SOLUTION BRIEF

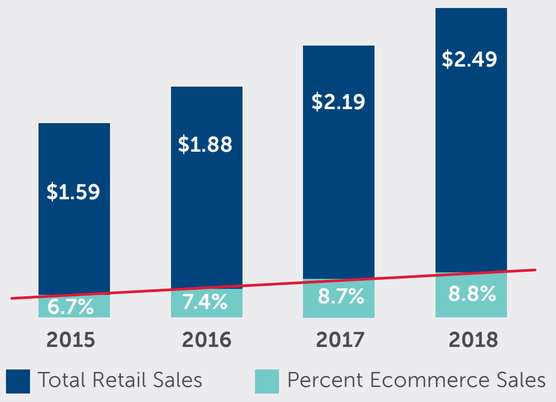
Enable Retail Growth While Leveraging Technology to Protect Customer Data

SecureWorks®

Introduction

Retail is one of the largest global industries in terms of employment and revenue, contributing on average 9 percent of a country's gross domestic product (GDP).[1] Retail sales globally generated $22 trillion in 2014 revenue according to *eMarketer*.[2] As you've experienced firsthand, the pervasiveness of the Internet has reduced barriers to entry and evened the playing field for smaller retailers to attract customers from around the globe.

Total Retail Sales Worldwide, 2015–2018
(In Trillions and % Ecommerce of Total Retail Sales)



Source: *eMarketer*, December 2014,

The retail industry worldwide is still recovering from an economic slowdown, an upturn in price comparison shopping and less consumer loyalty than in years past. Other macro trends contributing to mixed results for the retail industry include lower consumer sentiment and confidence, which are key drivers of retail sales. In recent years, customers have become more knowledgeable and empowered as they seek out the retail provider with the lowest price or fastest delivery. This power shift from retailer to customer is leading to seismic shifts in the retail industry, just one challenge among many that are impacting the retail industry overall.

Retail Industry Challenges

Changing Landscape
The retail industry continues to face a number of key challenges that impact in-store as well as back office operations and efficiencies. The rise of ecommerce has propelled omnichannel retailing where consumers blend online research and shopping with in-store browsing and "click and pickup." Although $10 out of $11 is purchased in a store today, ecommerce adoption is already transforming and even disrupting retail today.[2] Shopping malls and individual stores alike are seeking ways to remain relevant and enhance the in-store shopping experience in light of anytime, anywhere ecommerce and product delivery. Mobile shopping is accelerating and creating new opportunities for retailers to enhance customer engagement, loyalty, and therefore, repeat business. In addition, the retail industry faces increased competition and cost efficiency pressures. A top priority for the low-margin retail industry is streamlining operations and functions to reduce costs. Some retailers are pursuing technology and innovation as ways to optimize operations and enhance the customer experience to gain more market share and revenue.

Retail Technology Brings Opportunity and Risk

New retail technology approaches and systems bring opportunities as well as risks. Existing point of sale (POS) systems provide reams of data regarding customer purchases, pricing, product assortment and upsell statistics to be harnessed for useful decisions that are enabled by big data analytics. Too much inventory can lead to margin-impacting discounting; too little inventory can lead to out-of-stock conditions and dissatisfied customers who purchase elsewhere. In addition, retail technology can also be used to augment products and services to enhance the in-store customer experience, such as with digital dressing rooms where shoppers "try on" clothes electronically. Retail sits on a foundation of sensitive credit card data that is sought after by hackers who are persistent and evasive. Although retail only accounted for 10 percent of the data breaches in 2015, the consumer notification process and resulting bad publicity keep retail data breaches in the press and public consciousness.[3] More than 60 percent of global consumers surveyed say they are unlikely to shop at or do business with a firm that experienced a data breach where financial information was stolen.[4] In addition to retail industry objectives developed to maintain customer loyalty, reduce costs and accelerate growth, there are several technical challenges facing the retail industry overall:

- **Expanding POS and Mobile Devices:** The retail industry is an information-intensive one, harnessing a wide array of analytics such as inventory, pricing and promotions, store performance, ecommerce statistics and customer data. Much of this valuable sensitive information is from your POS system that is the heart of the retail store, but creates a wide attack surface that is challenging to monitor and protect. Threat actors, for example, have been caught placing skimming devices on retail POS devices as a way to collect credit card data to be sold on the underground market.

- **Protecting Data Security and Privacy:** Trust is at the center of a retailer's relationship with its customers. The retention and storage of vast amounts of sensitive credit card and payment data, often unencrypted, have made retail industry data a key target for hackers.

- **Increasing Staffing Implications:** Retail is one of the most labor intensive industries. Frequent new hires and high staff turnover rates, coupled with a lack of cybersecurity training and awareness, increase the likelihood of human error. At the branch or store level, there is often a lack of technical or IT expertise to maintaining equipment and infrastructure or understanding security risks. Social engineering, where hackers exploit personnel and their human weaknesses, appear to have been a source of compromise for data breaches at several fast-casual food retailers in 2016.

