Last Mile Delivery Optimisation

The Three Success Factors for online retailers to focus on during and post COVID -19

April 2020

"While the entire world is in a lockdown, one of the key responses to the situation we've seen is a huge overnight change in the shopping behaviour. Consumers are changing what they're buying, how and when, from bulk-buying to online shopping."

-Susan Meyer-

Enterprise Content Marketing Manager

Understanding the Situation

Immediate response of the consumers to the COVID-19 pandemic is panic buying and stocking up essential items. This has created a logistical nightmare to the online retailers where on one hand, they're struggling to meet the demand for several categories resulting in huge non-moving stock of non-essential items and on the other hand pushing the supply chain to its breaking point.

The demand for online retailing is expected to continue well beyond COVID-19 and is even expected to grow as opposed to the traditional retail model and have lasting impacts on the overall retail supply chain of Sri Lanka.

Having a robust online platform is a vital element to catering to the exponential increase in online shopping. The key area that threatens the success of online shopping is the Cyber Security of these online platforms. The colossal amount of confidential data captured by the e-commerce platforms, increases the cyber security risk and vulnerabilities, which could result in disrupting the supply chain.

In order to streamline the last mile delivery operation, KPMG proposes the online retailers to focus on three critical success factors.

1. Dynamic Route Optimisation

2. Automated Replenishment

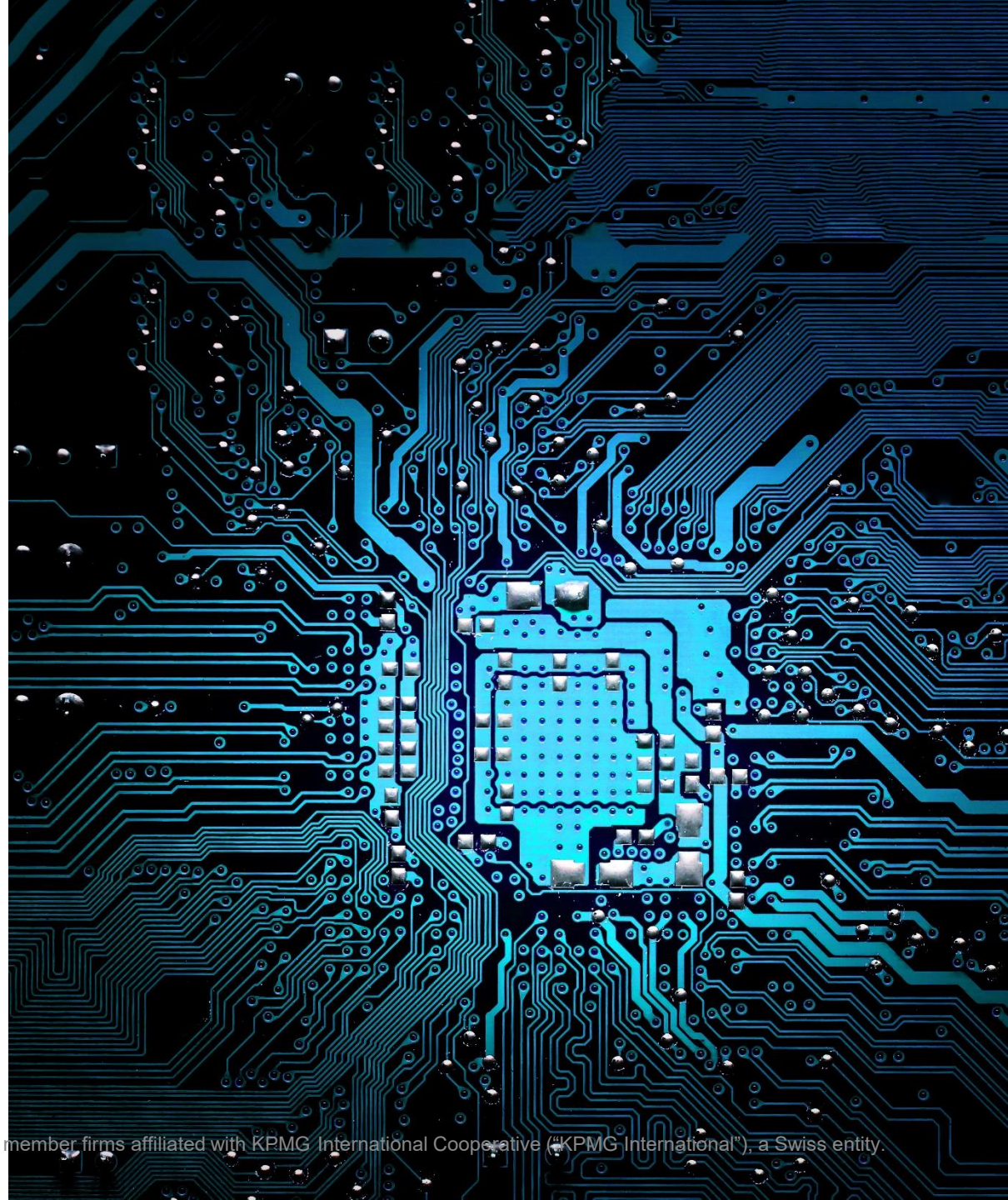
3. Cyber Security

Dynamic Route Optimisation

During the COVID 19 period what we've seen is most of the retailers are struggling to schedule their deliveries on time and in full. The main reason is even though online retailers have invested in the ecommerce platforms with rich user interfaces to target consumers and capture the orders, minimum investments have made in automating the back-end and integrating route planning capabilities.

Automated route planning tools enables optimization of the delivery scheduling by optimizing the service level and the cost rather than depending on human which takes a lot of time, effort and results in costly errors to the brand. An effective route optimization program needs to be equipped with several functionalities, which include:

1. **Automatic Optimisation**
2. **Real-time Map Data**
