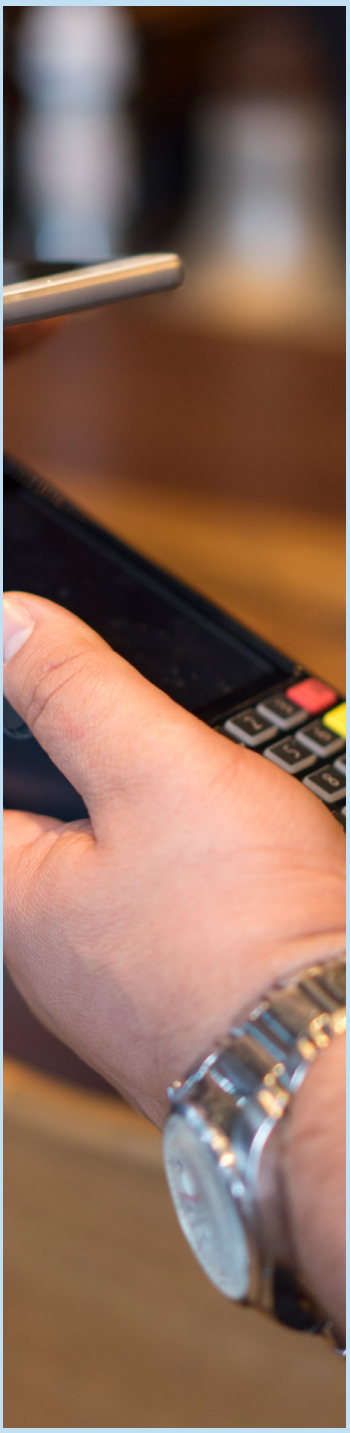
VIEW POINT



CYBERSECURITY SOLUTIONS FOR RETAIL AND E-COMMERCE INDUSTRY

Infosys®
Navigate your next

With the realignment of brick-and-mortar and direct to customer (DTC) models of retail, the evolving landscape is resting its future on online platforms. The adoption of digital technologies for an immersive user experience, personalized offers, frictionless checkouts, innovative loyalty programs & rebates, has laid the foundations for newer ways of retail businesses. Many traditional brick-and-mortar retail chains have begun investing heavily in digital technologies to stay afloat amidst the evolving consumer behavior.

The consumer shopping and buying behavior is highly influenced by various demographic factors. Consequently, retailers are challenged to manage the expectations of brand loyalists in baby boomer cohort on one side of the segment while also cater to digital native short duration loyalists in millennials & Gen Z on the other. Generally, retailers plot different demographic cohorts on the X-axis and the shopping behavioral attributes on the Y-axis to understand market patterns. The typical XY-plot for attributes of consumer behaviors and the respective demographic cohort is depicted below:

Once the retailers are ready with a market segmentation, they can plan a go-to-market strategy. Subsequently, the corresponding execution starts with the evaluation of online platforms such as BigCommerce, Shopify Plus, SAP Hybis, Magneto, Oracle ATG, Episerver and other integrated systems for the payments, analytics data storage and cybersecurity.

With the evolving landscape of Direct to Customer (D2C) and the emergence of significant demographic cohort of Digital Native Millennials and Gen-Z the traditional brick-and-mortar retailers have been forced to reimagine their existence with digital transformation. In the current scenario, be it the traditional retailers who are rewriting their go-to-market playbooks with the inclusion of in-house or outsourced digital transformation platforms, or the new gen retailers who are thriving on digital native advantages but with limited period of brand loyalty, they are continuously innovating to stay relevant in their consumer segments. Hence, there is a massive dependence on technology and its platforms. In order to render secure services virtually or physically, retailers and e-commerce companies need to consider cybersecurity and privacy protection as key attributes for business continuity.

The retail and e-commerce companies are segregated into 4 key categories for customized and easy implementation of cybersecurity strategies and programs

Type-1: Manufacturers with stores & online presence

- Stores with brick-and-mortar philosophy
- Embraced digital transformation
- Various Industries – Sports, Apparels, Fashion, Furniture, Home Products, Office Stationery

Type-2: Merchandisers with stores & online presence

- Stores with brick-and-mortar philosophy
- Embraced digital transformation

Type-3: E-commerce merchandisers

- Online sales in the business model
- Strong architecture with digital native core
- Embracing digital technologies very fast and playing major role in evolving the consumer buying behaviours
- They are aggregators of variety of industries and serve as the online marketplace for buyers and sellers.

