Next Generation Digital Retail & Cyberdefense

The retail sector is currently witnessing an intense technological disruption. The proliferation of online shopping, social media and ever-changing expectations of consumers are the key forces driving the change. The future of retail players would highly depend on how effectively they use technology to interact with their customers.

The stores of the future are very likely to have no queues for checkout and will enable hassle free payments. Payments would be simplified using connected devices, such as wearables.

Key features that next generation digital retail will exhibit are following:

- A future of hands-free shopping enabled via connected devices
- New levels of shopping convenience enabled by digital reality - virtual and augmented reality
- Enriched customer experience enabled by hyper connectivity and hyper personalisation
- Shopping at robot enabled shopping arcades
- Highly technology-enabled experience

The variety of wearable gadgets available in the market is rapidly growing and envisioned to reach roughly 600 million through 2020. This means that an increasing number of people will be carrying smartwatches, activity trackers and other wearables that will help track data of their personal identity details, banking and payment transactions, as well as their buying behaviour. We are also seeing a boom in tap-and-go mobile payments, with biometric technologies, such as facial recognition, eliminating the need for credit scorecards, pin codes and signatures. Thus permitting a consumer to walk into a shop, take what she or he desires and then without a doubt walk out. Imagine a future of hands-free purchasing wherein the complete purchasing experience – from browsing to buying, are completed digitally.

The reality of digital retail:

Virtual reality (VR) and augmented reality (AR) enable retail stores to personalise the delight of the purchasers. The sector is gaining momentum with VR and AR funding in retail estimated to attain around $30 billion.

Virtual reality immerses the person in a simulated environment, while augmented reality overlays digital records onto the real world experienced through a tab or smartphone. Both VR and AR offer offline and online retailers the opportunity to revolutionise the way their customers shop. Whether a customer wants to try on an outfit or see if a piece of furniture fits in their living room, virtual reality and augmented reality are making it all possible. With online VR applications, customers can engage with retail stores anytime, anywhere. For instance, an e-commerce apparel retailer could create 3D surroundings that offers customers the experience of being in a brick-and-mortar shop and allow them to try apparels at the convenience of their homes.

Cyber and Privacy Risks of AR /VR

Ransomwares – recording of consumer behaviour in a personal immersive environment and later misusing the information for extracting ransom.

Device control compromised – hackers gaining control of the consumer's device / store devices with destructive intent.

Privacy breach – compromised AR/VR devices can lead to data breach of the consumer's personal information.

Device damage – compromised AR/VR devices can enable hacker to damage the firmware and in turn the device too.

The hyperconnected retail:

In a hyperconnected world, 'Everything' might be communicating with 'everything'. In the retail sector this means that indoor and outdoor digital signage, show cabinets, sensors, smart product tags, wearables, smartphones and other devices will monitor, track, analyse, report, endorse and advise. Retailers' stocks get tracked and replenished mechanically and clients will receive automated updates on new arrivals and special personalised offers while they are in near proximity of a store they have formerly shopped at or had proven interest. Advertising and content streamed to connected digital or digital presentations can expect and address the demands of customers based on time of day, month, season, region and weather. By using a drone, groceries can probably be delivered to your house routinely. Hyperconnectivity allows products, gadgets and appliances to form multidimensional layers, streamlining operations in stores, offices and homes in addition to enriching client experiences.

Cyber risks of IoT devices

Device discovery - You can't protect what you can't see.

Authentication and authorization – unauthorized connected devices for attack surfaces.

Device updates – illegitimate OTA updates.

Disruption, DDoS attacks and IoT botnets – sophisticated automated attacks.

Lot passwords – weak passwords including no password.

Weak Encryption – weak encryption algorithms leading to decrypting of the information and compromising the communication channel.

A Hi-Tech shopping arcade:

The automated shopping experience is made possible by a system of sensors, computer vision and deep learning, what we call artificial intelligence and deep machine learning. This enables the sophisticated virtual shopping cart system to keep track of what is taken off and/or placed (back) on the shelves. When the consumer is done with shopping, he or she can just walk out of the store, after which the amount is debited from his or her shopping account.

Consumers are now seeking to fulfil their specific needs with services and products. For retail to thrive and remain vibrant, embracing new technological innovations will be crucial.

Cyber risks associated to technology

Vulnerable libraries used within the software package, exposing attack surfaces.

API integrations over unsecured protocols leading to information disclosure while parsing.

Open source stack used as-is without undergoing security sanitization.

Inadequate skilled workforce to support the technology stack.

Functional and Operational behaviour anomaly – the technology stack does not function or operate as intended

Cyberdefense measure for the next generation digital retail:

With the massive scale of digital transformation within the retail sector, shopping experiences with wearables (IoT), smart devices for AR and VR and hyper data personalisation will definitely enrich the end consumer experience. However, as the data grows to drive analytics-based business, so will the exposure to the various cyber threats, such as data breach, data exfiltration, online frauds - both identity and financial, IoT based attacks, multi path attacks over 5G network etc.

The control objectives one should focus on to secure the next generation retail, are as mentioned below, though not limited to:

Identification of your critical crown jewels and securing them from the core to the perimeter.

Continuous assessing of the critical crown jewels (both IT infrastructure and applications) for cybersecurity threats and anomalies.

Envisaging strong DevSecOps principles across the business IT landscape.

Envisaging strong data exfiltration prevention techniques, such as strong passwords, multifactor authentications, strong data encryption, robust digital identity management, such as Blockchain-based identity management and more.

Envisaging strong authentication techniques for the IoT devices connected over the 5G network avoiding the risk of unauthorised accessing of these devices to execute a multi path attack.

Envisaging AI enabled near real-time Personal Identifiable Information(PII) data identification and updating the inventory for protection measures.

Envisaging Security by Design while architecting the business solutions.

Conducting frequent Privacy Impact Assessments (PIAs) to assess privacy risk across the AR and VR technologies and upcoming new technologies enabling the business.

Conclusion

As we foresee the coming years to bring in more enriching experience to the consumers, elevating their spending on shopping, all on the foundation of hyper data personalisation, technology enablement into the digital space. This will increase the drivers for hackers to attack and mine into the technology anomalies stealing a huge amount of personal data, financial data and executing more sophisticated attacks. Cybersecurity will become an essential and hygiene element of any business, including the next generation retail, and will not be limited within the organisation board. It is time for each one of us to be vigilant and educated on protecting our personal data and identity of the future.

About the author

Hiten Panchal, Practice Director - Cyber Risk Services, Consumer Business

Hiten has around two decades of experience into the information security and cyber risk. He spearheads the Change & Transformation of the Cyber Risk Advisory and Services for the Consumer's Business Unit @ Wipro. He is a thought leader backed with certifications in Blockchain, Data Privacy - GDPR, PCI-DSS and Information Security Management.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/BRD/MAR 2020-FEB 2021