REPORT

Retail security trends and the impact of artificial intelligence

LUMEN®

Table of contents

Security trends in retail 4
- Vulnerabilities 4
  - Phishing/email compromise 4
  - Internet of Things (IoT) devices 4
  - Human error and staffing challenges 5
- Increasing cyber threats 5
  - Ransomware 5
  - Supply chain attacks 6
  - AI-driven threats 6
- Cost of a breach 6
- Regulations and policies impacting retail IT 7
- Artificial intelligence 7
  - Uses of AI in retail 7
  - The role of AI in retail security 8
- Recommendations for IT security in retail 8
  - Strengthen cybersecurity posture 8
  - Foster a culture of security 9
  - Prepare your network 9
- How Lumen can help 9
  - Networking and security solutions 9
- The bottom line 11

Introduction

The retail industry has increasingly relied on technology to improve customer experiences, streamline operations, reduce risk and enhance overall efficiency. We've come a long way from the manual "knuckle breaker" credit card machines, which relied on physical imprints and carbon paper forms, to “checkout free” stores that use advanced technologies like computer vision, sensors, and AI to create a seamless shopping experience. This transformation has revolutionized the shopping experience, blending efficiency and innovation to meet the demands of a fast-paced world.

This reliance on technology, however, has also made retail organizations prime targets for cyber threats. One recent report concluded that a whopping 80% of retailers experienced cyberattacks in the past year.[1]

It is easy to see why the industry is so highly targeted. Financial gain is the primary motivator behind cyberattacks, and retail organizations store vast amounts of sensitive customer data that can be exploited for identity theft, financial fraud, or ransomware if it falls into the wrong hands.

In recent years, the integration of artificial intelligence (AI) into retail has brought both opportunities and challenges from a cybersecurity perspective. AI has emerged as a powerful tool in retail, offering solutions for predictive analytics, personalized shopping experiences, and automated administrative tasks. At the same time, the integration of AI has introduced new vulnerabilities and ethical concerns that must be addressed. For example, the retail industry typically has IT infrastructure with numerous connected devices and third-party vendors, which increases the potential attack surface and makes it harder to secure

In this report, we explore the state of cybersecurity and compliance in retail, along with the impact of an AI-driven future. By understanding these dynamics, retail organizations can be better prepared to avoid and mitigate technology-related risks.

Security trends in retail

We begin this report by looking at retail's most common security vulnerabilities and attack types, followed by the rising costs of breaches and the fluid regulatory landscape that impacts retailers worldwide.

Vulnerabilities

The retail industry has faced many of the same vulnerabilities for several years, but AI is changing the game for both threat actors and cyber defenders.



Phishing/email compromise

Phishing continues to be a prevalent method for cybercriminals to gain unauthorized access to retail systems. A recent report highlights that 58% of attacks in the retail sector originated from phishing incidents.[2] These scams often target employees and trick them into revealing login credentials or other sensitive information that can be used to infiltrate the company's network.

Internet of Things (IoT) devices

The proliferation of IoT devices is a multi-faceted vulnerability for retailers. Some of the issues these devices create include:

- **Increased attack surface and complex interconnectedness.** Retailers use IoT devices to enhance operational efficiency, improve customer experiences, and streamline inventory management. Tools such as smart shelves and in-store sensors provide real-time data that help retailers make informed decisions, automate processes, and personalize customer experiences. However, the integration of these devices also introduces significant risks as each connected device becomes a potential entry point for threat actors, increasing the vulnerability of the retailer's network. IoT devices can also be susceptible to physical tampering and data breaches, which can compromise sensitive customer information and disrupt operations.
- **Weak authentication.** Many IoT devices have weak authentication mechanisms such as default credentials or simplistic passwords, and these vulnerabilities make it easier for attackers to gain access to the target network. In 2025, the resurgence of the Mirai botnet, known as "Mirai Resurrection," exploited weak authentication to compromise millions of devices, demonstrating the severe impact of inadequate security practices.[3]
- **Inadequate firmware updates.** IoT devices often lack regular firmware updates, leaving them exposed to known vulnerabilities. Retailers may struggle to keep all devices updated – especially if they deal with a large number and variety of devices – which can lead to security gaps for threat actors to exploit.[2]
- **Insecure application programming interfaces (APIs).** Insecure APIs are common in IoT devices, and they can provide attackers with opportunities to gain network access and compromise sensitive information.
- **Point of Sale (POS) systems.** POS systems are critical for retail operations, but because they handle sensitive payment information, they are attractive targets for cybercriminals. Additionally, POS systems are susceptible to malware and RAM scraping attacks, which can harvest credit card data and

compromise customer information.[4] As retailers continue to digitize their operations, the complexity and interconnectedness of POS systems increases and can further expose them to sophisticated cyber threats.