Type-4: Retail-as-a-service providers

- Offerings for one or multiple business functions, like frictionless payment platforms, on demand shipping logistics, on demand e-commerce platform, AR-VR integrated platform for online immersive shopping experience, etc.

Getting along with cybersecurity

As retail and e-commerce businesses have evolved and embedded the "everything digital" philosophy in their ecosystem, the following two important aspects need to be considered with regards to cybersecurity

- Data Security
- Consumer Privacy or PII (personal identifiable information) security

Data is always considered as a key asset in the digital native era, and consumer privacy has been a growing concern amongst buyers and regulators. The 2018 enforcements of GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) compelled many online retail & e-commerce enterprises to redefine their security controls & data usage principles so as to not just detect, respond & report every data breach, but also prevent any kind PII abuse.

Data Security

Securing data at all times and in all forms is critical for all retail and e-commerce

companies. Organizations have been investing in traditional security controls like, perimeter security, VAPT (Vulnerability Assessment and Penetration Testing) engagements, and data loss prevention solutions. However, the traditional security controls and solutions may not be sufficient when it comes to today's data that may be at rest or in motion. The following table depicts data types with their respective objectives and cybersecurity goals.

Data Type	Data Objectives	Cybersecurity Goals
Customer Data	Customer information for loyalty programs; Loyalty points	PII protection, data breach detection and reporting, data masking
Transactions Data	For customers and sellers	PCI DSS compliance, dynamic data masking & encryption
Internal Data	Customers' and suppliers' data for business analytics on customer buying patterns/ behaviors	PII protection, data breach detection and reporting, data masking
Logistics Data	Understanding the spending vis-à-vis delivery performance	Security controls for the 3rd party integrations

PII Security

Personal Identifiable Information (PII) provide privacy information of consumers. This data is usually obtained when consumers make purchases online and need to divulge their basic information. But its important that retail organizations safeguard and not misuse any such information as mandated by consumer's laws like GDPR and CCPA enforcements of 2018. Additional security controls like data breach prevention, dynamic data making & encryption solutions, SaaS/PaaS cloud security solutions, etc. should be applied. According to the law, if a data breach with regards to a EU citizen's PII takes place, up to Euro 20 Million or 4% of the Global Turnover of the previous year, whichever is higher will need to be paid. The actual value will also depend on the compliance practices, data security hygiene, number of records in the breach, and total number of data elements in the breach.

Brick-and-Mortar Stores Security

Apart from the cybersecurity solutions for the online retail and e-commerce business models, retailers with brick-and-mortar stores too need to incorporate additional security controls. these controls include the Point of Sale (POS) systems, malware protection of the POS terminals, appropriate security controls for the building maintenance systems and the POS terminal networks.

88% of the attacks in Retail were either a malware or data breach.

20% of Big Box Retail customers would cancel their accounts if they are a victim of a data hack irrespective to retailer response

- KPMG Consumer Loss Barometer

Securing the Retail Sector – Robustly.

Data Security – Traditional methods

These controls ensure protection of the data crown jewels hosted in data centres or in self managed facilities

- **Perimeter Security Controls** - Firewalls, IPS, antivirus, identity & access management (IAM) solutions, jump server for remote administration
- **Applications Security** - Applications servers' OS hardening, automatic patch management, host anti virus & IPS
- **Security Services** - Frequent vulnerability assessment, periodic external & internal penetration testing
- **Physical Security** - It is applicable for the Brick-and-Mortar stores for the protection of the cash registers and POS systems and terminals

Data Security – Advanced methods

These controls are deployed over and above the traditional security controls to offer protection

