JULY 2021

WHITE PAPER

RETAIL'S KEY TO DEFEATING CYBERATTACKS

INTRODUCTION

In the wake of the global COVID-19 pandemic and continuing competition from online giants, retailers are scrambling to drive customers to their websites and physical stores to propel them along the buying process. To do that successfully, stores are implementing more ways to interact with customers, including adding web-facing applications and installing new technologies online and inside physical stores. These new advancements are already influencing customer behavior and increasing sales, but they come with risk to both on-premises and cloud environments.

Retailers have long been familiar with risks that online devices create. Point-of-sale (POS) systems have now been around for decades, but they're still difficult to secure because they connect to the internet, and hence have been vectors for many highly publicized breaches. As retailers embrace new technologies to create a more seamless shopping experience, they must take care that the speed at which they adopt new technologies does not outpace their ability to protect customer data. Artificial intelligence (AI), internet of things (IoT), and digital transformation are all being used to better engage with customers and to attract more business. But to keep customers happy, a retailer must protect its data.

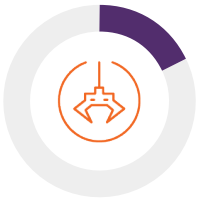
45%

OF RETAILERS ACROSS THE GLOBE CLAIM TO HAVE EXPERIENCED A DATA BREACH IN THE PAST YEAR.[1]

TOP INDUSTRIES TARGETED BY THREAT ACTORS IN 2020[2]:

23%

FINANCE & INSURANCE



18%

MANUFACTURING

11%

ENERGY

10%

RETAIL

 | 21030727 Copyright © 2021. Armor, Inc., All rights reserved.

New cybersecurity solutions are needed to protect environments from the latest attacks. Device makers are slow at integrating security to their products, which makes it necessary for retailers to see all incoming and outgoing traffic on any devices. Retailers can finally do that without buying or managing equipment such as firewalls, intrusion detection/prevention systems (IDS/IPS) and other security tools. Small and medium-sized retailers without large IT security budgets can now have visibility of on-premises, cloud, and hybrid environments, and threats that get past prevention solutions can be detected and remediated immediately and automatically.

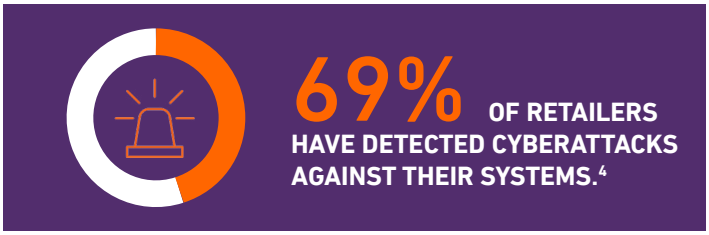
2020 RETAIL INDUSTRY CHALLENGES (ACCELERATED BY COVID-19)[3]

- Reinventing In-Store Shopping
- Security and Compliance
- Moving to the Cloud to Overcome Retail Industry Challenges
- Greater Demand for E-Commerce and Omnichannel Payments
- Optimizing the Supply Chain and Customer Service
- Maintaining Visibility and Competitiveness

 | 21030727 Copyright © 2021. Armor, Inc., All rights reserved.