Human error and staffing challenges

Human error, often linked to inadequate cybersecurity training, is a leading cause of data breaches in the retail industry. A recent survey from VikingCloud looked at the biggest cybersecurity challenges for retailers and found three of the top four issues relate to an overextended workforce:

Whether it's phishing scams, IoT devices, POS systems or human error, these vulnerabilities highlight the urgent need for retailers to implement comprehensive cybersecurity measures to protect their systems and customer data.



Increasing cyber threats

As retailers seek to mitigate the above-listed vulnerabilities, threat actors continually look for opportunities to launch catastrophic attacks and steal data. Some of the most common types of attacks on the retail industry include:

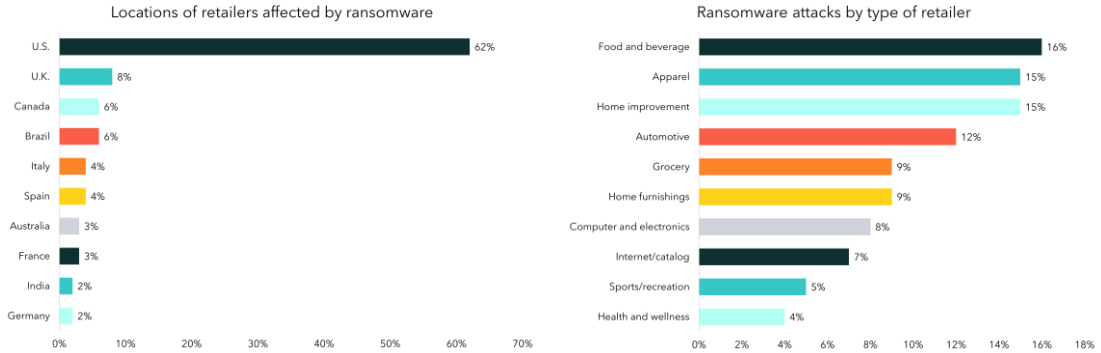
Ransomware

Ransomware remains a significant threat to retailers, with cybercriminals increasingly targeting retail systems to encrypt sensitive data and demand hefty ransoms for its release. According to a recent report from TrustLabs, the vast majority of retail ransomware attacks occur in the United States.[5] In addition, the sub-industries vary widely from food and beverage, to apparel, automotive, home improvement and more.[4] This underscores that no subsector is immune, and the latest cybersecurity measures are a "must have" for all retailers.

Figure 1

Locations of retailers affected by ransomware; types of retailers most impacted by ransomware

Source: Trustwave | Nov.2024



Supply chain attacks

Supply chain attacks are dangerous because they enable threat actors to target multiple retailers by exploiting vulnerabilities in a single supplier's software. The interconnected nature of modern retail operations exposes retailers to a larger attack surface and could potentially make them vulnerable to attack. According to a recent report from SecurityScorecard, nearly one-third of breaches involved a third-party attack vector, with ransomware groups focusing on software supply chains.[6] Another survey found that inadequate cybersecurity training among temporary employees, which are common in retail, exacerbates these vulnerabilities.[7]

AI-driven threats

The rise of AI-driven cyberattacks poses a new challenge for large retailers, and a few types of attacks are particularly prominent in the retail industry. These include:

