CROSSVIEW™

Security
PLAYBOOK

OVERVIEW

Today, security threats to retail organizations leave little margin for error. Retailers face increasingly complex security challenges – persistent threats that can undermine the success and longevity of a retail brand. Data protection, transaction security and compliance are just some of the high-stakes challenges retailers must address head on – particularly in a cross-channel commerce environment.

Many retailers struggle to:

- Prevent data breaches and keep the company out of news headlines.
- Minimize costly system downtime due to security issues.
- Achieve, maintain and demonstrate compliance and avoid penalties.
- Manage security with improved visibility, control and efficiency.
- Align security with the business to truly reduce risk and improve sustainability.

To address complex challenges, your retail enterprise security must incorporate constantly evolving technologies and technical disciplines. CrossView offers an array of security services that offer preemptive protection integrated with existing IT business processes to help strengthen your commerce infrastructure. Our services address multiple facets of security, including: physical, data and identity, application, and infrastructure.

What differentiates CrossView is our ability to deliver a robust portfolio of security services for all retail touchpoints – in store, over the web, through call centers, via mobile devices and more. As a premier provider of cross-channel commerce solutions, our expertise not only embraces all facets of the cross-channel experience, including strategy, technology and security, but extends throughout the lifetime of your investment.

"With just 10,000 customers in your database, the cost of a data breach averages more than $2 million."

– Michael D. Peters, MBA, CISSP, CRISC, CISM, CMBA, CCE – Chief Information Security Officer, CrossView

A Comprehensive Portfolio

CrossView provides a comprehensive portfolio of security services extending across the complete lifecycle of your commerce systems and strategy. From source code to professional managed services, whether you are focused on a single sales channel or you serve customers across multiple channels, CrossView Security Services identify, manage, monitor and resolve security threats, and preserve your most valuable assets – your customers and your brand.

CrossView Security Services cover a wide range of areas, including:

- Cloud-based application, server and data security
- Data protection
- Cross-channel security best practices
- Online transaction security
- Information security policies and procedures
- Cross-channel risk management
- Vulnerability assessment and management
- Emerging threat evaluation
- Security configuration management
- Security audits
- Disaster recovery strategy
- Business continuity
- Security business process development and management
- Compliance

Project Implementation Security Services:

- Code certification
- Segregation of duties
- Best practices for secure software development and delivery
- Application vulnerability assessment and certification
- Environment vulnerability assessment and certification

Professional Managed Security Services:

- Application vulnerability assessment and certification
- Environment vulnerability assessment and certification
- Path and update software security certification
- Software Development Life Cycle (SDLC) security certification

"A substantial number of data breaches have occurred over the last five years, despite compliance with the industry standard. There will need to be a move to a higher level of security, and the major challenge is institutional."

– Mark MacCarthy, Stanford Technology Law Review

PCI DSS: Achieving Compliance

Customer loyalty hinges on the expectation of a secure shopping experience and protection of private data. Retailers accumulate vast amounts of highly sensitive, customer-specific data. But safeguarding it can present a significant challenge. In fact, data breaches and credit card fraud continue to grow at an alarming rate.

CrossView Security Services can help you reduce the cost and complexity of protecting customer information with services that allow you to secure data, and achieve compliance with all retail data privacy mandates, including the Payment Card Industry Data Security Standard (PCI DSS).

Industry standards such as PCI DSS, along with government regulations, and security best practices require retail organizations to adopt encryption of sensitive data, both in transport across the Internet, and as it is stored and shared within an organization.

CrossView can help you achieve and maintain compliance and, more importantly, protect the information customers entrust to you in every transaction – every interaction.

"The rapid deployment of new mobile payment technologies has brought a level of complexity to the industry never seen before. This and the resulting influx of mobile payment applications introduce a new set of risks and threats that may affect the security of cardholder data."

internet® RETAILER

– Bob Russo, General Manager of the PCI Security Standards Council

Article: http://www.internetretailer.com/2011/03/31/mobile-payment-applications-need-second-security-check-pci-says

Get it Together

An integrated approach to security helps ensure that an organization's information resources and critical infrastructure are protected. This is the consensus from interviews with security leaders from 59 different organizations surveyed by Poneman Institute, the pre-eminent research center dedicated to privacy, data protection and information security policy.

