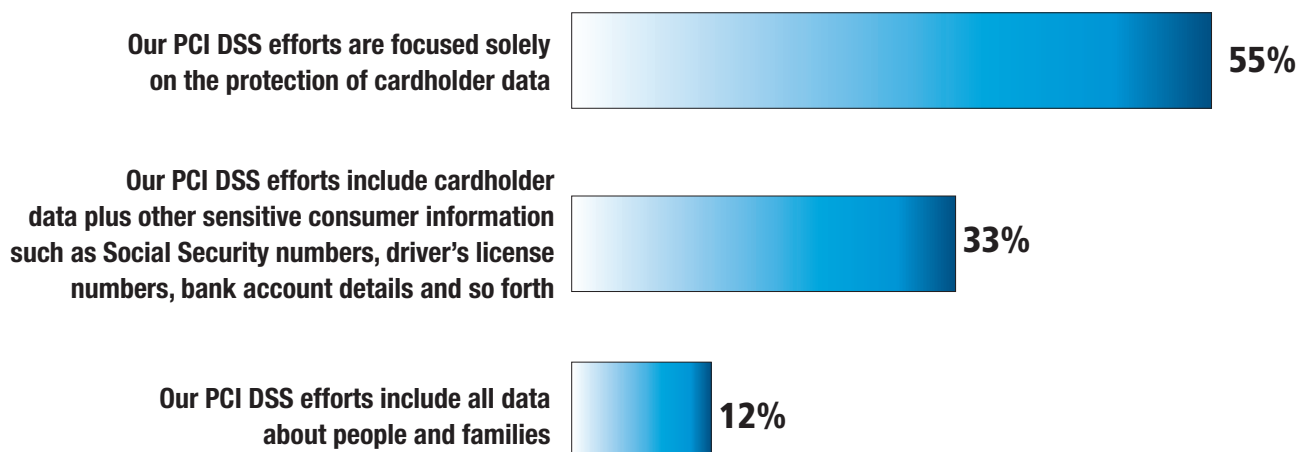
PCI compliance remains essential, but here are some things to consider in formulating a response that also accommodates the greater goal of comprehensive security:

- **THE PCI STANDARD IS NOT A ONE-TIME TARGET.** Retailers' IT environments are constantly changing, so a retailer can fall out of compliance even in the midst of an audit. At the same time, PCI requirements continue to evolve. Dave Hogan, senior VP and CIO at the National Retail Federation (NRF), told RIS News in March, 2008 that "PCI is a valiant attempt to prevent large stockpiles of credit card data from getting into the wrong hands. However, it is unlikely PCI will ever be able to keep pace with the continually evolving sophistication of the professional hacker. Nor will it be able to anticipate every possible variation of future attacks. We believe the time has come to rethink the assumptions behind PCI." The lesson: keep up with PCI, but comply in the context of larger security goals.

### [TAKEAWAY]

➤ **MANY COMPANIES HAVE IMPLEMENTED SECURITY TECHNOLOGIES THAT AREN'T INCLUDED IN THE PCI STANDARDS, BUT PROVIDE EQUAL OR GREATER LEVELS OF PROTECTION.**

## FOCUS OF PCI DSS COMPLIANCE EFFORTS



SOURCE: PONEMON INSTITUTE 2009 PCI DSS COMPLIANCE SURVEY, SEPTEMBER 2009

- **PCI COMPLIANCE IS NOT A ROCK-SOLID LIABILITY SHIELD.** Hannaford Bros. is among retailers whose credit card data was breached while the company was deemed PCI compliant. Compliant retailers' protection from civil suits is now also under serious threat; the viability of consumers' suing for the time and effort required to reclaim their identity in the Hannaford case is being heard by the Maine Supreme Court. Even if that effort fails, future protection from consumer suits is not guaranteed.

Retailers must remain vigilant about evolving PCI needs and consider compliance solutions in the context of their comprehensive security plans. Among the recent changes:

- **NEW WIRELESS STANDARDS:** In July 2009, the PCI Security Standards Council published guidelines delineating how wireless security applies to PCI DSS 1.2 compliance. The guidelines recommend the use of Wireless Intrusion Prevention System (WIPS) to automate wireless scanning for large organizations. Even those not using wireless networks may still be required to ensure wireless nets do not exist in their environments; hackers have used rogue wireless networks secretly placed in stores to obtain sensitive data. According to wireless network vendors, a comprehensive approach to wireless security might also include a pre-audit assessment, perimeter firewalls, comprehensive and up-to-date security support, a seamless portfolio of PCI-capable data capture products, policy compliance, 24/7 monitoring, and use of a WIPS tool, which can help retailers prove compliance at any given moment via reporting and forensics.