- **Business logic abuse.** A recent report from Viking Cloud found that business logic abuse is the most common AI-driven attack on retail sites, accounting for 30.7% of all attacks.[8] This type of attack occurs when threat actors exploit the intended functionality of an application to achieve unauthorized outcomes. For example, they may manipulate promotional codes or exploit return policies to obtain goods or services at a lower price. The danger of this threat is multiplied by AI's ability to analyze patterns in user behavior and identify potential loopholes. As attackers use AI to devise more effective exploitation strategies, retailers must implement stringent controls to monitor and validate user actions on their platforms. Without these protective measures, retailers risk substantial financial losses and damage to their reputation.[7]
- **Distributed Denial-of-Service (DDoS).** DDoS attacks continue to be a persistent threat, and cybercriminals are using AI to orchestrate complex attacks that overwhelm retail websites. Imperva's latest DDoS report noted a 61% increase in application-layer DDoS attacks on retail sites, with the holiday season being the most targeted time for retailers.[9] This is particularly devastating for retailers that rely on online sales, as just a few minutes of downtime can cost millions.

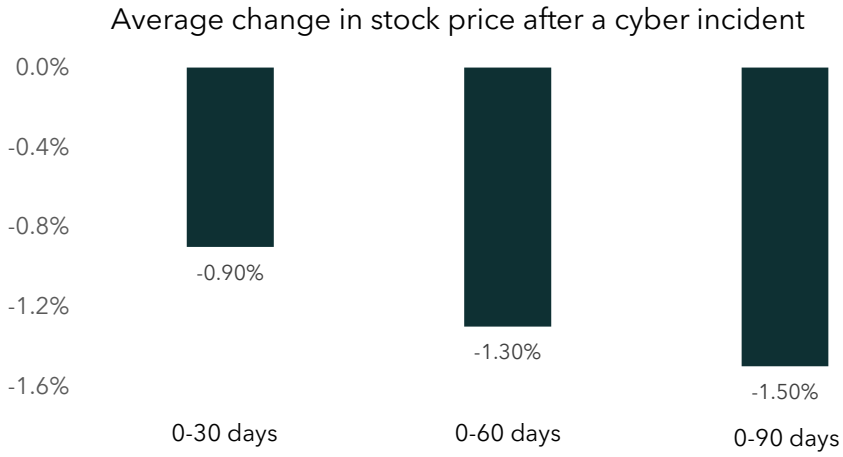
Cost of a breach

Cybersecurity breaches have a substantial financial impact on the retail sector, encompassing direct monetary losses, operational disruptions and reputational damage. In 2024, the retail industry reported a 24% increase in ransomware incidents compared to the previous year, with 256 incidents in the U.S. alone.[10] The financial repercussions of these breaches are significant, with businesses facing costs related to recovery, regulatory fines, decreased productivity and loss of customer trust. Additionally, Ernst & Young recently reported that companies experiencing cyber incidents typically see their stock price decrease by 1.5% over the following 90 days.[11]

Figure 2

Average effect of a cyber incident on a company's stock price over time.

Source: Ernst & Young, 2025



Regulations and policies impacting retail IT

Compliance in the retail industry is increasingly intertwined with cybersecurity and AI, reflecting the sector's evolving digital landscape. Retailers must adhere to stringent regulations like the Payment Card Industry Data Security Standard (PCI DSS) to safeguard customer payment information. Additionally, the integration of AI in retail operations necessitates compliance with frameworks such as the EU AI Act, which sets standards for ethical AI use.

These regulations aim to protect consumer data, ensure transparency, and mitigate risks associated with AI-driven decision-making. Failure to comply can result in severe financial penalties and damage to brand reputation. Retailers must prioritize robust cybersecurity measures and ethical AI practices to maintain consumer trust and operational integrity.

National Retail Federation (NRF) recommendations

NRF's Principles for the Use of Artificial Intelligence in the Retail Sector supports the industry's artificial intelligence governance and strategic planning. The principles encourage appropriate and effective governance of AI, promote consumer trust, and facilitate ongoing innovation and beneficial use of AI technologies.[12]



AI regulations

Regulations like GDPR and CCPA set standards for data protection and privacy, requiring retailers to follow strict guidelines. These regulations help protect consumers and ensure ethical AI use.[13] Future trends may include increased transparency requirements, stronger consumer rights regarding data usage, and stricter data security measures. These changes aim to protect consumers and ensure fair AI practices.[14]

Ethical considerations

The Institute of Electrical and Electronics Engineers (IEEE) and the European Union have published principles and guidelines for the ethical use of AI. While the IEEE focuses on ensuring AI is designed and used responsibly, the EU emphasizes the need for AI to be lawful, ethical, and robust. For both organizations, the principles and guidelines include[14]:

- **Fairness:** Ensure AI systems are fair and do not discriminate.
- **Transparency:** Make AI decision-making processes clear and understandable.
- **Accountability:** Hold entities responsible for the outcomes of AI systems.
- **Privacy:** Protect the data and privacy of individuals.