Findings include:

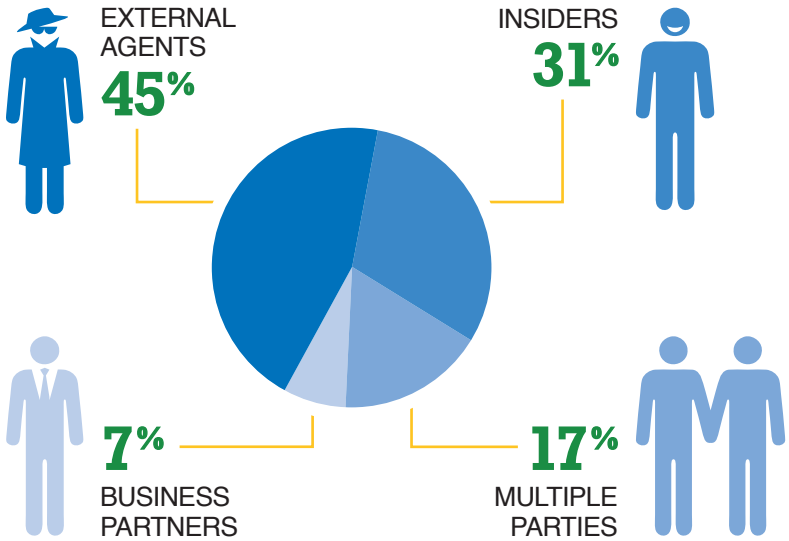
- *90% of study participants agreed or strongly agreed that aligning security with explicitly defined business objectives is the single most important purpose of a security strategy.*
- *The most important priorities for a successful security strategy are to focus on people (42%), technology (39%), processes (14%), and policies (5%).*
- *71% of study participants agreed or strongly agreed that security objectives must be flexible, and that rigid objectives may stymie operations.*
- *75% of participants agreed or strongly agreed that collaboration between departments and business units is essential to achieving security objectives.*

Source: Security, Integrated & Holistic: Benchmark Study of IT Security Leaders, Ponemon Institute

Security Assessments

CrossView security and compliance assessments of your applications, point-of-sale systems, governance and IT controls offer a better understanding of potential threats. CrossView can make you aware of problems before auditors and establish a roadmap to resolve security vulnerabilities.

WHO IS BEHIND DATA BREACHES?



Source: U.S. Secret Service Data Breach Report

"The average organizational cost of a data breach increased to $7.2 million and cost companies an average of $214 per compromised record."

– The Poneman Institute

Study: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf

CrossView: Trusted Partner, Valuable Expert

Keeping pace with ever-evolving security threats that put retail enterprises at risk can be costly. Enterprise security is a 24x7 proposition that includes identifying and monitoring potential threats, device management over a diverse IT landscape, and the creation and enforcement of security policies that can impact employees, vendors and customers.

Moreover, effective security requires highly skilled personnel – experts who can be expensive to recruit, hire and retain. For many companies, the solution is turning to a trusted partner such as CrossView to share the benefit of robust skills, vast industry expertise, proven methodologies and deep insights into the world of retail, commerce solutions.

CrossView can help you:

- Manage and resolve security and compliance issues across all sales channels.
- Protect retail assets with end-to-end solutions and services.
- Manage customers' transactions across multiple channels, while protecting privacy and transaction integrity.
- Assist with achieving and maintaining PCI compliance.
- Define and enact effective security policies, and put in place technologies to enforce these policies.

"Organizations that engage third parties to assist in the response and compliance following a data breach actually spend much less per record compromised ($170 versus $230)."

Ponemon INSTITUTE

– The Poneman Institute

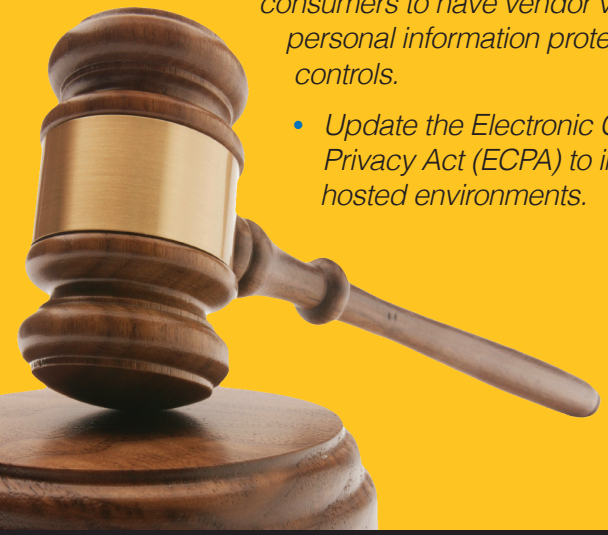
Study: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf

Privacy as Policy

The U.S. Commerce Department has proposed establishing a Privacy Policy Office (PPO) to serve as a center of commercial data privacy expertise.

