CLOSING THE GAP ON THE BLACK HATS: FUTURE-PROOFING PAYMENT SECURITY
Maturity Ladder: Future-Proofing Payment Security

The RIS News Retail IQ Report Maturity Ladder is a diagnostic measurement tool for a retailer’s state of technology advancement in a specific category. There are four key phases: 1. Basic – minimal capabilities, 2. Intermediate – mostly basic with some advanced capabilities, 3. Advanced – mostly advanced capabilities with some limitations, and 4. State-of-the-Art – comprehensive capabilities are fully integrated and up to date. Note that it is possible to be on more than one step of the ladder simultaneously as specific technology components and processes are upgraded in phases.

1. Basic
- Retailers begin to adopt business operations and “future-proof” their organization by adopting omnichannel business models that support “connected devices” and web-enabled strategies.
- Retailers’ existing legacy systems are not robust or secure enough to handle increasing web-enabled processes and supporting devices.
- Retailers are susceptible to new vulnerability points, both conventional and unconventional, throughout the retail enterprise.

2. Intermediate
- Omnichannel operations become mission-critical, forcing retailers to transition legacy-based systems and networks to more agile infrastructures.
- Retailers transition to wireless and broadband networks, leaving connections and WiFi access points vulnerable to potential attacks.
- Retailers begin accepting mobile wallets. The evolving payment option lacks standards, making retailers susceptible to fraud.

3. Advanced
- Retailers remediate networks to comply with the Payment Card Industry Data Security Standard (PCI DSS) and the Europay, MasterCard, Visa (EMV) Liability Shift Mandate.
- Savvy retailers use industry data breaches as learning tools to improve their own security processes and operations.
- Retailers secure next-gen mobile payments options by adhering to PCI DSS and EMV guidelines.

4. State-of-the-Art
- Retailers adopt new payment terminals designed with end-to-end encryption and tokenization functionality, both of which protect customers and sensitive information.
- Integrated device management systems monitor device usage, and potential failure points, among other key performance indicators.
- Cloud-based security solutions identify vulnerabilities, monitor unauthorized access to cloud repositories, as well as block threats on cloud networks in a more cost-effective, scalable manner.
Becoming an omnichannel player goes far beyond providing a seamless shopping experience. Behind the scenes, new networks are required to support evolving business processes, new digital touch points and channels, and evolving payment options.

However, weaknesses among these new networks are attracting menacing hackers, and encouraging a new wave of cyber-threats. Eager to protect their networks — and future-proof their businesses — retailers are leveraging innovative solutions, including new industry standards, integration methods, and virtual security solutions.

Omnichannel retailing is synonymous with convenience — granting shoppers access to their favorite brands via new business channels, digital touch points, and electronic payment options. Described as a multichannel approach to sales, this all-encompassing process is designed to deliver a seamless shopping experience that enables customers to “channel-hop” between e-commerce, mobile commerce, call centers and physical store locations as they research, choose and procure merchandise.

Omnichannel retailing success also requires a network infrastructure designed to connect business channels, both virtual and physical; share business and customer data between digital touch points; and process evolving payment options. Besides making the always-on retailing model increasingly complex to manage, these new factors expose the network to more security threats. The top challenges include:

- **Legacy Network Infrastructures.** Retailers are quickly learning that the retail experience is now in the shoppers’ hands. They expect to use tools — both on their own and on their favorite retailers’ behalf — that will simplify and speed up the shopping experience. Realizing their consumers’ preferences are always subject to change at a moment’s notice, retailers are quickly learning that their legacy networks are not adequate enough to support these demands. Oftentimes, they fail to satisfy on-demand availability; create an unbalanced data flow stemming from a variety of sources; and most importantly, fail to automatically scale resources as demand increases.

  “Legacy systems that are not designed to accommodate today’s retail environment [force] retailers to scramble to cobble things together in the...
attempt to deliver the omnichannel capabilities customers expect,” Ken Morris, principal, Boston Retail Partners, said in the “2016 POS/Customer Engagement Benchmarking Survey,” from Boston Retail Partners. “The risk of losing customers due to disappointing shopping experiences caused by flawed omnichannel architecture is deadly.”

Omnichannel operations collect an abundance of sensitive customer and business-specific data, and it is filtered in and out of every mission-critical operational solution. However, when legacy systems manage these day-to-day operations, they rely on very different, rigid code compared to modern web-based, firewall- and password-protected solutions, making them an unprotected and vulnerable asset in data centers. And with 72.5% of companies still operating among absent or underdeveloped capabilities needed to support an end-to-end, cross-channel shopping experience, according to “A New Era for Retail: Cloud Computing Changes the Game,” a report from Accenture, the landscape is ripe for havoc.

Mobile Payments. Payment options have come a long way in the last decade. An era defined by cash, check and credit card based products has been expanded. While traditional payment methods are still viable and widely used, new payment options, including debit and electronic gift cards have increased exponentially.

Over the last year however, another new option has emerged: mobile wallets. A product that electronically stores users’ debit and credit card numbers, digital wallets enable consumers to tender orders directly through their personal smartphones via near-field communications (NFC) processes. And as new players including mobile operators, hardware developers, payment issuers and processor segments join forces, the mobile payment ecosystem continues to heat up.

Retailers have learned the more mobile wallet products they can accept and process, the more consumers they can attract and retain as loyal shoppers. Consider SPAR UK, a British convenience supermarket chain that was bombarded with consumer demand for more sophisticated payment methods, including the ability to use mobile wallets — specifically Apple Pay. To make the transition, SPAR retired its antiquated PIN payment terminals in favor of new devices that support NFC and contactless payments.
Q: When it comes to securing network peripherals, what are the vulnerable points that retailers often forget?
CLIFF DUFFEY: WiFi is often inadequately secured, creating entry points into the network. This is troubling given WiFi is the transport medium for so many applications, including payments and loyalty, carrying sensitive cardholder data, making it prone to attack. IoT and always-connected devices create the perfect storm by exposing more inadequately secured network entry points.

Q: How have new innovations, such as IoT and constantly connected devices, further created vulnerability points that need to be protected?
DUFFEY: Most businesses approach security with an outdated network construct — assuming well-defined corporate boundaries. IoT and constantly connected devices compromise perimeter-centric security postures. Moreover, IoT security is a moving target because it is immature and non-standard, with each device manufacturer creating its own proprietary security mechanism with varying levels of security robustness and complexity of configuration. And finally, the always-on nature of many of these devices creates a “persistent” attack surface that needs to be monitored 24x7x365. Constant connectivity and evolving form factors demand a “zero-trust” security posture, meaning no default trust for any user, device, application or network traffic regardless of its location inside or outside the corporate network.

Q: How does end-point security differ from end-to-end segmentation?
DUFFEY: The primary goal of end point security is to protect against outside threats. In the event of a breach, these mechanisms no longer work because they are not looking on the inside to protection applications from each other. Contrast that with segmentation that assumes zero trust of all users, devices and applications regardless of location. The goal is to reduce threats so an entire site is no longer exposed, reducing the attack surface of a business. In segmentation, each application is isolated into its own dedicated logical network, preventing its traffic from mingling with other application traffic. Granular security policies can be defined on a per application basis, allowing the co-existence of mission critical applications like payments with public facing WiFi hotspots on a single physical network. By segmenting security policies for each unique device, security becomes simplified and networks less vulnerable.

Q: What role do VAN connections play in creating cost-effective, secure networks?
DUFFEY: Virtual Application Networks (VANs) are software-defined private area networks for each application. VANs create cost effective, simple and secure virtual networks that can be overlaid on any network with no redesign. Security is enhanced through the concept of end-to-end segmentation that enables application specific security policies. VANs eliminate the need for multiple, dedicated premise devices by integrating functionality such as WiFi, wireless backup, VPN, firewalls, intrusion detection, multi-factor authentication and security event management into a single device. This consolidated device removes the management complexity and integration associated with multi-box solutions. Moreover, security intelligence and automation is abstracted into the cloud so the retailer is left with a very simple lightweight device. The true impact of this paradigm shift is felt when secure application and policy enforcement can be achieved by in-store personal with no security or IT in minutes.

Cybera is a leading provider of secure virtual application networks to many top enterprises. It dramatically reduces customer cost and complexity by integrating cloud and premise-based security technology into a single, easy-to-use offering that can be installed within minutes with no security expertise and network re-design. http://rsa.cybera.com/
“The NFC and contactless enabled terminals combined with the managed service platform allows us to deliver a targeted and unique solution to our customers,” said Roy Ford, retail IT controller at SPAR UK.

In some instances however, this emerging payment option is becoming a new vulnerability point. Retailers need to adopt new software and hardware designed to accept these NFC-based payments, but oftentimes, NFC is subject to weak security controls. Specifically, criminals have uncovered NFC vulnerabilities in the account provisioning and verification processes, enabling them to commit fraud, according to a joint advisory bulletin, “Mobile Payment System Vulnerability,” from the U.S Secret Service, in collaboration with the Payment Card Industry (PCI) Security Standards Council.

Add in the complexity of smartphones and wearables facilitating cardless electronic payments, and cyber-thieves have a new frontier to claim customer-specific information. While this information can be manipulated in various ways, many cyber thieves use this stolen information to create fake accounts on NFC devices, and make illicit transactions both online and in the brick-and-mortar environment.

**Peripheral Hardware Solutions.** When retailers become targets of data breaches, consumers can’t help but wonder how well their favorite brands are protecting their personal information — especially with identity theft on the rise. The Federal Trade Commission (FTC) received 490,220 consumer complaints about identity theft in 2015 — a 47% increase over 2014, according to “Identity Theft Reported to the FTC,” a report from the FTC.

While retailers are taking new measures to protect consumer data across anticipated exposure points, too often they forget vulnerable points that have become prerequisites in the all-channel shopping journey. Consider Target, the unfortunate owner of one of the industry’s most highly-publicized data breaches. Thieves entered the retailer through virtual private network (VPN) credentials lifted by a third-party heating and air conditioning (HVAC) firm, and then successfully pushed malicious software to payment terminals across the enterprise. These cyber-thieves claimed 40 million credit card numbers and 70 million additional customer records.

Casey’s General Store found itself in a similar situation when criminals
compromised the over 1,800-strong convenience store chain via its fuel pump readers. Connected to the company’s network, devices across six Casey’s stores in Nebraska and one store in Iowa were installed with credit card skimming devices, giving cyber thieves immediate access to vulnerable information.

Both examples illustrate how important it is to protect any enterprise device, no matter how critical or supplemental, that interacts with customers, or transmits sensitive information — two factors that need continuous protection.

**WiFi Connections.** Whether supporting customer engagement, running in-store software applications, or supporting in-store mobility, WiFi is becoming a mission-critical architecture. In fact, 53% of companies are currently deploying WiFi access points, and 33% will follow suit over the next two years, according to “Building a New Digital Foundation for Retail and QSR with Wi-Fi,” a report EKN Research.

WiFi successfully supports the increasingly seamless shopping experience, from mobile channels and mobile wallets to in-store applications, such as loyalty, inventory management, and internal human capital management solutions — all processes that manage sensitive cardholder data.

Stores that unwittingly support unprotected or minimally-protected WiFi access points are creating vulnerable entry points directly into the general network.

**Keeping Pace With Cyber Thieves**

The sobering truth is that data breaches are a scary and seemingly unavoidable cost of doing business. The annual cost of card fraud in the United States is estimated at $8.6 billion, and this figure was expected to rise to $10 billion or higher by the end of last year, according to “State of the Industry Research Series: 2015 Retail Point-of-Sale Blueprint,” a report from EKN Research.

Highly-sophisticated cyber-thieves are armed with the resources and technical expertise needed to infiltrate any potential vulnerability, and perpetuate even more devastation. With every data breach the industry gains exposure to the limitations of the current data security landscape,
Q: What are the trends shaping retailers’ security decisions?

ROBERT McMILLON: I think the trends that are facing retailers today are the same that have been in front of them for the last couple of years: staying out of the headlines, and playing catch up with changing regulatory requirements. For the last several years, the payment industry has been talking to retailers about P2PE, tokenization and EMV. We are still early in the adoption curve of all three technologies. I think this will probably be the big trends for the next few years still. However, the payment industry isn’t standing still. We see new entrants and new technologies trying to influence the way consumers and retailers interact. These increased commerce interactions obviously carry new benefits for the retailers, but they also open new avenues of risk. I think the next wave of security related discussions will be centered on the changing way in which retailers and consumers interact.

Q: What is the difference between integrated payment security and semi-integrated payment security?

McMILLON: Integrated versus semi-integrated is related to the point of origination of the payment message. In the integrated model, the payment terminal is used simply for data capture. The payment data is sent to an ECR or point-of-sale, and that device creates the payment message that is used as a request for authorization, with the ECR handling the sensitive payment data. Most of the major retail breaches have been related to a compromise of the ECR.

In semi-integrated, the responsibility for creating the payment message stays with the payment terminal. The flow is essentially reversed, and the ECR sends the information relevant for the creation of the payment message to the terminal. The terminal takes that data, captures the card information, and then formats and creates the payment message inside of the secure, purpose-built hardware. The card information is never shared outside of the secure hardware.

The semi-integrated model greatly eases the certification burdens. Many people don’t realize that EMV introduced vast new certification requirements into the payment ecosystem. Semi-integrated systems help to ease the burden by reducing the number of certifications required in the system.

Q: How is e-commerce impacting payment security, and what steps will retailers need to take to secure card not present payments online?

McMILLON: Huge advancements related to consumer authentication, tokenization, shipping verifications, etc. have all made shopping online a much safer place than it used to be. The next challenge area will be omni-commerce, where the consumer is able to cross shopping channels seamlessly. In many ways, I think this signals one of the upcoming changes in payments: a move from credential protection to consumer authentication.

Q: How are mobile wallets changing the payment security game? What can retailers do to prepare their systems?

McMILLON: Mobile wallets are merely another form factor. Obviously, the use of EMV tokenization on a mobile wallet provides additional protections for the consumer. However, it also introduces new challenges and new opportunities for the payments industry. For example, the use of EMV tokenization breaks consumer analytics for the retailer. In response, EMV Co introduced the Payment Account Reference (PAR) as a part of the last proposed update. The PAR provides a unique reference number for each account that is consistent across implementations (so you can perform analytics), but can’t be used for payment — so it is different than the token schemes we have seen for the last few years. It’s too early to make predictions about how retailers are going to need to change their systems, but I think it’s safe to say that changes will be coming over the next several years.
providing insight into just how far ahead the bad guys are in the security arms race.

Clearly, retailers have plenty of work to do if they are going to close the gap on the black hats. However, industry observers urge retailers to use the Payment Card Industry Data Security Standard (PCI DSS) as a guideline. While the PCI DSS roadmap centers on compliance as well as security, the standard can also act as a blueprint to “future-proof” systems in preparation of an inevitable attack.

Too often, merchants accept magnetic stripe cards or process “card not present” transactions via mail order, call center, or e-commerce without adhering to PCI standards, putting transactions — and customer data — at risk. As the omnichannel retailing model becomes mission-critical however, the data security standard (DSS) continues to provide controls to ensure the security of cardholder data across all retail environments, and throughout the entire transaction process, as summarized in “Increasing Security and Reducing Fraud with EMV Chip and PCI Standards,” a report from the PCI Security Standards Council.

PCI DSS should be used in concert with the adoption of the EMV Mandate. As of October 1, 2015, retailers are required to comply with a standard set of guidelines associated with accepting the proliferation of EMV cards containing microprocessor chips that create a unique code for each transaction. The mandate requires merchants to adopt new payment terminals that read the smart chip, as well as software and network security upgrades all designed to protect consumers’ payment card information. While all retailers strive to optimize the security of credit, debit and cash card transactions — and protect consumers’ personal information — only 18% of retailers met the October 2015 EMV deadline, according to “13th Annual Store Systems Study: Brave New World of Unified Commerce,” a report from RIS News.

While industry progress remains sluggish, both EMV and PCI DSS have forced brands to re-evaluate their current network security practices, and determine how efforts need to change in regard to connectivity and data security. “Direct fraud is on the rise,” said Larry Fretz, practice lead, gaming and hospitality, Info-Tech Research Group. “With compliance contactless payment trends and fraud pushing organizations to change,
now is the perfect opportunity to update POS systems and take advantage of new payment technology trends.”

**Securing Systems for Tomorrow**

A secure payment ecosystem is within reach as long as retailers adhere to industry standards. Retailers originally focused specifically on end point, or perimeter security, concentrating their energy to protect the enterprise against outside threats. Moving forward however, retailers must monitor the entire enterprise. This requires a process that moves away from a fully-integrated system and toward a semi-integrated model.

It is no secret that the POS is a preferred point of entry for data-hungry criminals, especially at a time when brands support integrated models. Historically, legacy payment terminals, whether POS devices or payment terminals, captured data, and a payment message requesting authorization was delivered via the network and back to the POS software. With that sensitive information floating around inside of PC-based systems, retailers remain at risk.

In an innovative move to ward off these attacks, more brands are transitioning operations to a semi-integrated model. Here, the data flow is essentially reversed, with the POS sending payment messages to secure, purpose-built hardware — a move that keeps card information specifically within the dedicated, secure hardware.

What makes these messages even more secure is the model’s reliance on tokenization. A process that encrypts sensitive data so only authorized users can read it via a dedicated decryption process.

Like most game-changing solutions, the pace of adoption is off to a slow, but steady, start. To date, 20% of retailers have adopted tokenization (16% claim it is working well, and 4% are making improvements), and another 52% will be implementing the service within the next 12 months-to-three years, according to Boston Retail Partners’ “2016 POS/Customer Engagement Benchmarking Survey.”

SPAR UK is one of these innovators. Its new NFC and contactless PIN terminals bundle hardware, software, gateway services, and end-to-end encryption, among other services. “The terminals, combined with the managed service platform, allows us to significantly reduce the threat of criminal attacks.”

**“Criminals have uncovered NFC vulnerabilities in the account provisioning and verification processes, enabling them to commit fraud.”**

fraud,” said Roy Ford, retail IT controller at SPAR UK.

Since adding the new devices, SPAR reduced the overall scope and cost of maintaining PCI DSS compliance, a move that is creating cost savings and improving fraud protection.

Shining Through the Cloud

Besides keeping omnichannel initiatives streamlined and swift, retailers need secure access to business solutions, including network and payment systems, if they want to stay relevant in an on-demand world. As a result, cloud-based security solutions are hitting the top of “to-do lists.”

Cloud-based systems are reminiscent of the “thin” client computing configurations that emerged within the first decade of the 21st century. What were merely stripped down computers, thin clients were designed to remotely access applications that resided on servers located in data warehouses versus on desktops.

Fast-forward to present-day. Hardware and software may have changed from desktops, laptops and packaged solutions to web-based devices, such as smart technology, and virtual software solutions, but the concept remains the same. Retailers are trading in personal computers and local servers in favor of managing operations via a network of software, databases and remote servers hosted on the web, on an as-needed basis.

The good news is retailers plan to increase their IT spending for the coming year, and 26% of these IT budgets will be allocated to cloud-based software spending, according to “13th Annual Store Systems Study: Brave New World of Unified Commerce,” a report from RIS News.

Known for its flexibility, scalability and low total cost of ownership, cloud is increasingly becoming a strong option for retailers striving to offload the complexity of legacy-based business operations to a more agile option. Cloud-based solutions are designed to authenticate and manage user identities so only authorized associates can access mission-critical IT solutions. While nothing is bullet-proof, cloud technology providers are doing due diligence to fight against potential breaches that threaten their retail clients. For example, providers are designing cloud-based solutions to identify vulnerabilities, monitor unauthorized access to cloud repositories, as well as block threats on cloud networks.
Conclusion
The omnichannel retailing model may promise flexibility and convenience for consumers, but for unprepared retailers, it also presents a slew of new opportunities for savvy hackers. As cyber thieves patiently await an opportunity to pilfer unsecured information from digital touch points or the networks transferring this information, retailers must be on top of their game.

By adhering to industry standards, new integration methods and virtual security options, retailers are learning how to protect business and customer information, future-proof payment security operations, and hopefully, stay one step ahead of savvy cyber-criminals.

“"The risk of losing customers due to disappointing shopping experiences caused by flawed omnichannel architecture is deadly."
— KEN MORRIS, PRINCIPAL, BOSTON RETAIL PARTNERS
Retailers still operating absent or underdeveloped capabilities needed to support an end-to-end, cross-channel shopping experience.

Source: Accenture, “A New Era for Retail: Cloud Computing Changes the Game”

<table>
<thead>
<tr>
<th>72.5%</th>
<th>490,220</th>
<th>20%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retailers</td>
<td>Consumer complaints about identity theft in 2015.</td>
<td>Retailers that have adopted tokenization.</td>
</tr>
</tbody>
</table>

Source: Federal Trade Commission, “Identity Theft Reported to the FTC”

Legacy systems that are not designed to accommodate today’s retail environment [force] retailers to scramble to cobble things together in the attempt to deliver the omnichannel capabilities customers expect.”

— KEN MORRIS, PRINCIPAL, BOSTON RETAIL PARTNERS

$8.6 BILLION

Annual cost of card fraud in the United States.


“Criminals have uncovered NFC vulnerabilities in the account provisioning and verification processes, enabling them to commit fraud.”


“The risk of losing customers due to disappointing shopping experiences caused by flawed omnichannel architecture is deadly.”

— KEN MORRIS, PRINCIPAL, BOSTON RETAIL PARTNERS

18%

Retailers that met the October 2015 EMV Liability Shift deadline.