- **Network Controls:** Advance Persistent Threat (APT) Protection, DDOS protection, data loss prevention solution
- **Applications Security:** File integrity monitor, hypervisor security, privilege identity management & privilege access management (PIM & PAM) solution for administrative access, Workloads Visibility
- **Security Services:** Periodic applications scanning, Static Applications Security Testing (SAST) & Dynamic Applications Security Testing (DAST) of the APK (for Android) / IPA (for iOS) apps whenever new updates are to be released, 24x7 security events monitoring
- **Insiders Threat Protection:** URL filtering, Web 2.0 applications control solution, Endpoint Data Loss Prevention (DLP), Endpoint Antivirus, User & Entity Behaviour Analytics (UEBA), Secured DNS
- **DevOps Security:** Additional security controls like VPN, SSL proxy, or reverse proxy for the applications development teams'

Data Security - Cloud Abstractions

These controls are necessary for all retail and e-commerce business entities that either have their infrastructure hosted with the help of a cloud service provider or are integrating their data interfaces with any cloud service provider. Irrespective to the abstraction of Cloud, viz. IaaS, PaaS, SaaS, or Serverless, that is delivered through an external entity, the security of consumers' data is the responsibility of the retailer or e-commerce entity. We recommend all the cybersecurity teams of retail/e-commerce companies to thoroughly study the shared responsibility matrix published by their respective Cloud Service Providers, like AWS, Microsoft Azure, Google GCP, Salesforce, SAP C4 and Snowflake and assess the risk associated with respect to consumer data based on the corresponding services or infrastructure taken from the Cloud Service Provider.

- **IaaS Security Controls:** If the company will be using hosted infrastructure in AWS, Google, Azure or Alibaba, all the network and application security controls described in the Advance Data Security section, will be as desired
- **PaaS or Serverless Security Controls:** Security solution for appropriate container access and container security needs to be mplemented. There are specific security controls for secured access to Kubernetes, Dockers, Lamda Function, etc. that may be taken for data assurance and security
- **SaaS Security Controls:** Cloud Security Access Brokers (CASB) or Apps specific Reverse Proxy Solutions are desired for the security of data exchange
- **Security Services:** VAPT, periodic external penetration testing including the cloud abstractions in use, applications scanning, SAST & DAST of the home grown apps, 24x7 security events monitoring, 24x7 cloud solution administrative anomaly detection.

PII Security

All the retailers and e-commerce merchants are expected to comply to PCI DSS 3.2.1. However, the retailers and e-commerce companies conducting business with citizens of the European Union and California State in USA, need to comply with GDPR or CCPA, respectively.

- PCI DSS 3.2.1 Compliance: The payments card industry data security standard has laid out the framework for one-time compliance and then periodic compliance before allowing the plastic money transaction. Once the assessment of compliance is completed the Attestation of the Compliance (AOC) through the authorized agencies has to be filed. As the PCI compliance is attained the merchant or retailer/e-commerce company has to file a periodic AOC. In order to ease the process PCI has also released the PCI DSS 3.2.1 SAQ-D (self assessment questionnaire - type D) for merchants. As the merchants or retailers achieve the SAD-Q, they can file the AOC to attain the re-assessment. If the traditional and advanced data security controls are deployed and data security for cloud abstractions are adhered to, compliance to PCI DSS 3.2.1 can be done very easily.
- GDPR Compliance: Although there are 99 articles in GDPR, but the retail or e-commerce companies need to focus more on articles 5, 6, 7, 8, 9, 11, and 32. It is important to have all - the traditional, advanced and cloud abstractions' data security controls to attain GDPR compliance. Besides, companies also have to deploy solutions for the following controls:
  - Static Data Masking
  - Dynamic Data Masking
  - Encryption of Data in Motion & at Rest
  - Column Level Encryption for the DBAs
  - Data Breach Detection
  - Deception Technologies.

55% of Retailers haven't made CAPEX in Cybersecurity in 2019. Retailers and E-commerce companies should take cybersecurity as a Business Enabler

About the Author

Ravinder Pal Singh
Senior Project Manager

Ravinder has 22 Years of Experience with last 16 years at Infosys. As SPM/Project Manager, he has successfully managed deliveries across various countries, dealing with various clients and vendors in USA, UK/Europe and Asia Pacific under strict timelines, cost and quality control. In addition to these, Ravinder has been associated with the business process improvement initiative by analyzing "AS IS" process and designing "TO BE" business process workflow to meet the short term/long term goals of stakeholders.

For more information, contact askus@infosys.com

Infosys®
Navigate your next