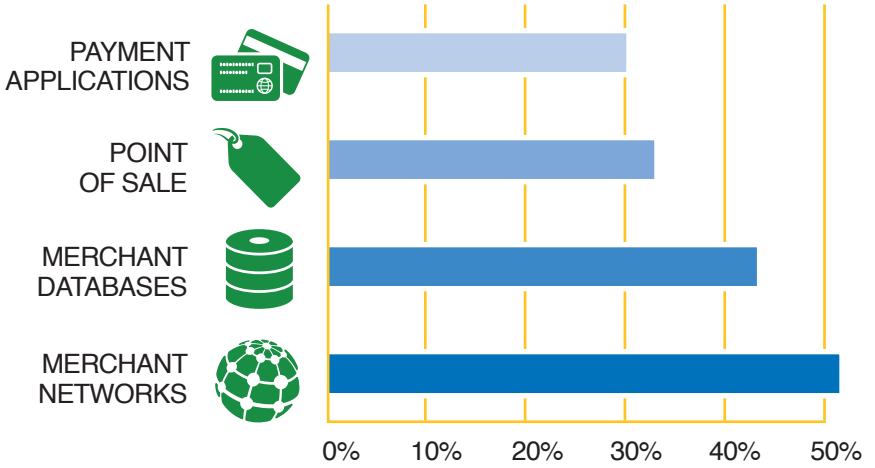
This is likely to result in more legislative requirements imposed upon retailers and commerce companies, including:

- *Increased corporate disclosure requirements.*
- *Breach notification requirements.*
- *Consumer privacy technologies allowing consumers to have vendor verification of proper personal information protections and usage controls.*
- *Update the Electronic Communications Privacy Act (ECPA) to include cloud and hosted environments.*



CrossView Security Services can help resolve retailers' security and compliance issues holistically. The approach is to address and manage the multiple dimensions of security across people and identity, data and information, application and process, IT and network, and physical infrastructure.

SYSTEMS MOST AT RISK FOR CARDHOLDER DATA BREACHES



Source: PCI-DSSS Trends, 2010, Poneman Institute

"The potential damage to brand, business reputation, and revenues mandates that data security is no longer optional – it is more essential than ever before."

– Michael D. Peters, MBA, CISSP, CRISC, CISM, CMBA, CCE – Chief Information Security Officer, CrossView

Seeing the Complete Picture

To get a full picture of where your retail enterprise stands in relation to threat vulnerability, you need to understand the weaknesses in your IT infrastructure and address the potential problems. Consider these critical areas where CrossView offers assistance:

- **Finding the gaps.**
  Our information security and application assessment services can help evaluate the security of specific applications, an entire network or your overall organization. These can vary from one-time benchmarking for gap analysis to regularly scheduled events that ensure that you are maintaining your security goals.
- **Defining the plan to close the gaps.**
  Policy development, regulatory compliance and implementation planning help you determine how to move from your current level of security to your desired state of protection.
- **Protecting ahead of the threat.**
  Having a good security application or platform in place before handling large amounts of customer data can protect your network and servers and the applications that access them.
- **Ensuring that gaps remain closed.**
  Consistently monitor and manage your security devices and applications, ensuring that they are updated, that you are protected and that an intrusion is not taking place.
- **Developing business continuity plans.**
  Have a recovery plan in place for unexpected outages or interruptions.

"It is especially incumbent upon suppliers to provide inherently secure applications, security-focused implementation services, and aggressive, ongoing security support services to commerce-based companies."

– Michael D. Peters, MBA, CISSP, CRISC, CISM, CMBA, CCE – Chief Information Security Officer, CrossView

CrossView Insight

Data Security & Mobile

As retailers create more robust cross-channel experiences that include mobile commerce and selling through social networks, existing payment data security solutions need to be extended to embrace these game-changers.

The growth of mobile point-of-sale devices requires the protection of wireless data transmissions and managing access to the mobile devices themselves. Because individual devices may be lost or stolen, for instance, sensitive data cannot be retained on these hand-held devices.

The fact is that as shopping evolves – and technology along with it – cybercriminals are becoming smarter and bolder. Retailers are facing new and more complex challenges when it comes to outwitting these tech-savvy criminals.