The good news is that wireless security tools and practices already in place seem to be working; Verizon's *2009 Verizon Data Breach Investigation Report* examined 90 data breaches and found just one case in 2008 and one in 2007 involving a wireless network, down from 13% in 2004 to 2006. Motorola AirDefense's *Retail Shopping Wireless Security Survey* showed 44 percent of the wireless devices used by retailers, such as laptops, mobile computers and barcode scanners, could be compromised, down from 85 percent of wireless devices in 2007.

- **PIN FINES DELAYED:** Visa agreed to back off imposition of fines related to its PIN pad compliance deadline originally set for July 1, 2010, to the new date of Aug. 1, 2012.
- **NEW COMPLIANCE STRATEGIES:** Newer technologies retailers are applying to their PCI and other security efforts include **Tokenization**, substituting a token or reference number for a credit card number or other sensitive data to eliminate on-site storage of that data; **Application Whitelisting**, deciding which applications and devices are approved to run in their retail environment while blocking any unauthorized software or storage devices to eliminate risks from unwanted software; and **Virtual Terminal Systems** to eliminate local storage of card data, touted in a recent report from PricewaterhouseCooper for the PCI SSC. The NRF web site lists 25 best PCI practices in content available to members.

In the view of the National Retail Federation, PCI is overly complex and has done little to stop payment card data thefts and fraud. Nevertheless, addressing evolving PCI requirements is a critical part of a retailers' security strategy. PCI not only forms a foundation on which a broader plan can be built, but it becomes the first line of defense against increasingly sophisticated hackers.

### [TAKEAWAY]

› **IF YOU DON'T NEED THE DATA, DON'T COLLECT IT. KNOWING WHAT DATA YOU WANT TO PROTECT AND HOW YOU WANT TO PROTECT IT IS CRITICAL BEFORE YOU SET YOUR SECURITY PLAN IN MOTION.**

## THINK BIGGER: SECURITY BEYOND PCI

Instead of shaping data security plans and spending around PCI requirements, retailers will maximize their cost-benefit by creating a comprehensive security plan that strives to secure data across the enterprise. Such a strategy digs deeply into technology infrastructure and the organization's standard operating procedures, but pays off because it minimizes risk while offering a competitive advantage in the marketplace.

A comprehensive plan also helps retailers comply with other data privacy laws. California's is well known, but recently Massachusetts and Nevada strengthened protections of personal information; businesses must prove they have proactive data security measures in place to prevent a data breach from occurring. Other states could follow suit. A well-thought-out plan can also help retailers comply with regulations such as Sarbanes-Oxley.

Best practices for creating a comprehensive security plan include:

**1) BASIC ASSESSMENT:** You can't protect what you don't know. Start with a basic assessment of data and networks used to run the business and how they're used. View data as a lifecycle from birth to death, and as it resides within business processes. Track data through all possible channels. This process is best executed by a cross-functional team including data owners, IT, legal and the data security staff.

**2) SEGMENT AND CLASSIFY DATA:** According to *How PCI Leaders are Different from Other Merchants*, by Dave Taylor, Research Director of the PCI Alliance and Founder of the PCI Knowledge Base, PCI Leaders protect other data besides card numbers.

Useful segmentations are: public, confidential or highly confidential, and structured or unstructured, such as IMs, Web pages, Word documents, spreadsheets. In Aberdeen Research's *Securing Unstructured Data*, October, 2009, respondents estimated that an average of 40% of their sensitive data is in unstructured formats. Another way to sort data is to rank it by the impact of data loss on the business. The cardinal rule of data security: if you don't need the data, don't collect it. Knowing what data you want to protect and how you want to protect it is critical before you buy a tool.

**3) AUTHORIZE USERS:** Assess which users must access which data based on role. Enable business units to review and remediate only those incidents relevant to their role and privileges. According to Verizon's *2009 Data Breach Investigations Report*, end-users and IT administrators were responsible for an equal number of insider data breaches studied, though the latter have much more opportunity due to increased privileges.

**4) FORMULATE DATA CLASSIFICATION, PROTECTION AND USAGE POLICIES:** Start with a narrow set of policies, implemented incrementally, and then expand them once incident types, volumes, workflows and processes are better understood. Expect it to take about three to six months to tune and optimize a new policy, depending upon its complexity. Look for technologies to automate enforcement.

**5) SECURE THE RIGHT LEVEL OF RESOURCES:** Ensure both corporate and rank-and-file buy-in. The most carefully crafted technical and policy solutions are brought to their knees by non-compliance. Budget for continuous upgrades. Assign ongoing ownership and responsibility for both process and technology solutions.

