Interface

How Digital Transformation Can Open Doors for Retail Cybersecurity Attacks

Retailers are Investing in Digital Transformation

60% retailers have either implemented digital transformation initiatives or are in the process of implementing digital transformation projects.[1]

Primary focus of digital transformation: Customer Experience · Workforce Experience · Supply Chain Optimization

Digital Transformation Projects Can Create Security Vulnerabilities

Retailers' data lakes are attractive targets, often combining detailed identity and demographic data with credit card information. [2]

24% organizations sacrificed the security of mobile devices to facilitate their response to restrictions put in place due to the pandemic. [3]

76% organizations said that they'd come under pressure to sacrifice the security of mobile devices for expediency.

8% percent of consumers are confident that retailers will be able to navigate the challenges of a data breach [4]

Retailers are apparently more likely to pay off ransomware attackers. Of those that experienced such an attack, 51% paid the ransom directly (versus 37% of their peers in other industries). [5]

Retailers surveyed tend to have smaller SOCs than their peers[6]

8% report that their SOC consists of more than 50 FTEs (versus 20% of SOCs across industries).

33% say the cybersecurity team being understaffed for the size of their organization is a top challenge (versus 25% across other industries).

4

Four basic security policies are needed for today's enterprise

01 Restrict access to data on a need-to-know basis.

02 Encrypt sensitive data sent across open public networks

03 Regularly test security systems and processes

04 Change all default, vendor-supplied processes

14% of organizations complied with all four requirements in 2018

Only 9% of organizations complied with all four requirements in 2021

Retail Cybersecurity Threats - Targets, Actors & Implications

Targets

84%	attacks include one of the following - System Intrusion, Social Engineering, Basic Web Application attacks

Threat actors

87%	Extrernal actors
13%	Internal actors

Data lost

45%	Credentials
27%	Personal
25%	Other
25%	Payment

Data compromised

45%	Credentials
27%	Personal
25%	Other
25%	Payment

Cybersecurity Risks Have Gone Mobile[7]

Retailers are betting big on enabling employees to work from anywhere. Convenience is now offered in the form of:

- BYOPC (Bring Your Own PC)
- BYOD (Bring Your Own Device)
- CYOD (Choose Your Own Device)
- COPE (Company Owned Personally Enabled)
- COBO (Company Owned Business Only)

The top compromised asset varieties were

- 88%
- 14%
- 10%

40% respondents said mobile devices are their company's biggest IT security threat

31% respondents agreed that mobile device threats were growing faster than other threats.

How Can Retailers Secure Mobile Devices?[8]

- Define a BYOD and WFM policy
- Implement Mobile Device Management (MDM) solutions
- Implement Endpoint Detection and Response (EDR) solutions
- Implement Data Loss Prevention (DLP) solutions
- Implement Mobile Threat Defense (MTD) and Unified Endpoint Management (UEM)
- Provide adequate training to employees and IT teams

Cybercriminals Are Checking Out POS

Cybercriminals Are Checking Out POS

Retail chains face a variety of security challenges, from connected POS systems and devices to online ordering and delivery applications.

Self-checkout solutions in the Retail Environments setting could generate $430 billion to $520 billion in economic value in 2030.

Adoption of self-checkout use cases is expected to increase from a relatively low 15 to 35 percent of organized retail today to 80 to 90 percent in 2030.[9]

In-store purchases are vulnerable to fraudulent purchases according to 49.3% of retailers. Multichannel purchases (bought online and picked up in-store) are vulnerable to fraudulent activities according to 18.8% of retailers. (NRF, 2020)

Modus Operandi of a POS data breaches

POS applications are directly connected to credit card data, loyalty management applications, and inventory management systems. They are easily accessible to anyone and retailers struggle to manage the sheer number of in-store terminals, self-service kiosks, mobile payment devices, and phone-based payments directly from customers.

62% attacks on POS environments are completed through remote access.[10]

Scamsters rely on "shimming" and man-in-the-middle (MITM) attacks to impersonate EMV credit cards at the POS. [12]

In 2019, an employee clicked on a malicious link in a phishing email and downloaded a Remote Access Trojan. The attackers used the Trojan to move laterally into the merchant's PoS environment where they deployed a RAM memory scraper for harvesting payment card data. [11]

Data breaches are expensive

$3.28M is retail industry's average cost of a data breach (IBM Cost of Data Breach Report, 2022)

How Can Retailers Secure POS?

