HADRIAN

eBook

Securing the Retail Sector in 2024

HADRIAN

Introduction

Cybersecurity has become a critical concern for businesses across all industries. The retail sector, in particular, faces significant challenges as it increasingly relies on digital channels to connect with its customers.

Recent statistics[1] paint a concerning picture of the retail industry's cybersecurity landscape.

Retailers are amassing a large amount of customer data, making them attractive targets for cybercriminals. Risks posed to the retail sector:

- Lost revenue due to downtime
- Financial losses resulting from incident response
- Regulatory fines, especially from laws such as GDPR
- Lost customers caused by brand damage and lower trust
- Lawsuits from customers who had their data breached

24%

Of cyberattacks target retailers.

98%

Of applications in the retail industry have security vulnerabilities

16%

Of all retail companies experienced a data breach resulting in website downtime over the past two years

30%

Of retail businesses state that maintaining security upgrades is their biggest challenge

HADRIAN

Top Retail Attack Vectors

The retail sector faces significant challenges in managing its digital attack surface, with concerns mounting among IT and business leaders.

	Retail (n=244)	Cross-Sector Average (n=1974)
Exploited Vulnerability	41%	36%
Compromised credentials	22%	29%
Malicious Email	15%	18%

HADRIAN

Exploited Vulnerabilities

Exploited vulnerabilities make up a large proportion of attacks encountered due to the unique makeup of the retail sector's attack surface:

Dynamic Environment

71% of retail IT and business leaders are concerned about the size of their digital attack surface. Over a quarter (27%) express being "very concerned", while two-fifths (40%) believe the attack surface is spiraling out of control.[2]

Global Complexity

Managing the attack surface is particularly challenging for global retailers, according to 61% of respondents. The global nature of operations adds a layer of complexity to cybersecurity efforts.[2]

Limited Visibility

Over half (54%) of retail IT and business leaders admit to having blind spots in securing their attack surface. Cloud assets pose the greatest challenge, with 38% of respondents acknowledging a lack of insights, followed by network (33%) and end-user assets (29%).[2]

HADRIAN

Timeline of Notable Retail Incidents

2013

Target
40 million debit/credit card accounts and 70 million customer records compromised.

2014

eBay
Personal info of 145 million users exposed.

Home Depot
56 million card details and 53 million emails compromised.

2015

Costco
Data of 58,000 customers, including payment info, breached.

2018

Saks Fifth Avenue / Lord & Taylor
Nearly 5 million customer payment card details were stolen.

Under Armor
150 million of MyFitnessPal user accounts were compromised.

Forever 21
After obtaining network access malware was deployed to gather credit card data from their point-of-sale (POS) system.

2020

NutriBullet
Hackers gained access to NutriBullet's infrastructure, placing card skimming code on the site to steal credit card data.

2021

Bonobos
A 70-gigabyte SQL backup file containing 7 million shipping addresses was stolen from a third-party cloud provider.

HADRIAN

Timeline of Notable Retail Incidents

2021

Neiman Marcus Group
4.6 million customers had their personal information compromised by hackers.

IKEA
TaskRabbit operations were temporarily halted due to a cyberattack.

CVS Health
A massive, misconfigured database containing 1.1 billion records was found publicly available and unsecured.

2022

MediaMarkt
A 240million dollar ransom was demanded from the company, and in-store computers and services were offline during the attack.

Sobeys
Estimated $25 million annual net earnings loss from payment processing disruption.

2023

Indigo
Ransomware attack disrupts operations and impacts payment systems.

Hot Topic
Breached through credential stuffing, posing risks to customer accounts.

JD Sports
The personal information of 10 million customers was stolen from a database of purchases made between 2018 and 2020.

VF Corporation
In the run-up to the December shopping season, VF discovered that personal data belonging to 35.5 million customers had been exposed.

Exploring Web Store Exposures

To execute a modern penetration testing strategy the following capabilities could be considered:

Insecure User Traffic

Without secure communication protocols user traffic can be intercepted, manipulated, and redirected through session hijacking, packet sniffing, and DNS spoofing.

