9 CRITICAL CYBERSECURITY FACTS FOR RETAILERS

In the cutthroat retail landscape, your data's safety can set you apart. Here are nine cybersecurity and compliance facts every retailer must know.

1 Retailers Are Primary Targets for Cyberattacks

Retailers are hot targets for cyberattacks, with 24% of all attacks being directed at retailers to access personal payment data they process. Retail reported a 75% increase in the rate of ransomware attacks over the last year. Only 22% of retailers train employees in cybersecurity, which is an issue since ransomware starts with phishing.

2 Consumers Won't Do Business with Retailers Who Are Breached

Clients won't purchase from you if you're hit with a cyberattack and thanks to retail attacks, such as JD Sports in 2023 and CVS in 2021, trust in retailers is low. In fact, according to a 2023 report, 59% of customers would avoid doing business with organizations who experienced a cyberattack in the past year.

3 Cyberattacks Are Costly to Retailers, No Matter Your Size

Retailers of all sizes have to deal with the consequences of cyberattacks, including:

- Financial Cost
- Legal Consequences
- Consumer Trust
- Limited Cyber Insurance Payouts

4 Cyber Insurance Drives Retail Cybersecurity Investment

97%

97% of retailers have upgraded cyber defenses to secure coverage.

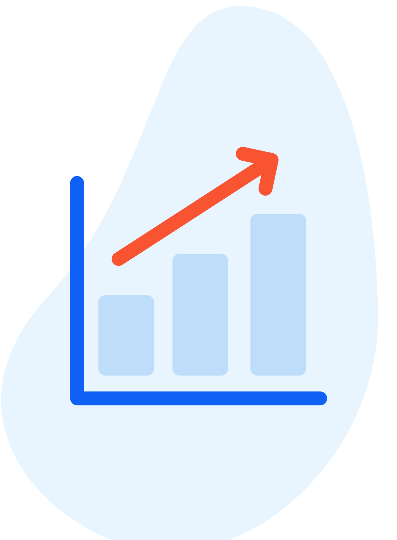
88%

88% of retailers reported having cyber insurance coverage against ransomware; the second highest rate across industries.

35%

Despite cybersecurity investment, retail has one of the lowest ransom payout rates by insurers at 35%.

* Stats according to a 2022 State of Ransomware in Retail Report.



5 Cybersecurity Budgets Are Increasing

In 2023, retailers were increasingly investing in cybersecurity as a response to the growing threat of ransomware.

70% of CISOs anticipated that their budgets would increase in 2023, according to the CISO Benchmark Report from the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC).

The rise in budget and staff for cybersecurity shows it has become vital for retail operations.

6 PCI DSS v4.0 Compliance Deadline is Fast-Approaching in March of 2024

PCI DSS compliance is a well-known requirement for most retailers, but the new v.4.0 compliance requirements come into effect on March 31, 2024, and contains 63 new requirements retailers need to account for. Retailers should consider partnering with a knowledgeable MSP to prepare for these new compliance changes.

7 PCI DSS v4.0 Has New Requirements

- ✓ Expanded MFA
- ✓ Phishing & Breach Requirements
- ✓ Specifications of Roles & Responsibilities
- ✓ Password Specifications
- ✓ Security Controls Procedures
- ✓ Compliance Activities Enhancements
- ✓ Encryption & Network Security
- ✓ Higher Frequency of Security Controls Testing
- ✓ Comprehensive Risk Assessments
- ✓ Annual Penetration Tests
- ✓ Quarterly Vulnerability Scans

8 Retailers Should Partner with an MSP

Consider partnering with an MSP if:

- You need specialized expertise in cybersecurity
- Your IT team is stretched too thin
- You want your IT team to focus on other tasks

9 Consider TPx

Retailers like to choose TPx because:

- TPx offers PCI DSS-compliant solutions
- TPx has hundreds of retail clients
- TPx offers a PCI DSS gap assessment

In a dynamic retail environment, let a dedicated partner like TPx handle your security challenges. Equip your IT team with the resources and peace-of-mind they need to prioritize revenue-generating operations.

Learn More About How TPx Helps Retailers Stay Competitive

LEARN MORE

TPX
www.tpx.com