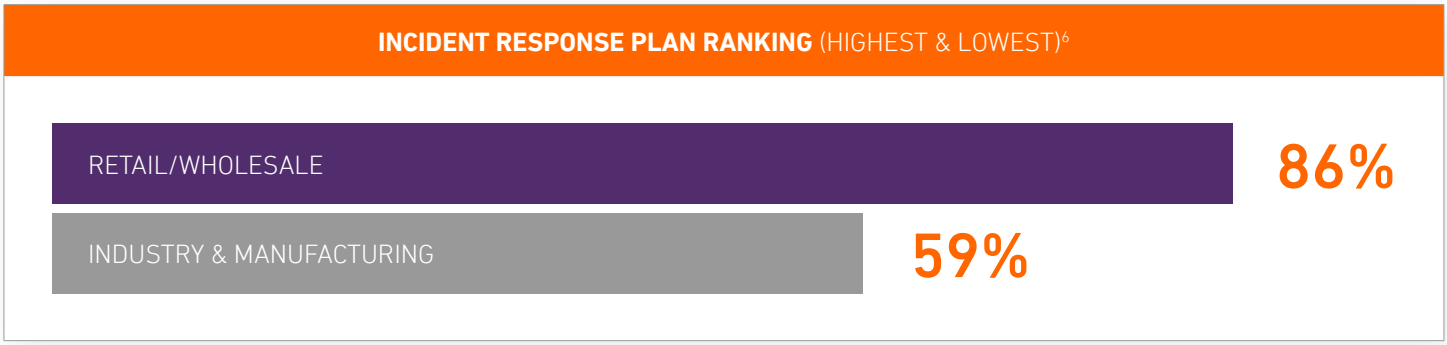
DIFFICULTIES SECURING THE NETWORK

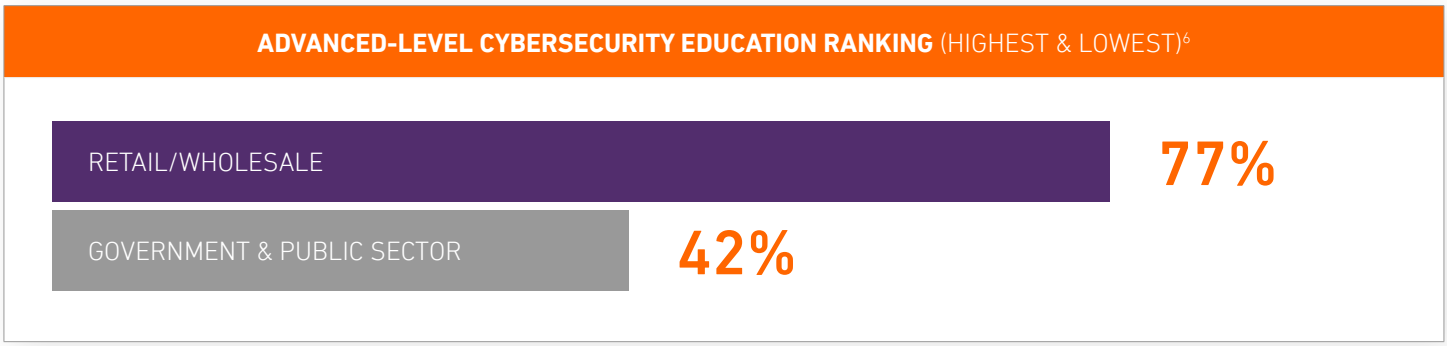
According to a report by Retail CIO Outlook, nearly one-third of all retail businesses had experienced financial losses due to cyberattacks in just the past few years. Retailers are starting to realize just how much of a target they are to hackers. Still, only 52% of companies feel that their security infrastructure is updated, and 61% of companies think that they are in compliance with security standards.[5]



Unless retailers take action, their risk is only going to climb with digital transformation. A March 2020 survey by WSJ Pro Research Cybersecurity found that retail has joined manufacturing and government in falling behind other industries in being prepared for threats. Fewer than two-thirds of manufacturers and retailers have any cybersecurity program, and retailers were least likely to feel equipped to defend themselves against ransomware attacks, with only 62% of companies confident in this area. Government was also ill-prepared for ransomware attacks and inadequate in its cybersecurity training to executives. Health care, on the other hand, was unexpectedly well equipped to handle an attack.[6]

Still, retail/wholesale should not be discounted, as it ranked the highest for having an incident response plan, at 86%. Industry and manufacturing ranked the lowest with 59%. Retail/wholesale also topped the list for having its leadership teams receive executive or Advanced-level cybersecurity education with 77% having offered training. Government and the public sector came in last place with 42%.[6]





 | 21030727 Copyright © 2021. Armor, Inc., All rights reserved.

HISTORICAL RETAIL SECURITY

In the past, retailers only had to be concerned with the devices on premises, POS systems, and employees who fell for social engineering attacks. To combat these vulnerabilities, over the past decade endpoint and email server protections have been implemented. To keep up with continual changes in IT, the Payment Card Industry Data Security Standard (PCI DSS) has often changed the requirements to meet PCI compliance and secure data. However, time and again retailers that have been PCI compliant have been breached.

The industry has been trying to find different ways to secure data. In 2017, the National Retail Federation (NRF) conducted a survey and found that 60 percent of small brick-and-mortar retailers had installed chip-card readers.[9]

But in recent years, as the retail industry has moved transactions more to a web-focused infrastructure, cyberattacks have shifted away from POS devices and chip-card readers and focused on web applications. In fact, e-commerce attacks seeking to steal card-not-present (CNP) data are, by far, the leading cause of breaches in retail, making up 53% of retail attacks in 2019, according to the 2020 Trustwave Global Security Report. Twenty-seven percent of attacks targeted retailers' financial data, 10% stole user credentials, and 10% sought card track data. Criminals go where the action is. As this has happened, POS-related breaches have dropped from 31 percent of incidents in 2016 to just 5 percent in 2019.[7]

Now retailers need to strengthen the security of their online stores to block growing attacks from that front. One sophisticated hacker to look out for is Magecart, a network of criminal groups that target retail websites that use the Magento e-commerce platform. They infiltrate sites, typically through malicious scripts that steal customers' payment card information during checkout.[7]

E-commerce attacks seeking to steal card-not-present (CNP) data are, by far, the leading cause of breaches in retail, making up 53% of retail attacks in 2019.