Active Content

Scripts and active content introduce potential vulnerabilities, especially in e-commerce applications with dynamic product displays. While enhancing user experience, these technologies also create opportunities for malicious script insertion, increasing the risk of attacks like Magecart and credit card skimming.

Scale of Attack Surface

Retail applications often have extensive page counts due to the range of products sold. However, this abundance of pages increases the attack surface, making it challenging to maintain security across every page, link, and input field.

Cookies

Vital for real-time security, cookies monitor session activity and regulate access. Proper cookie management is essential for preventing unauthorized access and fortifying defenses against potential breaches.

Page Creation Tools

Varied based on the coding language used, with some languages more susceptible to vulnerabilities than others. Outdated or insecure code exposes applications to potential exploits, making them prime targets for cyber attacks.

Weak Authentication

Strong authentication and authorization mechanisms are critical for verifying a user's identity. Without them, users could gain access to content or be able to perform actions that they should not be able to do.

Input Fields

The number of input fields in web applications correlates with the attack surface, with more fields posing a higher risk of XSS and SQL injection attacks. Thorough input validation is crucial for mitigating these vulnerabilities.

HADRIAN

Technical Challenges Managing the Attack Surface

Manual Mapping and Information Silos

A quarter (25%) of retail security professionals say that they still manually map their environments, while a third (33%) do so regionally, risking the creation of information silos and hindering comprehensive visibility.[2]

Understanding and Quantify Risks

Respondents in the retail sector cite several challenges in understanding and managing cyber risk, including limited resources (40%), difficulty in quantifying risk (38%), and reliance on too many tools and vendors (30%).[2]

Inadequate Risk Assessment Methods

51% of retail firms admit their method of assessing risk exposure isn't sophisticated enough. Less than half (46%) claim to have a completely well-defined process for this. Additionally, 34% of respondents review or update risk exposure only every month or less, while just 20% do so daily.[2]

Constant Changes to the Attack Surface

The biggest challenge for respondents in managing the digital attack surface is keeping up with constant change (40%).[2]

HADRIAN

Business Challenges Managing the Attack Surface

Change Management

The evolving technology landscape presents both opportunities and challenges in managing the attack surface. Understanding the impact of new technologies, such as cloud assets and network configurations, is crucial for effective cybersecurity strategies.

Information Silos

Cybersecurity is not solely the responsibility of the IT department. Other departments also play a role in contributing to vulnerabilities, such as through the use of active content and authentication practices. Collaboration across departments is essential to ensure a holistic approach to cybersecurity.

Supply Chain Risks

Supply chain risk, particularly concerning third-party connections, poses significant challenges in securing the attack surface. Incidents like the breach at Target, which originated from a compromised third-party vendor, highlight the importance of vetting and securing all connections in the supply chain to mitigate potential risks.

Staff Turnover

Retail respondents confront a notable challenge with a high turnover of IT staff, standing at 63%, exceeding the average turnover rates across industries.

North American and European retail organizations, concerns loom large over missing alerts (76%) and alert fatigue (61%). Moreover, inadequate employee training is a prevalent issue, flagged by 71% of retail respondents, along with a substantial 69% reporting a shortage of qualified security staff.[3]

HADRIAN

Visualizing the Fallout of an Attack Impact

71%

Of retail IT and business leaders are concerned with the **size** of their digital attack surface.

41%

Of ransomware attacks in the retail sector stemmed from **exploited vulnerabilities**.

+50%

Of retail firms say that their method of **assessing risk exposure** isn't sophisticated enough.