### [TAKEAWAY]

› THE MOST CAREFULLY CRAFTED TECHNICAL AND POLICY SOLUTIONS ARE BROUGHT TO THEIR KNEES BY NON-COMPLIANCE

**6) IMPLEMENT TECHNOLOGIES:** Design a complete, programmatic approach that works across channels, to address the problem in the most thorough and cost-effective way. A comprehensive solution will include multiple components, such as collaboration tools, content management, access management, encryption and key management, enterprise rights management, data loss prevention, and other content monitoring and filtering solutions. The difference between this and current approaches is they are thoughtfully layered together to create an end-to-end solution, rather than deployed piecemeal to meet the latest threat.

The best security solutions enable, rather than hamper, progress toward business goals, and ideally, allow for innovation. Some points to consider in the process of developing a plan include:

- **MONITOR:** According to the Verizon *2009 Breach Investigations Report*, the ability to detect a breach when it occurs is a huge stumbling block for most organizations; 69% of breaches that occurred in 2008 were discovered by a third party. Monitoring tools must be tuned to accurately monitor and detect security violations for all data types, all data endpoints, and all network protocols, including e-mail (SMTP), instant messaging (such as AOL, MSN, Yahoo!), Web, secure Web, FTP, P2P, and generic TCP sessions over any port, and at the right level of detail.

Plan to measure the effectiveness of your information security plan over time, so you can reassess risks, fix broken processes, and identify potential compliance issues. PCI Knowledgebase's Taylor says PCI leaders take monitoring the extra mile, using controls to predict breaches and monitoring their service providers and partners as well as themselves. "PCI only requires a letter of agreement that a service provider will adhere to PCI. Leading firms are doing real due diligence of their service providers and partners," Taylor says in *How PCI Leaders are Different from Other Merchants*. "Some are sending out questionnaires, others are sending auditors to review the security of their service providers."

- **EMPLOY ENCRYPTION.** Encryption is an effective and powerful tool, but it must be applied properly. Data must be protected when it moves physically or virtually; when it's at rest; and access to data must be restricted. Encryption combined with tokenization is widely viewed as a powerful combination. Visa's new Data Field Encryption Best Practices (DFEBP) are designed to complement PCI DSS.
- **CONSIDER OUTSOURCING PAYMENT.** According to PCI Knowledge Base's Taylor technologies such as end-to-end encryption and tokenization make it viable to outsource most PCI compliance tasks by having payment processors and payment gateways actually control most of the process from the initial card data collection. "The PCI DSS mandates have caused what appears to be a fundamental shift in the willingness of even large organizations with extensive, well-trained IT teams to consider IT security outsourcing to an extent that I've not seen before," Taylor says, though he cautions that potential outsourcers consider their ability to understand and measure their risks.

**7) EDUCATE.** With any technical implementation, ensure employee education/awareness and skills transfer are part of the implementation process. Technology can automate many processes, but humans are intrinsic to their execution, and intentional or unintentional deviation from processes lie at the root of many breaches.

## DON'T THINK COMPLIANCE, THINK SECURITY

Key conclusions from a wide body of research include the following:

- Many retailers have devoted disproportionate resources to PCI over to the detriment of other security priorities, or assembled an array of point solutions that leave dangerous gaps in coverage. Evidence is ample that, even after a months-long audit, attaining PCI-DSS compliance certification does not even guarantee that the enterprise was completely compliant at that moment, and change within the enterprise and in PCI regulations themselves is inevitable.
- Retailers must adopt the mindset that data security is a critical and constantly moving target, and devote sufficient resources to developing a comprehensive framework to continually assess and address risk.
- A comprehensive plan also helps retailers comply with other data privacy laws.
- Security best practices call for approaching the task systematically, starting with an assessment data, channels, networks and users, formulating policies, developing and deploying an integrated technology plan, then predicting, monitoring and measuring on an ongoing basis.
- A comprehensive plan can reduce costs by abandoning a patchwork approach and enable innovation by providing a secure environment in which to develop new initiatives.

---

### ABOUT MOTOROLA

Motorola is known around the world for innovation in communications and is focused on advancing the way the world connects. From broadband communications infrastructure, enterprise mobility and public safety solutions to high-definition video and mobile devices, Motorola is leading the next wave of innovations that enable people, enterprises and governments to be more connected and more mobile. Motorola (NYSE: MOT) had sales of US \$30.1 billion in 2008. For more information, please visit [www.motorola.com](http://www.motorola.com).

---

Sponsored By:



**MOTOROLA**