- Encrypt all POS data end-to-end
- Implement EMV and NFC technologies
- Whitelist applications to run on a POS system
- Keep your POS software up-to-date
- Segment the POS network
- Address PCI-DSS compliance gaps proactively
- Physically secure POS devices including mobile POS devices
- Watch out for unusual transactions
- Integrate security camera with POS transactions

Cyberattacks on the Cloud

50% of retailers surveyed have a cloud-first policy for new applications compared to 38% of organizations across other verticals.[13]

Cloud misconfiguration accounted for 15% of the breaches and costs the company $4.14 million on average.[14]

Malware targeting Linux environments rose dramatically in 2021—a surge possibly correlated to more organizations moving into cloud-based environments, many of which rely on Linux for their operations. [15]

Cloud Security Maturity

17%	Not have any specialized security measures
26%	Begun applying cloud security practices
34%	Apply many security practices
23%	Consistently apply security practices

Sky-High Cost of Cloud Security Breaches[16]

- Hybrid cloud: $3.8M
- Private cloud: $4.2M
- Public cloud[17]: $5M

How Can Retailers Secure the Cloud?

- Adopt a zero trust security model to help prevent unauthorized access to sensitive data
- Understand the scope of cloud service provider security responsibilities
- Protect sensitive data in cloud environments using policy and encryption
- Organize ongoing security awareness training for all employees
- Invest in security orchestration and automation of response (SOAR) and extended detection and response (XDR) to help improve detection and response times

Loyalty Programs and Gift Cards

22% consumers shop exclusively with retailers to take advantage of loyalty programs.

$140 billion Estimated value of loyalty points in the US

$100 billion Estimated value of rewards that go unclaimed

$259B by 2026. The gift card market in the US will increase from US$172 billion in 2021 to reach US$259 billion by 2026.[18]

5X number of gift card cyberattacks when compared to other targets

Impact of Loyalty and Gift Card Fraud

01 Estimated value of rewards fraudulently redeemed each year: $1 billion [19]

02 The FTC estimates an 88% increase in gift card scams in 2021 based on 64,000 consumer complaints that amount to a collective loss of $233 million.

03 Any data breach involving loyalty management applications could potentially attract regulatory fines under the provisions of the California Consumer Privacy Act (CCPA) and GDPR

Loyalty account takeover fraud is a ticking timebomb. According to Forter, "As fraudsters accrue more account data during this period, merchants should remain vigilant. Fraudsters are breaching accounts and stealing personal data, using this time to "age" the accounts they steal. They are taking the time to build the account's reputation, making it more difficult for rules-based systems or manual review teams to detect a hacked account from a legitimate one.

How Can Retailers Minimize Loyalty and Gift Card Frauds?

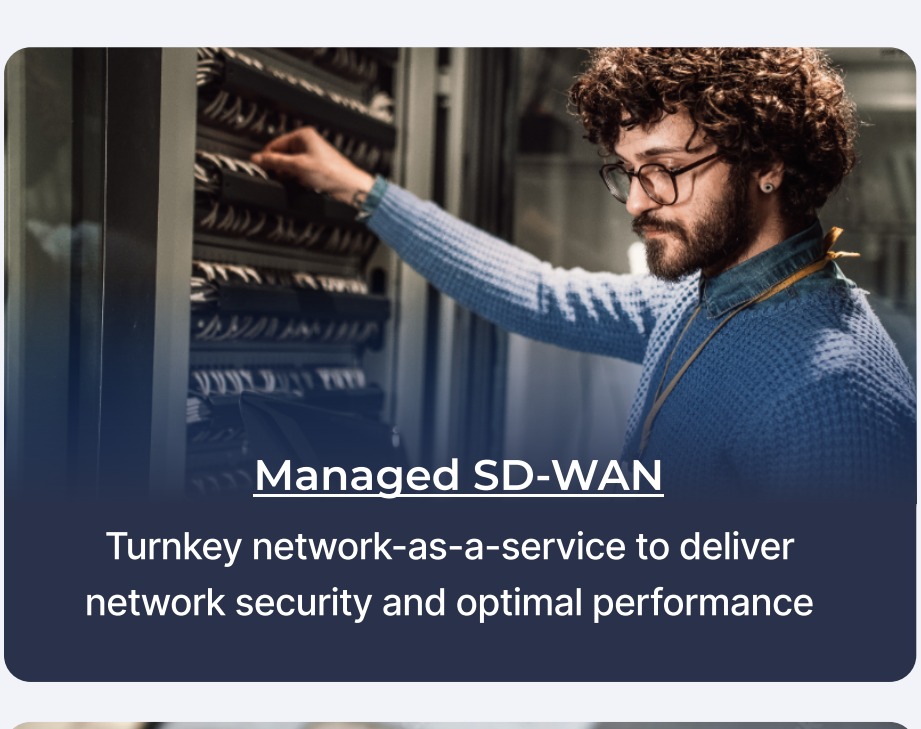
- Implement a robust data analytics system to flag suspicious transactions.
- Enforce password policies and encourage multifactor authentication.
- Limit the personal data needed to enroll in the rewards program.
- Regulate access to loyalty management systems and implement a zero trust security framework.