54%

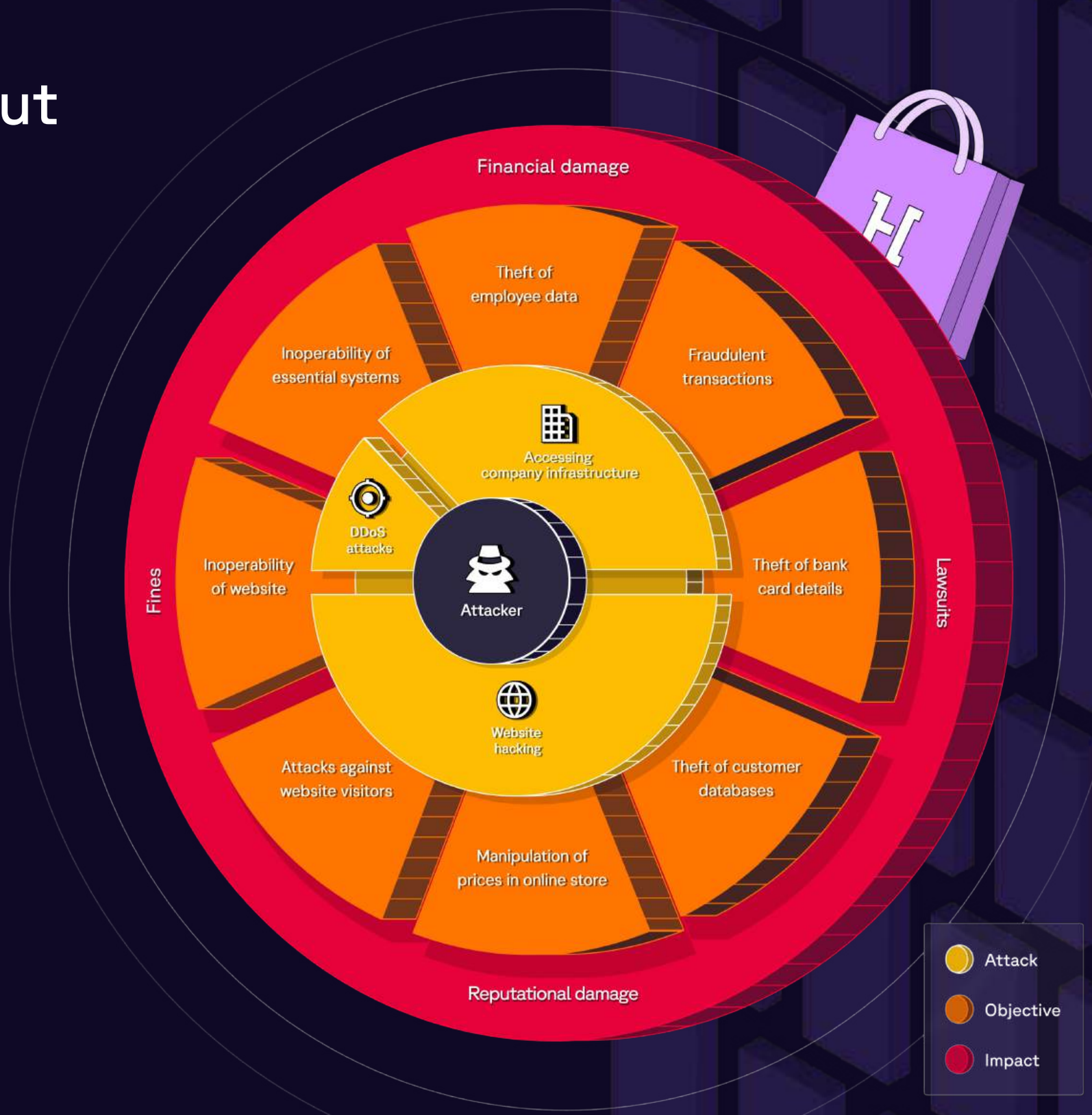
Of retail security teams admit to having too many **blind spots** in their attack surface.

40%

Of security teams struggle to keep up to date with the **constant change** to their attack surface.

38%

Of security teams cite difficulties quantifying risk when **prioritizing remediation**.



HADRIAN

Three Pillars of Proactive Security

To respond to threats and mitigate risks before they are exploited the retail sector must be able to monitor and identify threats, vulnerabilities, and risks in real-time. By looking at cybersecurity through the eyes of a real threat actor, security teams can focus on the realistic ways they could be attacked, enabling security teams to mitigate attacks before they happen.

