Gold Sponsor

Diebold Nixdorf

2019 SPECIAL REPORT: Security

SECURITY KEY FINDINGS

CUSTOMER EXPECTATIONS

RETAILER CAPABILITIES

33% are likely to allow retailers to save credit card details if it eases the checkout process

→ **61%** have implemented end-to-end encryption to offer customers greater security of their personal and payment data

50% are likely to allow retailers to save personal details if it eases the checkout process and allows for more personalized offers

→ **38%** have implemented a single token solution across the enterprise to offer customers greater security of their personal and payment data

38% are likely to choose a store if it offers mobile wallet/payments

→ **59%** offer mobile payment acceptance

Based on findings from BRP's 2019 POS/Customer Engagement Survey and the BRP Consumer Study.

Secure your most valuable asset

Technology is bringing new life to brick-and-mortar stores as the physical and digital worlds collide. The physical store is transforming to adapt to new technology and rising customer expectations to add value beyond simply offering merchandise – it now must offer a truly personalized experience to remain relevant.

With personalization also comes the need to gather, analyze and protect customer information to offer contextual offers and suggestions. Consumers expect that retailers will protect their data to ensure a safe and personalized experience. While consumers in the BRP Customer Study indicated they would allow a retailer to save personal information if it helped ease the checkout process and offer personalized offers and recommendations, there are limits to what they want to share. Half of consumers are likely to allow retailers to save purchase history, personal preferences and personal details but they are less likely to allow retailers to save credit card details (33%).

In the wake of major data breaches, retailers must continuously reexamine their policies surrounding cybersecurity. Every day, new dangers seem to emerge and enhanced security measures are necessary to adequately defend against these malicious attacks. A single security breach is enough to deal a crippling blow to many companies. Therefore, a fortified multi-tiered defensive cybersecurity strategy is more important than ever before.

Adding to the security and risk complications retailers are facing is the continuing flood of consumer data protection legislation. One thing in common across this legislation is the large fines and fees that are associated with noncompliance. The recent enactment of the General Data Protection Requirements (GDRP), which impacts U.S. retailers, has started a ground swell of similar legislation in many states.

The ***SPECIAL REPORT: Security*** is based on findings from the BRP Consumer Study and the 2019 POS/Customer Engagement Survey. To download the POS/Customer Engagement Survey visit https://brpconsulting.com/download/2019-pos-survey/

Unfortunately, many retailers remain vulnerable to potential hacking threats, with key areas of susceptibility being sensitive data encryption, retention and payment card authentication. In addition, with the migration of critical enterprise systems, transactional data, and customer data to the cloud, it is imperative that retailers continuously evaluate their network, controls, and security processes as it relates to this shift.

Industry best practices dictate that the most effective strategy is a multi-layered security approach. There are a large number of security and data protection practices that each retailer must consider. Many of them are specific to their business processes, employee authentication and the types and amounts of customer data they store (or want to store). The following is a combination of measures that apply to almost all retailers and will help ensure that your customers' payment and personal data is protected:

- End-to-end encryption (E2EE) starting at the time of card swipe or data entry in the mag head/chip reading device and ending with a single decryption point at the processor
- Tokenization at the earliest point possible outside of your environment and for all data at rest

- EMV technology to validate payment card authenticity for in-store purchases
- Fraud prevention tools to help reduce risk and fraudster activity for online purchases
- Storing customer data once, encrypting it, and then using a customer ID or token in other systems where the information is needed

As significant financial harm and negative publicity from a data breach can adversely affect consumer perception and loyalty, it is now critical for retailers to defend themselves and their customers against potential security breaches. Examining the adequacy of current information security practices must be a top priority. Sufficient budget resources and funds should be dedicated to the identification and implementation of measures to protect the valuable consumer data your organization processes every day.