Accelerate Retail Digital Transformation with Interface

Interface's managed network services can help retail chains proactively address cybersecurity threats and accelerate digital transformation. Interface handles design, implementation, and maintenance for all services. With Interface, retail chains can improve security, eliminate operational complexity and focus on innovation.

Retail Network-Technology-in-a-Box

PCI-compliant LAN, WAN, Firewall, SD-WAN, and VoIP in one standardized package

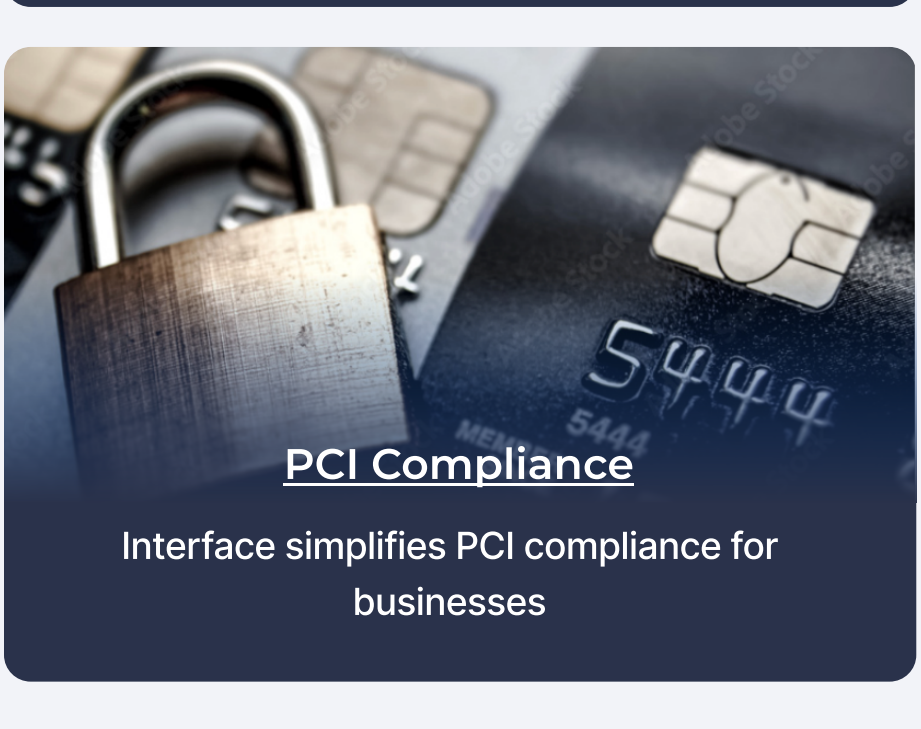


Managed SD-WAN

Turnkey network-as-a-service to deliver network security and optimal performance

Managed SASE

Unified ZTNA, FWaaS, SWG & SD-WAN solution



PCI Compliance

Interface simplifies PCI compliance for businesses

Schedule a Free Consultation

1https://www.bdo.com/BDO/media/Report-PDFs/Digital%20Transformation/2021-Retail-Digital-Transformation-Survey_Web.pdf
2https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it
3Verizon Mobile Security Index 2021
4Fiserv
5https://www.splunk.com/en_us/form/state-of-security/thanks.html
6https://www.splunk.com/en_us/form/state-of-security/thanks.html
72022 Verizon Data Breach Investigations Report
8https://www.verizon.com/business/resources/reports/mobile-security-index/
9https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it
10https://www.akamai.com/blog/security/understanding-point-of-sale-security
11https://www.darkreading.com/attacks-breaches/visa-warns-of-targeted-pos-attacks-on-gas-station-merchants
12https://www.experian.com/blogs/ask-experian/what-is-an-emv-chip/
13 14https://www.splunk.com/en_us/form/state-of-security/thanks.html
15https://www.ibm.com/security/data-breach/threat-intelligence/
16 17IBM Cost of Data Breach Report 2022
18https://www.globenewswire.com/en/news-release/2022/03/23/2408637/28124/en/United-States-Gift-Card-and-Incentive-Card-Market-Report-2022-Market-is-Expected-to-Grow-by-9-5-to-Reach-188-832-7-Million-in-2022-Forecast-to-2026.html
19https://www.forter.com/blog/loyalty-program-protection/