MAKEUP OF MOST RETAIL ATTACKS

AS A COLLECTOR OF CREDIT CARD PAYMENTS AND OTHER FINANCIAL TRANSACTIONS, RETAIL HAS LONG BEEN A FAVORED TARGET FOR MALICIOUS THREAT ACTORS.[2]

 | 21030727 Copyright © 2021. Armor, Inc., All rights reserved.

NEW RETAIL TECHNOLOGIES

Integrating technology is the only way to continue to enhance the customer experience and stay competitive. Social media, customer-interacting apps, automated robots that converse with buyers, interactive "magic mirrors," "buy online, pick up in store" (BOPUS), real-time inventory across a network of stores, and numerous other new technologies that increase customer satisfaction are just a few examples of digital transformation in retail. Based on DataDriven's Digital Transformation Trends survey, the great majority of respondents are using or planning to use these tools, such as social media (79.1%), digital marketing (79.1%), and smartphone apps (68.0%). Many retailers also are anticipating an increase (39.8%) in their overall IT budget. Other major areas of increase include Digital Transformation (39.8%), communications and networking (37.8%), and cloud services. Software-as-a-service (SaaS) is the most popular type of application source, preferred by one-third (32.3%) of those surveyed.[10]

This is despite the economic downturn from the pandemic because businesses recognize that investment in digital technologies is necessary to adapt to current consumer changes as well as remain agile for future disruption.

Artificial intelligence is helping retailers create interactive design stations that encourage customers to customize clothes, to identify internet leads, and to assist customers in determining what products would be best for them. Many retailers see AI as an opportunity (69.7%) with 73.6% believing that AI will accomplish some of the tasks currently performed by people.[10]

But not all technology adoption is focused on customer satisfaction. Retailers are also using the latest loss prevention technology tools to combat fraud and threats. According to NRF's more recent survey in 2020, POS analytics remains the biggest system in use, deployed by 56.5%, up slightly from 55.6%, and solution provider video analytics remained the same at 15.9%, while fingerprint ID at POS went down from 11.1% to 5.8%.[8]

As technology continues to transform the retail industry, it is critical for businesses to keep cybersecurity top-of-mind and assess the potential impact on risk and security.

52%

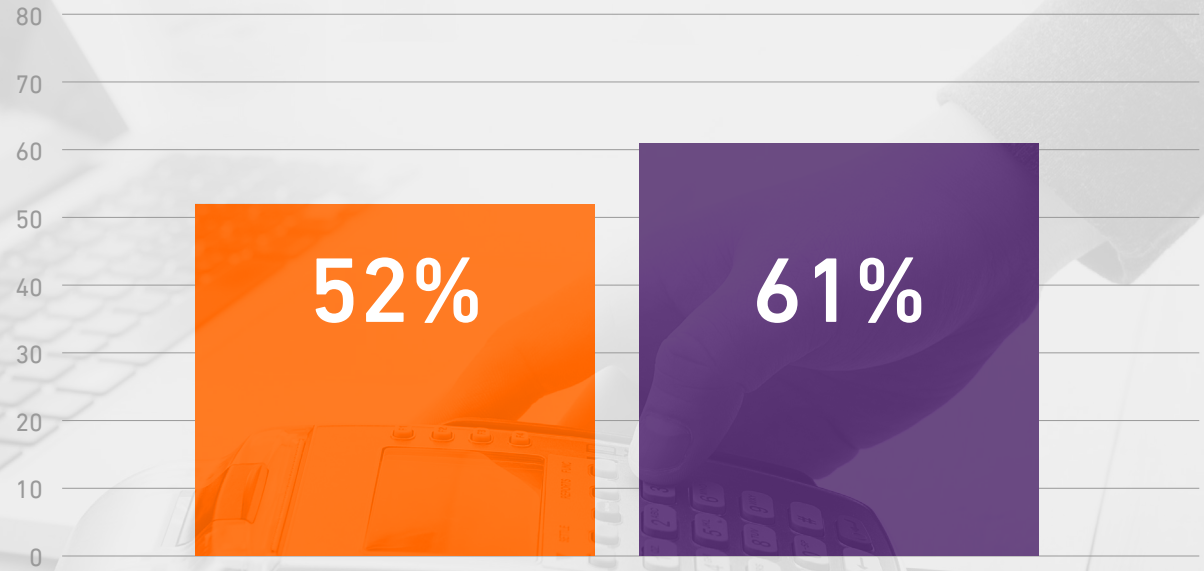
OF LOSS PREVENTION INVESTMENTS BY RETAILERS WILL GO TOWARD TECHNOLOGY TOOLS IN THE FOLLOWING YEAR.

These include remote monitoring technology, upgraded POS systems and exception reporting, and refund history tracking programs.[8]

 Copyright © 2021. Armor, Inc., All rights reserved.