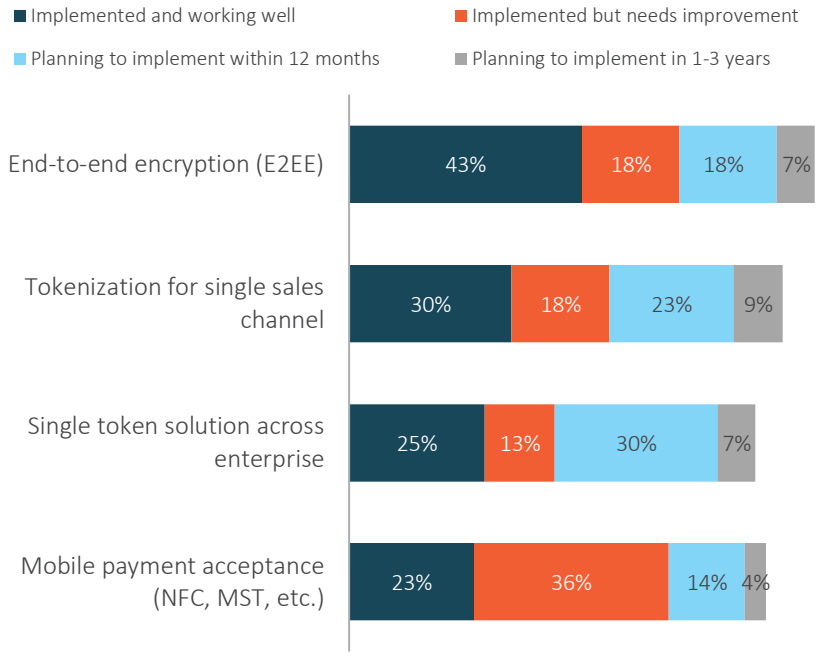
Encryption

The first major line of defense in securing customer data is end-to-end encryption (E2EE). E2EE has increased significantly over the past few years with a reported 61% of retailers utilizing it (Exhibit 1). E2EE prevents third parties from accessing data throughout the system because only the authorizing parties have access to the encryption keys.

Tokenization

The next protective layer involves tokenization, which enables retailers to remove sensitive information from the network by substituting payment card data with a token which is used as an identifier but has no exploitable value or meaning. 38% of retailers have implemented a single token solution across the enterprise, with

Exhibit 1
Payment Security Technology Plans



an additional 37% planning to implement within the next three years. This technology is critical to offering customers a single unified commerce experience for returns, customer profiles and electronic shopping carts that need to retrieve data across channels.

Moving store applications to the cloud makes security easier, as customer and associate information resides at a data center or home office instead of at the store-level. Securing data in one place is safer than securing data at every store and if retailers utilize encryption and tokenization there is no critical information residing at the store.

Leading retailers have already reduced the friction in omni-channel transactions by implementing a payment token that can be leveraged across all channels. Tokens, which are a key cornerstone of a payment security strategy, should also be seen a critical component in facilitating omni-channel transactions including, BOPIS, cross-channel returns, mobile wallets, and endless aisle transactions.

Data Rationalization and Reduction

Many retailers have customer data stored in dozens of online data stores, secondary spreadsheets and local analytical databases. This poses a major risk to retailers and should be addressed immediately to reduce risk and enable compliance with many of the new laws now in effect. Immediately identifying all of the points that customer data is stored within the enterprise and then tokenizing and rationalizing it, is the next major hurdle for many retailers and should result in a focus similar to that applied to payments data.

Payment security will remain a concern for retailers for the foreseeable future. Most of the retailers involved in the 2019 POS/Customer Engagement Survey reported moving towards a security plan with multiple layers to protect sensitive customer and organization data.

Mobile wallet security efforts

Mobile wallet/payments offer further opportunities for customers and retailers, as it enables customers to make purchases without their wallet (but with their ever-ubiquitous smartphone) and provides an additional level of security that isn't available with credit cards, even EMV-enabled cards.

Mobile payments in stores should use tokenization so that the retailer never actually has the customer's payment card number, which significantly reduces the security risk and speeds up transactions.