- **Enhancing Supply Chain Partners:** Hackers often seek out the weakest link in the supply chain to manipulate and exploit. Smaller retail establishments or supply chain partners of larger retail chains have been targeted by pervasive threat actors and breached to gain a foothold into selected accounts. You are never too small or less well known to be targeted by persistent and evasive hackers.

With thin profit margins and inadequate funding, the retail industry has underfunded cybersecurity relative to the risk and historical threat levels and breaches. Although the retail industry does not count as the largest contributor of data breaches, it has provided a majority of the credit card and personal identity thefts globally.

Conclusion

The retail industry is facing a new reality as customers gain more purchasing power, ecommerce adoption continues to impact brick-and-mortar stores, and global competition intensifies. In addition to those challenges, the retail industry has also been the target of widespread data breaches, with each incident costing an average of $3.8 million to detect and remediate.[5]

Retailers must enhance their cybersecurity funding and move from a mindset of mere compliance to focus more resources on detection and prevention of persistent and evasive threats. Retailers large and small must balance compliance funding with early detection and prevention of threats while working with security experts to enhance their security maturity. SecureWorks can serve as an extension of your IT and Security teams, providing solutions that streamline and strengthen your security while you focus on strategic core competencies.

SecureWorks Solutions

As a world leader in security solutions, SecureWorks provides an early warning system for evolving cyber threats, enabling you to prevent, detect, rapidly respond to and predict cyber attacks. We deliver intelligence-driven security solutions and expertise to retailers large and small in 59 countries around the world.

Managed Security Solutions

SecureWorks offers a wide range of managed IT security solutions for organizations. The Counter Threat Platform™ is at the core of our intelligence-driven approach to security solutions. The CTP analyzes billions of network events 24x7 to discover potential threats, deliver countermeasures, and generate valuable context and threat insights for all industries including the retail industry.

Our security analysts serve as an extension of your team to monitor for and detect threats across your environment. For retailers, maintaining a PCI DSS (Payment Card Industry Data Security Standard) compliant environment is challenging. We scan your externally facing systems, identify and help you remediate any detected vulnerabilities, and submit PCI scanning compliance reports directly on your behalf.

> "With more data mining and increased digital communications comes more risk. Cyber security will continue to cut across all aspects of the business: disruption, convergence of digital online, social, new ecosystems, and mining customer insights. Cyber continues to be a major concern for retailers and is now a board level issue."
>
> —Rod Sides
> Vice Chairman, US Retail and Distribution Leader,
> Deloitte Consulting LLP

Security and Risk Consulting

Our Security and Risk Consulting team provides strategic advice and analysis to help you enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency. Our highly skilled security consultants help you test and improve your security defenses, security processes and design and develop new security programs. We offer consulting, testing and remediation solutions to meet ever-increasing PCI DSS mandates. SecureWorks has deep retail and compliance expertise to augment your capabilities. We are a:

- Qualified Security Assessor (QSA)
- PCI Approved Scanning Vendor (ASV)
- PCI Forensic Investigator (PFI)

Threat Intelligence

The SecureWorks Counter Threat Unit™ research team collects relevant information wherever it can be found, and then analyzes it and synthesizes it into meaningful guidance on which you can act. Our threat intelligence can help you identify threat actors who may be specifically targeting your organization or your executives, and provides the insights to help you defend and even preempt the attacker. If you manage your own Security Operations Center (SOC), our experts can help you optimize and enhance your in-house security capabilities.

Incident Response And Management

Our incident management practices provide rapid containment and eradication of threats, minimizing the duration and impact of a security breach to your organization.

Leveraging our cyber threat intelligence and global visibility, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents. Retail entities large and small across the globe have been breached and had sensitive data stolen. Data breaches can lead to lost revenue, reduced customer loyalty, unwanted publicity, and compliance industry fines. SecureWorks has the people, processes and technology to help you detect threats sooner to minimize damage and identify root causes to avoid becoming re-compromised.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com

End Notes

[1] Ross, Sean, *Investopedia*, "What portion of the global economy is represented by the retail sector?" July 14, 2015, http://www.investopedia.com/ask/answers/071415/what-portion-global-economy-represented-retail-sector.asp, accessed August 11, 2016.

[2] eMarketer.com, "Retail Sales Worldwide Will Top 22 Trillion This Year" http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/1011765, December 23, 2014

[3] Gemalto releases findings of 2015 Breach Level Index," February 23, 2016

[4] "Consumers avoid doing business with companies hit with a data breach: survey", 11 December 2015, Firstpost.com. Survey included Australia, Brazil, France, Germany, Japan, United Kingdom and United States. http://www.firstpost.com/business/consumers-avoid-doing-business-with-companies-hit-with-a-data-breach-survey-2541748.html

[5] Ponemon Institute, *Cost of a Data Breach Grows as does Frequency of Attacks*, http://www.ponemon.org/blog/cost-of-data-breach-grows-as-does-frequency-of-attacks, May 27, 2015

SecureWorks®