Artificial intelligence

Artificial intelligence and machine learning are the newest trends impacting security in the retail industry. Given the vulnerabilities and increasing cyber threats outlined above, it's important to look at the role of artificial intelligence in the retail industry.

Uses of AI in retail

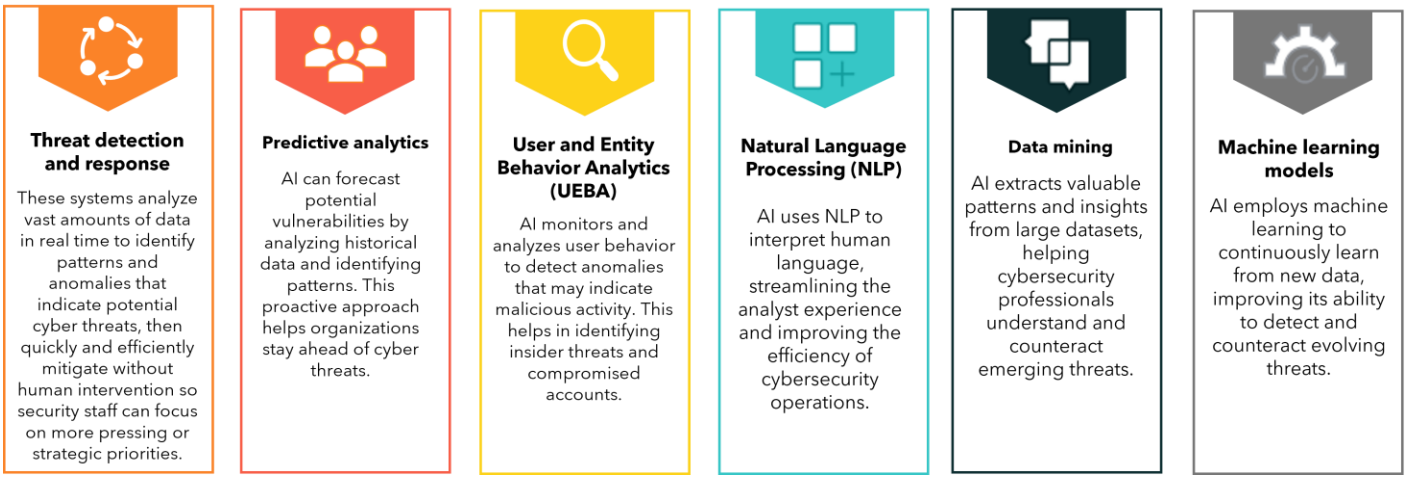
Some of the ways we're already seeing AI used in the retail sector include:

- **Personalized Shopping Experiences**: AI algorithms analyze customer behavior, preferences, and past purchases to provide personalized recommendations and targeted marketing. This creates a more engaging and relevant shopping experience, increasing customer loyalty and conversion rates.

- **Inventory Management:** Machine learning models predict demand and optimize inventory levels, reducing stockouts and overstock situations. This helps retailers manage their supply chains more efficiently.
- **Customer Service:** AI-powered chatbots and virtual assistants provide instant support to customers, answering queries and resolving issues. This improves customer satisfaction and reduces the workload on human staff.
- **Fraud Detection and Security**: AI systems detect fraudulent activities and enhance security measures by analyzing transaction patterns and identifying anomalies.
- **Dynamic Pricing:** AI enables dynamic pricing strategies, adjusting prices in real-time based on demand, competitor pricing, and customer preferences. This helps retailers optimize revenue and offer competitive deals.
- **Predictive Analytics:** Machine learning models analyze historical data to forecast future trends, helping retailers make informed decisions about product launches, marketing campaigns, and inventory planning.