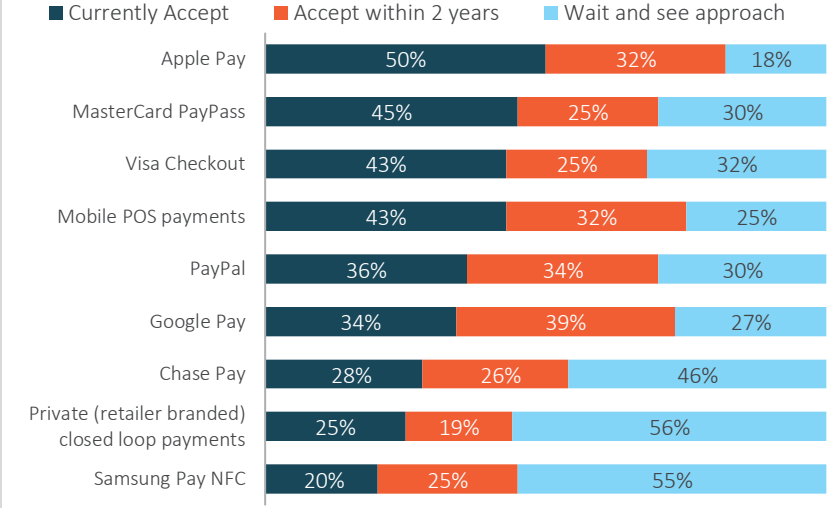
There are many mobile wallets and payment apps in the market today. In addition, various retailers are offering their own mobile payment options. In the store environment, many retailers continue to focus on private label credit cards to reduce interchange fees and processing time at checkout. A new entrant to the field, launching this summer, is Apple Card which offers a new kind of mobile payment opportunity.

PayPal and Apple Pay continue to be the most widely alternative accepted alternative payment types in this survey (Exhibit 2). This year fewer retailers are adopting a wait and see approach across the board – likely because of the growing support from the payment software ecosystem (including payment switch providers and card processors), and the increased adoption of mobile payment usage by consumers.

One critical factor for mobile payment success is education and training. We have found repeatedly that not only are most consumers unsure of how, when and if mobile payments can be used, but even more telling, associates are unsure. For mobile payments – or mobile wallets – to succeed, there must be further education at the point of sale to ensure that a transaction using a mobile device is no longer or more complicated than traditional payment methods for either the customer or associate.

While the pros and cons of each of these payment types – and future payment types – can be debated, what is most apparent is the adoption across the industry as customers and associates become more comfortable utilizing these emerging payment platforms.

