The bridge to possible

# Cisco Retail Thought Leadership

## The Security Risks of Digital Transformation for the Agile Retailer

## Adapting to a Changing Landscape

Every organization bears a responsibility to protect its customers' data. Cybercriminals will always look for new ways to get inside a network. A breach could ultimately result in damage to the brand, lost revenue, and loss in consumer trust. By adopting a zero-trust approach and implementing some basic cyber hygiene techniques, retailers can securely support future innovation, while being agile and responsive to changing business needs.

# The Security Risks of Digital Transformation for the Agile Retailer

In recent years, retailers have been forced to be more agile, responding rapidly to quickly changing business landscapes and consumer expectations. Retailers rushed to bring curbside and home delivery services to market and send their knowledge workers from the headquarters and contact center home in some hybrid capacity. Not infrequently, security took a back seat to the urgency of a business need and led to a spike in cybercrime against retailers.

Many transactions involve not only payment card information, but also some level of personal customer data. Retailers leverage advanced analytic tools to gather information on customer behavior, both online and in-store, allowing retailers to optimize product assortment, placement, and pricing in-store to drive increased margins and serve customers better.

So, how do retailers go about protecting the data they now rely on? They need to ensure they maintain Confidentiality, Integrity, and Availability, also known as the CIA Triad.

- Confidentiality – Only those authorized should have access, and only to the data they need.
- Integrity – Data should be securely stored and transmitted, and no one should be able to tamper with it.
- Availability – Authorized personnel should have access to the data, whenever needed.

## By the Numbers

According to Verizon's 2022 Data Breach Investigations Report, attacks against retailers have increased significantly over the last five years. Social engineering accounts for nearly one-third of all attacks and results in compromised credentials, which may be used at a later date to access business-critical data or to deliver malware or ransomware into the network.

Security Magazine supports that observation in stating that compromised usernames and passwords have risen by 300% since 2018. This data suggests that many organizations fail to meet the basic expectations of the CIA Triad, impacting their security posture and leaving them vulnerable to future threats.

# Protecting the Consumer and Retailer

The key tenets of any security operation are to reduce the probability of a successful cyberattack and mitigate the impact/loss should a breach occur.

Multifactor authentication (MFA) technologies, as part of a zero-trust or least-privilege approach, leverage an ID, password token, key, or code in some combination to ensure the user is who they claim to be and negate compromised credentials. The user's access is then limited to ensure they can only access data they should have access to.

Appropriate segmentation can then prevent lateral access to other systems or data sources the user is not authorized to access and can prevent propagation of malware and ransomware.

Retailers are increasingly moving workloads to cloud services, and more users are working, at least part-time, from home or on the road. New retail service offerings take the associate beyond the four walls of the store - from curbside and home delivery to the hybrid knowledge workers, appropriate access controls make sure that a trusted user can access appropriate data from a trusted location, and that those remote and edge locations can securely connect to corporate resources.

Availability is an area of the CIA Triad that is frequently overlooked. Any number of issues may prevent or degrade service availability, including cyberattacks. It is important that monitoring goes beyond discrete components of the network to assess end-to-end performance and reliability and detect and respond to potential issues in availability before they impact a user. This provides secure, consistent, reliable experiences for both consumers and associates, wherever they may be.

## More information

Visit these resources to learn more about:

- Retail Portfolio Explorer
- Retail Solutions
- Retail Cybersecurity
- Solutions to transform the IT experience