The role of AI in retail security

As retail enterprises implement AI to innovate, manage inventory and improve customer experiences, threat actors are weaponizing AI to create highly targeted campaigns. Retailers, in turn, are using AI-driven security solutions to help stop attacks before they occur. Some of these include:



Recommendations for IT security in retail

Given the vulnerabilities, threats, regulatory and ethical concerns, and AI-powered attacks impacting the retail industry, immediate, proactive steps are necessary to mitigate overall risk.

Strengthen cybersecurity posture

Investing in advanced, AI-driven security tools is essential. AI-backed cybersecurity technologies can protect sensitive customer data by quickly identifying fraud and blocking bad actors, thereby maintaining safe experiences and building trust between retailers and their stakeholders.

In addition, real-time data processing requires faster speeds for retailers to implement dynamic pricing, real-time inventory management and more. This is why edge solutions integrated with AI can enhance retail operations by keeping data close to the source and reducing latency.

Finally, regular audits and penetration testing are crucial to identify and address vulnerabilities, ensuring that retailers remain resilient and manage risks.

Foster a culture of security

A culture of security ensures that all stakeholders are aware of and actively engaged in protecting customer and company data. Continually training staff about best practices and encouraging collaboration between IT and retailers can significantly enhance the security posture of the organization. Retail enterprises should implement AI- and cloud-ready technologies to support scalable and secure data management.



Prepare your network

As we have seen, AI is transforming retail in profound ways. But an AI-enabled future requires preparation, and retailers' networks must be able to handle the increased data demands as more and more AI solutions are brought online. This is because AI applications process vast amounts of data in real-time, which can quickly overwhelm outdated systems and cause them to struggle to efficiently process and store data. The subsequent delays and operational errors can lead to financial loss and poor customer outcomes. Additionally, reliance on legacy infrastructure can expose critical weaknesses, which makes it easier for cyber attackers to exploit vulnerabilities and gain unauthorized access to sensitive information.

Upgrading to modern, secure systems is essential to be able to effectively handle the data-intensive requirements of AI technologies. Without modernized network infrastructure, retail organizations risk data bottlenecks, delays in critical diagnostics, and potentially compromised patient care.

By upgrading their networks, retail companies can help ensure seamless data flow, which can improve company and customer outcomes while helping decrease costs and minimize risks.

How Lumen can help

Networking and security solutions

With the integration of AI into retail, the demand for high-capacity, low-latency networks has never been greater. Lumen networking solutions are designed to support retailers as they prepare for this AI-enabled future. Our robust infrastructure, including our extensive fiber network and advanced AI-driven security solutions, ensures that retail organizations can leverage AI technologies to enhance customer experiences, streamline operations, and improve inventory accuracy.

Lumen provides the following networking and security solutions:

- **Control network connectivity and save money:** *Lumen® Network-as-a-Service (NaaS)* provides real-time, self-service, scalable control over network connectivity, enabling businesses to manage, bandwidth, path, and latency dynamically.
- **Lower costs, reduce downtime and enhance customer experiences:** *Lumen® DDoS Mitigation* services provide comprehensive protection against DDoS attacks by rapidly filtering malicious traffic and returning clean traffic to customers, leveraging a multi-layered scrubbing architecture and advanced threat intelligence from Black Lotus Labs.
- **Reduce risk:** *Lumen Defender℠ powered by Black Lotus Labs®* offers proactive network protection by automatically blocking traffic from risky sources before it breaches internal networks, leveraging unmatched threat intelligence.

- **Simplify networking and security:** *Lumen® SASE Solutions* unify network and security management through a centralized, cloud-based experience, simplifying the design, purchase, deployment, and orchestration of software-defined network infrastructure and information security.
- **Save costs and scale on your terms:** *Lumen® SD-WAN* solutions support secure, scalable, and cost-efficient deployment and management of hybrid networks, providing complete visibility, control, and security across various connectivity types.
- **Optimize efficiency for customers and employees:** *Rapid Threat Defense* integrates Black Lotus Labs intelligence to proactively block known malicious traffic, enhancing operational efficiency and reducing the burden on IT staff.
- **Focus resources, minimize expenses:** *Lumen Security Operations Center as a Service (SOCaaS)* offers fully managed cybersecurity threat detection, incident management, and response support, providing visibility across an agency into cyber activity.
- **Reduce costs and risks:** *Lumen Incident Reporting* system ensures prompt reporting and management of risk-related incidents involving company employees, vehicles, and facilities, facilitating rapid response and resolution.