3. **Tracking and Tracing**



Automated Replenishment

One of the most critical success factors for an online retailer is the replenishment planning. Specially in a situation like COVID-19 and immediate post COVID-19, the risk of failures in replenishment results in a complete breakdown of the supply chain. It's true that this could be a result of suppliers being unable to deliver which is an external force, beyond the control of the business. However, a significant part of the problem stems from poor replenishment planning.

Automated replenishment planning is an effective solution for online retailers to avoid this issue. Even though the automated replenishment is a common feature which can be found in many ERP systems, most of the online retailers have not configured or utilized it properly. An effective automated replenishment platform should provide:

1. **Predictive modeling of the demand**
2. **Automated calculation of the replenishment parameters**
3. **Inventory profiling**

Cyber Security

In times of crisis a cyber-attack can paralyse the functioning of organizations. Since mid-February, KPMG has seen the rapid build-out of infrastructure by cybercriminals used to launch COVID-19 themed spear-phishing attacks and to lure targets to fake websites seeking to collect enterprise credentials.

Our Cyber Defense and Cyber Response programs are designed specifically to think like the bad guys and help clients identify their threats, design security operations programs, deploy monitoring technologies, detect insider attacks, simulate fraud and cyber scenarios to evaluate defenses, design threat resistant applications, and measure the cost effectiveness of cyber monitoring investments.

Key Cyber Defense and Response Components

1. Web/Mobile/Network Vulnerability Assessment
2. Cyber Maturity Assessment
3. User Awareness Training / Computer Based Training (CBT)
4. Cyber Threat Management and Readiness Assessment
5. Business Continuity and Disaster Recovery Planning

Contact us:

Priyanka Jayatilake
Partner - Head of Advisory
T : +94 (11) 5426 401
M: +94 77 731 3390
priyankajayatilake@kpmg.com

Kamaya Perera
Partner –Management Consulting
T : +94 (11) 5426 270
M: +94 77 003 1701
kperera@kpmg.com

Thisara Watawana
Senior Manager –Management Consulting
T : +94 (11) 5426 288
M: +94 77 736 2543
tchathuranga@kpmg.com

Hasitha Karunaratne
Senior Manager – Cyber Security
T : +94 (11) 5426 354
M: +94 76 717 5645
hasithakarunaratne@kpmg.com

Follow us on,

KPMG Sri Lanka

@kpmgsl

www.home.kpmg/lk