To closely protect customer data, payment data security needs to be part of a robust enterprise-wide approach to security. Many retailers have focused their security efforts on PCI, but most experts agree that achieving PCI compliance does not necessarily equate to data security. More than 45 million customer credit card numbers were stolen from TJX Companies in the largest known data breach in retail history. What this illustrates is that vulnerability exists even among retailers that are in full compliance. PCI compliance is a starting point – not the end of the story. Protecting payment-related data needs to be a top priority in any retail organization.

Security Solutions

Are Your Doors Locked?

The best security solutions are a combination of the right tools – locks on the doors, so to speak. Consider these actionable steps for increased data security:*

- *Assemble a team of experts (internal and external) to work together toward a common objective of creating the "best" solution.*
- *Conduct a data mapping exercise to identify and document the location of all credit card and personal information.*
- *End to End encryption, starting at the network edge (MSR) and terminating outside the retailers' walls.*
- *Tokenization to protect data at rest and allows complex back office systems to function with minimal change.*
- *Run a data leakage tool or analysis to ensure that the steps above found and eradicated data at risk*

The Last Mile

"End-to-end encryption is typically defined as starting at the network edge and terminating outside retailers' walls. My definition starts with the point of transaction, such as a POS terminal or shoppers browser, and terminates with the acquirer. The 'last mile' cannot be forgotten. Sensitive data that remains from tokenization processes or from local data storage must be encrypted."

Michael D. Peters, MBA, CISSP, CRISC, CISM, CMBA, CCE – Chief Information Security Officer, CrossView

** Source: Association for Retail Technology Standards (ARTS), a division of the National Retail Federation (NRF).*

How We Work With You

As part of our managed services model, pre-allocated hours each month give you immediate access to CrossView security skills and expertise.

Our flexible delivery model can be adapted to the specifics of your project – whether we're collaborating with your team on a short-term security engagement or taking full responsibility for implementing and managing your security solutions on an ongoing basis.

CrossView builds, deploys, executes and manages winning cross-channel strategies and solutions, and delivers comprehensive security services that keep your cross-channel retail enterprise safe and compliant.

CrossView Security Services is led by Michael D. Peters, Vice President - Chief Information Security Officer (CISO), an industry-recognized expert who brings extensive security knowledge across multiple industries, including retail, military/defense, education, software development, manufacturing, transportation, healthcare, insurance, energy, financial and technology sectors.

We deliver comprehensive security services that keep your cross-channel retail enterprise safe and compliant.

CROSSVIEW™

Learn More

To learn more about CrossView's Security Playbook, contact:

Michael D. Peters *Chief Information Security Officer*

(706) 568.7722

(762) 822.4174

email

Michael D. Peters leads all aspects of Information Security, Cloud Security, IT Risk, Change Control and Compliance, Threat and Incident Management, Business Continuity, Disaster Recovery, management, and security strategy for CrossView. As an IT security professional, he has worked as an independent information security consultant, researcher, author, and catalyst, and has more than 25 years of information technology leadership experience.

Prior to joining CrossView, Michael was the Chief Security Officer for Fifth Third Processing Solutions, Chief Information Security Officer for BB&T BANK and Colonial Bank, and served in leadership roles in many Fortune 50, 100, and 500 companies across multiple industries. Presently, he holds a certified MBA in IT Management, BS in IT Security, CISSP, CRISC, CISM, CCE, CMBA, SCSA and is an ISSA Fellow. Michael is completing his final year of law school earning a Juris Doctorate focused on federal and international cyberspace law.

About CrossView

CrossView is a pioneering provider of cross-channel commerce solutions that empower organizations to deliver an integrated consumer experience and optimize transactions for all customer touch points. The cross-channel solutions we provide enable multi-channel organizations to transform their businesses by providing an integrated cross-channel platform which provides three major benefits: customer responsiveness, operational efficiencies and a lower total cost of ownership. *email us*

David Lebowitz *Vice President of Sales*

Dave Lebowitz uses his exceptional sales, technical, and marketing skills to identify and close revenue opportunities. With over 12 years of experience with IBM, Dave brings extensive expertise in designing and selling integrated e-commerce solutions while consistently meeting and exceeding revenue targets. He has developed relationships with large and midmarket clients such as Sears, BassPro, Fossil, Walt Disney, Hallmark, Home Depot, and many others. Dave holds a BS in Management Science from Southern Methodist University.

To learn more about CrossView, visit our website:

CROSSVIEW™

www.crossview.com