BLACK LOTUS LABS® by Lumen

Black Lotus Labs® is the award-winning, in-house threat research arm of Lumen. The team of data scientists, reverse engineers, security engineers, and threat analysts leverages their unmatched visibility into the Lumen network to protect businesses and help keep the internet clean.

Black Lotus Labs use advanced threat technology to identify and eliminate threats quickly, employing machine learning algorithms to automate protection and neutralize threats. The team has been involved in the identification and takedown of some of the most high-profile malware of the past decade.

- **Reduce workloads while defending critical apps and data:** Lumen's managed and professional security solutions provide comprehensive protection through proactive threat monitoring, incident response, penetration testing and tailored advisory services, ensuring robust security and compliance for businesses.

By providing secure, high-speed connectivity and real-time data processing capabilities, Lumen helps enable retailers to implement AI applications that help improve customer experiences, minimize security and compliance risks, reduce costs and increase revenue.

Lumen has won three consecutive Cybersecurity Breakthrough Awards including 2022 Network Security Provider of the Year, 2023 SASE Solution of the Year, and 2024 Threat Intelligence Company of the Year.







LUMEN®

The bottom line

The integration of AI into retail presents both opportunities and challenges in the realm of cybersecurity. By understanding current security trends, vulnerabilities, regulatory changes and the impact of AI, retail organizations can better prepare for and mitigate cyber threats. Implementing robust security measures, staying updated with regulations, and fostering a culture of security are essential steps in safeguarding customer and corporate data while ensuring the continued advancement of retail technology. Contact an expert about securing your retail enterprise today.

Your network infrastructure is the cornerstone of your AI efforts

The Lumen network supports the dynamic demands of AI-powered technologies and enhances customer experiences by providing high-capacity connections, deep IP peering and AIOps to leverage AI/ML apps without the constraints of a traditional network.

View security solutions

Footnotes

[1] Retail Cybersecurity Stats, Threats, and Solutions for 2025 | VikingCloud | April 2025
[2] Trustwave SpiderLabs Unveils Top Cyber Threats Facing Retailers in 2024 | November 2024
[3] Internet of Things (IoT) Vulnerabilities: A Critical Challenge in 2025 | Hoplon Infosec | March 2025
[4] POS System Security Risks & How to Protect Your Business in 2025 | POS USA | March 2025
[5] Trustwave SpiderLabs Unveils Top Cyber Threats Facing Retailers in 2024 | November 2024
[6] SecurityScorecard 2024 Global Third-Party Cybersecurity Breach Report | February 2024
[7] Retail Cybersecurity Stats, Threats, and Solutions for 2025 | VikingCloud | April 2025
[8] Cyber Threats That Could Impact the Retail Industry This Holiday Season (and What to Do About It) | The Hacker News | Nov. 2024
[9] 2024 Imperva DDoS Threat Landscape Report | Imperva | July 2024
[10] Retail Threat Landscape | Cyberint | November 2024
[11] Cyber study: How the C-suite disconnect is leaving organizations exposed | Ernst & Young | 2025
[12] Principles for the Use of Artificial Intelligence in the Retail Sector | NRF | November 2023
[13] Ensuring Ethical AI Use in Retail: Challenges and Solutions | Redress Compliance | August 2024

This content is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen products and offerings as of the date of issue.

Why Lumen?

Lumen is your single provider to enable digital transformation. With a comprehensive portfolio and experienced talent, we can help safeguard your customer experience, protect your confidential data, and manage threats. Backed by the extensive and deeply peered Lumen global network, Black Lotus Labs® threat intelligence, and our skilled and experienced team of security experts, Lumen is a trusted partner to help improve your security posture.

866-352-0291 | lumen.com | info@lumen.com

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice. ©2025 Lumen Technologies. All Rights Reserved.

LUMEN®