1

Monitor your attack surface at all times to understand potential exposures:

You can't defend what you can't see, so it's crucial to maintain continuous awareness of your attack surface to identify potential vulnerabilities and threats.

2

Continuously assess threats to prioritize remediation: Instead of waiting time on less crucial issues, prioritize remediation efforts based on validated threats.

By continuously assessing threats, you can ensure that resources are allocated effectively to address the most significant risks.

3

Working from a single source of truth: Centralize security monitoring to eliminate confusion and breakdown information gaps.

By establishing a single source of truth, you can engage the entire organization in addressing security issues and promoting a cohesive approach to cybersecurity.

HADRIAN

Proactive Security with CTEM

As outlined, reactively defending the perimeter is an impossible task for the security teams in the retail sector. Gartner has outlined continuous threat exposure management (CTEM) as a program that surfaces and proactively prioritizes threats to an organization's security.

Gartner's CTEM program is specifically designed to help organizations manage large, complex, and dynamic environments. The core components of CTEM are:

- continuous visibility of exploitable risks
- intelligently prioritizing threats
- quickly actioning remediation

Maturity Model

> Continuous threat exposure management is a pragmatic and effective systemic approach to continuously refine priorities and walk the tightrope between two modern security realities. Organizations can't fix everything, nor can they be completely sure what vulnerability remediation they can safely postpone.
>
> Jeremy D'Hoinne - VP Analyst, Gartner [4]

> By 2026, organizations prioritizing their security investments based on a continuous exposure management program will be 3x less likely to suffer from a breach.
>
> Gartner

HADRIAN

How Hadrian Can Help?

Solution Guide

Continuous visibility	Intelligent prioritization	Quick remediation
Real-Time Discovery Hadrian monitors the entire internet to map your attack surface, identifying new infrastructure the moment it appears.	**Automated validation** Hadrian's platform confirms which risks are exploitable before reporting them, providing step-by-step reproduction instructions.	**Workflow automation** Hadrian streamlines remediation with customizable tools to automatically trigger specific actions.
Complete scope Hadrian provides a complete view of your external attack surface, giving you visibility of every potential attack vector for your infrastructure.	**Threat Intelligence** Hadrian enriches risk data with the latest cyber intelligence to identify which exploits are being actively used by threat actors.	**Collaboration tools** Hadrian's platform removes information silos with intuitive features, such as Secure Share, to engage with teams across the organization.
Comprehensive assessments Hadrian's AI-driven platform can identify the widest range of threats for complete awareness of risk.	**Context enrichment** Hadrian considers the technical impact and business context of the asset when calculating risk prioritization.	**Regression testing** Hadrian confirms whether remediation has been successful by automatically conducting regression for two weeks to verify that the risk is resolved.

HADRIAN

About Haddrian

Hadrian provides the hacker perspective, revealing the targets and methods that could be used in a real-world data breach. Hadrian's continuous and comprehensive testing discovers and validates risks completely autonomously.

Hadrian's platform combines attack surface discovery, automated penetration testing, and threat exposure management technologies in a cloud-based and agentless platform. The cutting-edge technology is constantly updated and improved by Hadrian's in-house hacker team.

Trusted by market leaders

Leroy Merlin Case Study

ABN·AMRO
SHV ENERGY
macmillan education
CTC GLOBAL
WeatherTech
LEROY MERLIN
LOTTOMatica
CA
RITUALS...
BIOLANDES
nedap
Van Oord

HADRIAN

Sources

[1] - Zippo (2023) 'Essential Cybersecurity In Retail Statistics 2024'

[2] - Trend Micro (2022) 'Mapping the Digital Attack Surface: Why Global Retail Organisations are Struggling to Manage Cyber Risk'

[3] - Arctic Wolf (2023) 'The State of Global Security Operations'

[4] - Gartner (2023) ‘How to Manage Cybersecurity Threats Not Episodes’