An Expert Take on 4 Big ECommerce Business Risks - YourRetailCoach Dubai

The Middle East, including the UAE, Qatar, and Saudi Arabia, offers lucrative eCommerce markets, but comes with various business risks, both old and new.

An Expert Take on 4 Big ECommerce Business Risks

PUNE, MAHARASHTRA, INDIA, April 16, 2024 /EINPresswire.com/ -- While many countries in the Middle East like the UAE, Qatar, and Saudi Arabia are attractive markets for eCommerce, there are also many old and emerging business risks. Leaving them unattended could mean nothing good. In this communiqué, retail and eCommerce consultants - YRC offers expert insights on four such eCommerce business risks and ways to tackle them effectively.

Get advise for E-commerce retail business: http://www.yourretailcoach.ae/contact-us/

> Empowering Retail & E-commerce businesses worldwide."
>
> *Nikhil Agarwal*

□□□□□ □□□□□□□□ □□□□□

Sound cybersecurity is indispensable in the eCommerce business. A wide range of personal and organisational data are collected, stored, processed, and exchanged by retail and eCommerce companies to run their businesses. Cracks in technology and cyber security measures often create vulnerabilities that can be misused by hackers or similar entities for nefarious purposes. Two common cyber security risks emerging from poor cyber security management are highlighted below.

Data Breach: Personal data and information shared by customers with eCommerce platforms are illegally accessed by hackers for forging identities, committing financial irregularities, etc. Incidents of data breaches cause serious damage to brand reputation and customer loyalty.

Ransomware: In ransomware, hackers lock users out of their devices in return for ransom money. People in senior executive positions in eCommerce companies are prone to becoming targets of ransomware attacks.

□□□□□□□□□

ECommerce companies should have a dedicated IT team with able leadership with cyber security as a key area of responsibility.

Having cybersecurity policies and practices helps ensure that the necessary protocols and standards for maintaining cyber safety are known and religiously followed by all in an organisation.

Training helps impart the necessary knowledge and skills on various aspects of cyber security. Conducting drills helps employees get acquainted with actions to be taken in the event of cyber attacks.

Cybersecurity SOPs (e.g. GDPR checklist for eCommerce websites) help maintain strict adherence to the established standards and practices for cyber safety.

□□□□□□□□□□ □□□ □□□□□□ □□□□□ □□□□□

Complaints of receiving damaged products are infamous in eCommerce. Poor handling and transportation combined with poor packaging standards is the biggest reason for products getting damaged. Poor tracking leads to packages getting lost in transit. Inefficiencies on the part of 3PL entities make it difficult for eCommerce brands to prevent delayed deliveries.

Ecommerce companies also face risks of changes in fuel prices, tax regulations, and regulatory norms. These changes force businesses to make modifications in their SCM and logistical strategies.

Union strikes and shortages in the supply of labour can also slow down activities in the supply chain and logistical operations leading to delayed procurement, deliveries and scores of cancelled orders.

□□□□□□□□□

The best approach to cover any potential internal operational risk is to develop robust processes and eCommerce SOPs.

ECommerce businesses should adopt scalable logistical and warehousing strategies and solutions to meet with many changing variables in the external environment and lend agility to their operations.

Working with reliable 3PL partners is highly recommended to maintain consistency in operations and quality of performance.

Being a part of industry associations can prove to help accommodate big changes or negotiate their implementation.

Maintaining good relationships with unions and associations helps companies buy some time and space to fulfil their demands and requirements.

□□□□□□□□□□-□□□□□□□□ □□□□□

Unpredictable demand trends often make it difficult for eCommerce to achieve accuracy in demand forecasting. This makes overstocking and understocking a common feature in eCommerce. While overstocking leads to excess investment into inventory, understocking does not go well with customer experience.

The inability and inconsistencies on the part of suppliers to make stock available on time is another risk.

Faulty or defective products can enter the value chain due to lapses in quality control. Such orders are returned or replaced leading to escalation of costs.

Keeping track of inventory movement and reconciling physical and digital records is a tough job in eCommerce even with the use of technology that makes it hard to contain shrinkages.

□□□□□□□□□

To deal with overstocking and understocking, it is advisable to make use of advanced analytics for eCommerce market research and eCommerce demand forecasting.

Product listing should go live only after goods are available in the designated warehouses or fulfilment centres and are ready to be processed for order fulfilment.

In managing inventory risk in online retail, suppliers have a big role to play. The broad criteria for suppliers should be established as a part of eCommerce business model development. Experienced eCommerce consultants maintain that KPIs and KRAs should also be determined and communicated before onboarding any supplier.

Having adequate QA and QC measures reduces the odds of faulty or sub-standard goods entering the value chain.

Standard approaches like record-keeping, timely reporting, and automation are useful in

controlling inventory shrinkages combined with add-on tactics like measuring inventory in smaller lots or batches at every juncture.

□□□□□□□□□□□□□□ □□□□□

Downtimes are common for eCommerce apps and websites. Network and server-related issues like excess traffic, coding flaws, hardware failures, software crashes, poor internet services, and cyber attacks are often the most common reasons for downtime. Downtimes not only cause operational slowdowns but they also carry financial implications. The inability to place orders or disruptions in payment processing is a prime example.

Other technology-related risks include poor UX design, inadequate cyber security, misfit IT solutions, loopholes in SOP-IT integration, lack of necessary automation, etc.

□□□□□□□□□

The first step towards mitigating technology risks is having a sound and relevant IT infrastructure followed by associations with reliable and strategic service providers.

Regular backup of data (as per law) is highly recommended.

Frequent monitoring helps take timely actions.

Having a response or recovery plan helps restore normalcy in a planned and systematic manner.

User research and testing are critical to containing UX risks.

For cybersecurity solutions, it is best to hire or rely on professionals.

Get advise for E-commerce retail business: http://www.yourretailcoach.ae/contact-us/

Dr Rupal K Shah
Mind-A-Mend Consultancy Private Limited
+91 98604 26700
consult@mindamend.net
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube