In the past year, well over 106 million Americans had their credit card information stolen in data breaches at two of the country’s largest retailers alone.

With additional breaches at more than 13 other retailers and a number of unknown breaches that were never reported, 2014 was one of the biggest years for retail data breaches. Unfortunately, this trend is likely to continue as retailers continue to provide a target-rich environment for hackers. With large amounts of financial, personal, and even medical information, on their networks, the retail industry will continue to be an attractive target to attackers for years to come.

Even though both the retail and security industries have been talking about compliance (PCI, HIPAA, SOX, etc.) and security for over 10 years, these breaches continue to occur. According to the Verizon 2015 PCI Compliance Report, although overall compliance with the Payment Card Industry Data Security Standard (PCI DSS) has improved in yearly assessments, four out of five companies then failed during an interim assessment. Clearly, companies of all types are struggling to maintain consistent levels of compliance and security over time.

Additionally, compliance doesn’t always equal security. Despite changes to the PCI DSS 3.0 implemented in 2014, compliance requirements don’t always address the full attack continuum – before, during, and after an attack. Many are focused on implementing technologies and controls targeted to the before phase. But we are now in a threat-centric era, where the focus is shifting away from being mostly about controls and vulnerabilities to also being able to quickly analyze and remediate both during and after an attack. Resiliency addresses the issues before, during and after an attack.

Retailers today are at the forefront of the cyber security battle and payment security remains both a top priority – and a key to success. The consequences for a retail security breach are severe. Not only does news of a customer data theft expose customers to the risk of fraud, it can significantly damage a company’s brand, erode the trust of consumers, and negatively impact stock prices. In addition to these losses, recovering from a breach can cost millions of dollars as systems are investigated, cleaned and repaired, and new processes are implemented to prevent future attacks. All of which means a big hit to the bottom line – both at the time of impact and moving forward.

![Attack Continuum Diagram](image-url)
Retail Technology Trends – What Matters to Customers

As today’s consumers continue to rapidly embrace mobility and apps, retailers face a digital transformation that is changing the shopping habits of consumers on par with the rise of e-commerce in the late 1990s and early 2000s. Consumers have moved beyond the desire for engagements that are simply personalized; today’s consumer wants an experience that is hyper-relevant, delivering what they want, when and how they want it, both in-store and out.

The following key technology trends have a significant impact on retailers today:

- Creating a Hyper Relevant Experience and the Internet of Everything: Retailers are under pressure to innovate and unlock the value that new technologies like the Internet of Everything (IoE) can bring to their business in order to deliver this new hyper-relevant experience: Hyper-relevance happens when a retailer intuits and enables the shopper to accomplish what they want to do at that moment – whether that is maximizing loyalty points, or getting through a checkout line quickly, or obtaining help from a store associate.¹ To accomplish this level of real-time service, retailers will increasingly rely on a variety of new IoE technologies such as sensors, Wi-Fi, beacons, mobile devices, and RFID tags to better understand shopping patterns and product engagement in-store in much the same way web analytics reveal a shopper’s journey online. The challenge for retailers is to then take the vast amounts of data from multiple technologies and turn it into relevant insights. Retailers who can “go to the edge” by analyzing information in real time from these technologies in order to make targeted offers, deliver immediate information about whether items are in stock and suggest additional items, or provide a more efficient checkout, will provide the relevance today’s tech savvy consumers truly value.

- Mobile Point of Sale Systems (mPOS) are being rapidly adopted as legacy Point of Sale (POS) systems become out of date and are refreshed: Approximately 40% of current retail POS terminals and software are more than 5 years old.² These systems are often difficult to upgrade or patch and leave retailers vulnerable to attack. To meet the demands of today’s consumer, POS systems need to quickly access customer data and provide an efficient, secure experience. Retailers understand the need for more modern – and secure – POS systems and over 60% of retailers plan to increase their use of mobile devices for POS (mPOS)³. In our 2014 study, Cisco found that checkout optimization was one of the top two IoE Retail Concepts with 77% of respondents saying they were willing to use new technologies that deliver a more efficient process.

- Any Missteps are Visible to Customers: Security has become not only a key technology driver for refresh cycles and new technology adoption, but also a critical business driver for establishing consumer trust. As retailers upgrade existing systems and adopt the new IoE technologies needed to deliver the hyper-relevant experiences discussed, their success will inevitably depend on more than just technology: retailers must gain (and maintain) consumers’ trust. With a number of high profile retail data breaches within in the last year, security is now a top priority for consumers and retailers alike and the ability to protect payments as well as consumer data could impact not only where consumers choose to shop, but what information consumers will be willing to share with retailers. Retailers also now realize the need for protection across the entire attack continuum and budgets are now shifting to focus on security solutions that protect not only before a breach, but during and after as well. The use of security technologies such as tokenization and end-to-end encryption will increase by 145% and 151% respectively by the end of 2016⁴.

In 2013, Cisco analysis showed that retailers realized only 45 percent of the IoE Value at Stake for the industry - $80.8 billion out of a total possible value of $179.6 billion⁵. As consumers become even more tech savvy and look to engage with retailers in new, more relevant ways, the retail industry has a major opportunity to capitalize on these key technology trends to improve both consumer satisfaction and operational efficiency.

In today’s competitive marketplace, the most successful retailers will be not only those who deliver the high level of service their customers expect at every touch point – in-store, online, via email, etc. – but, those who also do so securely.

¹ Winning the New Digital Consumer with Hyper-Relevance; Cisco Systems, Inc. 2015.
⁵ Cisco Consulting Services, December 2014

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco public information. (1110R)
The Retail Threat Landscape: Knowing the Unknown

While each retail breach is unique, there are common paths attackers take. It is important to review how attackers compromise retail systems in order to understand how such intrusions can be prevented. A typical POS attack unfolds in the following manner:

1. Attackers first gain a foothold on a system. This may be by exploiting a vulnerability on a system, spear phishing a third party vendor, or even employee involvement.
2. Once having gained access to a system, attackers exploit vulnerabilities and weaknesses to gain full control over the system.
3. The attackers then survey the internal network to find ways to expand the breach and take control of further systems, ultimately reaching the point of sale systems.
4. Attackers install malware on point of sale systems by exploiting vulnerabilities in the POS system, or potentially by installing malware by compromising system update functionality.
5. Once installed on the POS systems, the malware collects financial and personal information.
6. Stolen data is transferred to a system with Internet access.
7. Stolen data is exfiltrated outside of the organization to the attacker.
Creating Resilient Environments: Security Before, During and After an Attack

To deal with today’s biggest security challenges and better protect their POS (and other) systems, retailers need a scalable, threat-centric approach that addresses security across the entire attack continuum – before, during, and after an attack.

Before an Attack

Attackers today spend significant time researching their targets and have more information about the infrastructure they are attempting to breach than ever before. Because they are singularly focused on finding weaknesses to exploit, they may know aspects of a network even better than those protecting it. In order to achieve information superiority over attackers, retailers need total visibility of their environment – including physical and virtual hosts, operating systems, applications, services, protocols, users, content, network behavior and more. As mPOS and other technologies continue gaining traction and rapidly expand the number of possible attack points retailers need to defend, gaining this level of visibility is critical to protecting systems before an attack.

With this full stack visibility in place, retailers can better understand the risks to their infrastructure, then see and understand how best to secure and segment their network. This goes well beyond just POS systems and must include both internal- and external-facing systems across the extended network to data centers, endpoints, virtual, mobile, and the cloud. To ensure that transactions and customer data remain highly secure, retailers must consider how network resources are separated and segmented in order to limit or prevent improper communications or the spread of malware as well as inhibit reconnaissance. In addition to segmentation, honeypots are another strategy often used to help thwart – and to better understand – attacks against POS systems. Creating a POS honeypot that looks like your typical POS system, but that isn’t ringing up transactions or transmitting customer data, can help detect or deflect malicious activity on the network.

It’s also important to establish baseline metrics on “known good” environments. The better an organization understands what “normal” traffic and activity looks like for each segment of their network, the easier it will become to identify anomalous behaviors and to monitor internal network traffic for malicious reconnaissance activity, particularly those related to unauthorized activity tied to POS. In addition to “fingerprinting” systems to understand how they act during normal and abnormal periods, retailers should also audit and understand all alerts on their internal systems.

It’s also important in this process to establish refresh strategies for all software, operating systems, etc. on the network to ensure that patches are being applied as recommended by the vendor and systems are up to date. Priority should be given to quickly patching high-priority vulnerabilities, then other reported vulnerabilities can be integrated into regularly scheduled maintenance and patching processes. Systems that are unpatched or out of date leave the door open for malicious actors who are constantly looking for vulnerabilities to exploit. Refreshing hardware and software on a regular basis is crucial to maintaining a secure environment.

Retailers will always be high-value targets for attackers. Because a significant breach can easily become front-page news, every organization should have a prepared incident response team with an established plan that is ready to respond to attacks. This team should determine what types of activity will lead to the activation of the response plan as well as establish communication plans based on severity that include internal audiences, customers, and even law enforcement, as required.

Retailers should also establish a relationship with an expert incident response organization that is able to provide the latest threat intelligence and best practices for readiness and response. With a worldwide shortage of security professionals, many organizations are understaffed and struggle trying to maintain their day-to-day activities in the wake of a significant breach. Working with an outside incident response team that provides a comprehensive range of capabilities can help retailers prepare, manage, respond and recover from incidents quickly and effectively.

During an Attack

Because relentless attacks do not occur in a single point of time, the ability to continuously detect and block malware is critical. During an attack, Next-Generation Intrusion Prevention Systems, Advanced Malware Protection for networks, endpoints and POS systems, and email and web security solutions provide the ability to detect, block, and defend against attacks that have
penetrated the network and are in progress. These
technologies allow you to block malicious traffic or
activity, while still allowing expected and permitted activity
between POS endpoints and internal networks.

In order to evolve security from an exercise at a point in
time to one of continual analysis and decision-making,
modern security technologies also need to provide
awareness. To detect advanced attacks as they move
laterally through the network and across endpoints,
defenders need technologies that automatically look for
Indicators of Compromise (IoC’s) left behind by malware
and exploits, as well as more advanced behaviors of
compromise that happen over time. By aggregating and
correlating data from across the extended network to
provide context, these technologies can automatically
correlate new threats against the vulnerabilities that exist
in your network to determine whether they can affect your
business. This enables defenders to cut through all of the
noise and focus efforts on responding to the events that
will have the most impact.

With this continuous approach to security, critical security
activities, such as policy tuning, or proactive measures,
such as isolating end points that exhibit suspicious
behavior, can also be automated. Not only does this save
time and effort, it also adapts the network’s defenses to
changing conditions and results in optimized security
policies that are specifically tailored to that network and
the threats it encounters.

After an Attack

Once an attack has been confirmed, the most critical
priority is to marginalize its impact. Here again, visibility
is crucial. Advanced malware protection for retailers’
networks and POS systems with retrospective security
capabilities can provide the visibility needed to quickly
identify the point of entry, determine the scope of the
breach, and also empowers them to take the steps
needed to contain the threat, eliminate any risk of re-
infection, and remediate any damage done by the attack.

Stopping the spread of malware requires full visibility into
and a deep understanding of all network activity. While
leveraging in-depth traffic analysis can help differentiate
between normal business transactions and suspicious
behaviors, there is now an increased need for integration
with accurate contextual data, such as user identities, user
privilege levels, etc. to deliver deeper network visibility and
more quickly take mitigation actions against a threat. This
integration gives network and security analysts the ability
to quickly and easily assess the significance of security
events by correlating context with security alerts.

Because every second counts once a breach has
identified, engaging with an advanced incident response
service organization can help get IT security teams
on solid ground and greatly reduce the impact of a
compromise. Bringing in an incident response services
team also gives additional support to existing security
teams by providing the expertise, staff, and tools needed
to evaluate threats, contain damage and mitigate risks.

As incident response and communication plans are
activated, the need for rapid response and coordinated
communications become even more critical. In the case
of a high-profile public breach, external communications
plans must be in place and are critical in mitigating the
impact a breach has on a retailer’s reputation, brand,
and, ultimately, the bottom line. Executives will need to
quickly understand details of the attack and the actions
being taken on an ongoing basis. Having visibility-driven
technologies, a continuous approach to security, and
strong incident response plans and teams in place can
significantly lessen the overall impact of a high-profile
breach.

Enabling Business, Minimizing Risk

The retail business moves quickly and “market trends wait
for no one.” Lines of business rely on speed to get ahead
of competitors and will try most any new technology to
do it – secure or not. IT and Information Security must get
ahead of the curve and maintain control to reduce risk to
the organization. As if this wasn’t difficult enough, retailers
are notoriously ‘frugal’ when it comes to security budgets.
The trends going forward are such that more retailers will
adapt by doing the following:

• Simplifying and operationalizing security enables teams
to respond faster and more effectively to mitigate risks.

• Unified, automated enforcement of policies allows for
consistent controls from the data center to the cloud to
the endpoint.

• Build trusted partnerships with vendors and service
providers and require that they follow information
security best practices.
Conclusion: Responsive to Customers, Resilient to Attacks

Historically, effort and budgets in security have been focused primarily on securing the network before an attack: building layers of defense with the goal of stopping threats at the perimeter. However, as we continue to see high-profile breaches occur over and over again, organizations are quickly realizing that it’s no longer a matter of if they are breached, it’s a matter of when. With this realization, we now see a shift in security spending to focus on technologies and services to help them better prepare both during and after an attack so that the impact to their organization – and more importantly for retailers, to their public image and bottom line – can be minimized.

As the retail industry further embraces technology trends such as the Internet of Everything, it will have an impact at every level of the business and security is foundational for meeting customers’ expectations. Security must now be seen not as just a business expense, but as a business enabler. Security has become foundational to the adoption of the new technologies that will help retailers deliver the kind of hyper-relevant experience and service that consumers demand today and is now critical for retailers to win the battle for brand loyalty and consumer trust.

Even though retailers will continue to be a key target for cybercriminals for the foreseeable future, organizations can act smarter and more quickly than ever by focusing on a new threat-centric security model that delivers the visibility and control organizations need across the extended network and the full attack continuum - before, during, and after an attack. By aligning the people, processes and technology needed to form a defense against today’s threats, remediation can be swift and retailers can greatly reduce their time to resolution and, ultimately, lessen the overall impact of a breach to their business.

Cisco offers a comprehensive portfolio of threat-centric cybersecurity solutions that span the entire attack continuum. To learn more about Cisco’s security solutions, visit www.cisco.com/go/security.