DO RETAILERS SEE THE THREAT?

ONLY 52% OF COMPANIES FEEL THAT THEIR SECURITY INFRASTRUCTURE IS UPDATED, AND 61% OF COMPANIES THINK THAT THEY ARE IN COMPLIANCE WITH SECURITY STANDARDS.[5]



IT PROFESSIONAL IN THE RETAIL SPACE IDENTIFIED THE FOLLOWING SECURITY CHALLENGES:[10]

57%	56%	55%	53%	57%
NETWORK SECURITY	WEB SECURITY	FRAUD PREVENTION	DATA PRIVACY	REGULATORY COMPLIANCE

 21030727 Copyright © 2021. Armor, Inc., All rights reserved.

SOLUTIONS

Securing retail environments requires gaining visibility into all the connected things on a network and in the cloud. A threat can only be remediated if it is identified. If an attacker breaks into a security camera or a web-facing app, a company must be able to spot the traffic and quarantine the threat before malicious activity begins. That's now possible to do even if a company does not have its own security team or limited resources.

By leveraging the power of the cloud, security-as-a-service (SECaaS) providers automatically scale up as a retailer's environment grows with the newest devices and applications. A team of trusted experts that specialize in protecting cloud, on-premises, and hybrid IT environments watch over environments 24/7/365, detect threats as soon as they appear, and help remediate them. These outsourced security providers can help organizations meet compliance requirements, alleviate the need to hire and maintain security researchers and analysts, as well as limit the need to purchase and manage expensive tools such as intrusion detection systems/intrusion prevention systems (IDS/IPS), firewalls, and security information and event management (SIEM).

1 SECAAS PROVIDES A VARIETY OF SECURITY SERVICES, INCLUDING THOSE LISTED BELOW:

- Intrusion detection
- Malware protection with constant updates
- Log and event monitoring
- Active threat hunting
- Vulnerability scanning and patch monitoring

2 WHEN CHOOSING A SECAAS PROVIDER, LOOK FOR ONE THAT OFFERS THE FOLLOWING BENEFITS:

- Intelligence-driven, proactive security that provides threat alerts and remediation
- Unified visibility and control for any environment
- Simplified, continuous audit-ready compliance
- Reduced dwell time for attackers
- Pay-per-use consumption
- Supported environments (On-prem, Cloud, and Hybrid)

ONLY 62%

OF RETAILERS WERE CONFIDENT THEY ARE PREPARED TO DEFEND THEMSELVES AGAINST RANSOMWARE ATTACKS.[6]

 | 21030727 Copyright © 2021. Armor, Inc., All rights reserved.

SOURCES

1. The Thales Group – "Thales Data Threat Report," 2021.
   https://cpl.thalesgroup.com/sites/default/files/2021-06/2021-thales-data-threat-report-federal-infographic_0.pdf

2. IBM Security – "IBM X-Force Threat Intelligence Index," 2021.
   https://www.ibm.com/security/data-breach/threat-intelligence?_ga=2.135134520.835129472.1623142403-1199389589.1623142403
   https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/

3. XAASJournal – "2020 Retail Industry Challenges and the Tech Solutions to Conquer Them," July 21, 2020.
   https://www.xaasjournal.com/2020-retail-industry-challenges-and-the-tech-solutions-to-conquer-them/

4. F-Secure – "Cyber Threats for Retail & E-Commerce Companies," Jan. 2, 2020.
   https://blog.f-secure.com/cyber-threats-for-retail-ecommerce/

5. Retail CIO Outlook – "Why Is Strong Security Measures Mandatory in Retail Industry?" Jan. 24, 2020.
   https://www.retailciooutlook.com/news/why-is-strong-security-measures-mandatory-in-retail-industry-nid-969.html

6. WSJ Pro Research – "Which Industries Aren't Ready for a Cyberattack?" June 21, 2020.
   https://www.wsj.com/articles/the-industries-most-vulnerable-to-cyberattacksand-why-11592786160

7. Trustwave – "Trustwave Global Security Report," 2020.
   https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/

8. National Retail Federation – "National Retail Security Survey," 2020.
   https://cdn.nrf.com/sites/default/files/2020-07/RS-105905_2020_NationalRetailSecuritySurvey.pdf

9. National Retail Federation – "Small Retailers Switching to Chip Cards But Still Worried By Lack of PIN," Aug. 10, 2017
   https://nrf.com/blog/small-retailers-switching-chip-cards-still-worried-lack-pin

10. DataDriven – "Digital Transformation Trends: Global Retail Industry," 2020.
    https://www.fujitsu.com/global/imagesgig5/DX-Trends-Global-Retail-Industry-Key-Findings.pdf

 21030727 Copyright © 2021. Armor, Inc., All rights reserved.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167

21030727 Copyright © 2021. Armor, Inc., All rights reserved.