Exhibit 2
Alternative Payment Types



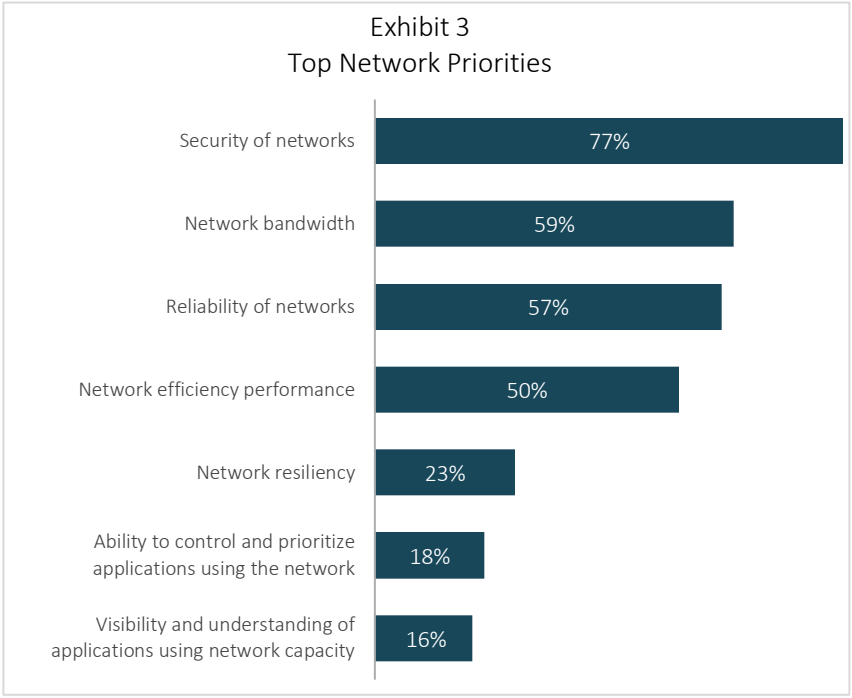
Network security is critical

Today's stores require a secure environment beyond retailers' current payments and network security. Retailers need to strike a balance with consumers between gathering information and maintaining trust. As retailers seek new ways to provide relevant information and experiences, like product recommendations via digital screens in the dressing rooms or facial recognition alerting an associate to a shopper's arrival, they must understand the impact on the customer relationship.

While additional information offers a more personalized experience, it also provides a greater opportunity for data theft and fraud. While retailers are focused on the security of their networks, with 77% indicating this is a top network priority (Exhibit 3), retailers need to also establish security policies that ensure the data privacy of their customers' information. The General Data Protection Regulation (GDPR), which became effective in May 2018, mandates the need for security policies, data monitoring, and purging functions related to customer data. Consumers want retailers to understand them as individuals – not put their personal information at risk.

While the attention of IT resources and business owners are occupied with the challenge of executing initiatives to drive store transformations, extra focus on security is imperative as the implementation of each additional touch point increases the threat of security breaches. In the current hyper-connected technology and media environment, it's not enough to satisfy security and compliance requirements. Organizations need to clearly understand their security risks, be prepared to protect and prevent damage to their most valuable assets, and isolate and respond to threats as soon as they appear. With the move of many applications out of the physical store and into the cloud, the security of the network is more critical.

Exhibit 3
Top Network Priorities



The challenge lies in deploying a comprehensive security strategy that mitigates risk, while at the same time protecting and maintaining corporate advances in omni-channel initiatives. This will remain a hurdle amid growing customer expectations of a seamless experience across all retail touch points. The development of this strategy is critical, and must incorporate industry best practices in order to ensure an appropriate balance is struck between the customer experience and data security.

About BRP

BRP is an innovative retail management consulting firm dedicated to providing superior service and enduring value to our clients. BRP combines its consultants' deep retail business knowledge and cross-functional capabilities to deliver superior design and implementation of strategy, technology, and process solutions. The firm's unique combination of industry focus, knowledge-based approach, and rapid, end-to-end solution deployment helps clients to achieve their business potential.

BRP's consulting services include:

- Strategy
- Point of Sale (POS)
- CRM
- Order Management
- Supply Chain
- Business Intelligence
- Mobile POS
- Unified Commerce
- E-Commerce
- Networks
- Business Process Optimization
- Payment Security
- Customer Experience & Engagement
- Merchandise Management
- Private Equity

For more information or assistance on any of the topics covered in this white paper, please contact:

Brian Brunk, Principal
(405) 590-0542
Brian.Brunk@brpconsulting.com

Perry Kramer, SVP and Practice Lead
(617) 899-7543
Perry.Kramer@brpconsulting.com

David Naumann, VP of Marketing
(916) 673-7757
David.Naumann@brpconsulting.com

Ken Morris, Principal
(617) 880-9355
Ken.Morris@brpconsulting.com

Ryan Grogman, SVP and Practice Lead
(972) 365-0257
Ryan.Grogman@brpconsulting.com

Kathleen Fischer, Director of Marketing
(330) 289-3342
Kathleen.Fischer@brpconsulting.com

BRP
Atlanta | Boston | Chicago | Dallas | Denver | San Francisco
www.brpconsulting.com