The world is in an unprecedented situation with the outbreak of the 2019 novel coronavirus (officially renamed, "**COVID-19**"). Numerous countries have instituted stringent policy measures to prevent the spread of the outbreak. While, for now, such policy measures comprise of widespread travel restrictions, workplace closures, city-wide lockdowns and mandatory quarantines, with the *World Health Organization* having declared COVID-19 as a pandemic, there are growing concerns of restrictions on trade with infected regions being imposed soon.

As crucial as such policy measures are in curtailing the rampant spread of this outbreak, business operations of companies, both, inside and outside of China, Italy, and South Korea are facing considerable commercial disruption as a consequence of these measures.

In this edition of our series, we examine the technology and cyber security issues to consider.

Business Continuity Plans

Business continuity refers to the maintaining of business functions or the ability to quickly resume them in the event of a major disruption. Considering the currently mounting number of COVID-19 cases reported, it is essential that businesses look at this event as a potential business disruption and aim towards updating their business continuity protocol.

A Business Continuity Plan (BCP) must focus on the employees continuing their functions without endangering them, while keeping in mind the core product or services of the business and the core business practices and the essential ingredient required to deliver/perform the same.

A few crucial aspects of ensuring business continuity are:

- Devising a time-sensitive plan for re-instating business practices in the case of any large-scale disruption.
- Carry out a high-level and low-level impact assessment of the disruption on your business and business practices before devising a business continuity plan.
- Accounting for the financial aspects for planning business continuity protocols.
- Maintaining sufficient server capacity.
- Considerations of any Government orders or notifications which may have been issued and which directly and materially affect the business of the company or the BCP of the organisation.
- Consider providing work-from-home options facilitated through secure online workplace models etc.

The essential element of BCP will need to capture the impact of COVID-19 on the business continuity on a micro and macro level, and devise a risk mitigation and management strategy in respect to it.

Safeguarding Against Increased Cybersecurity Threat

With an upsurge in working from home or remote locations, there can be an increase in the use of non-secure networks and channels. This presents opportunities for cybersecurity attacks and other systemic attacks such as phishing (a method of trying to gather sensitive information such as employee IDs, passwords which help in gaining access to confidential and protected information of the organisation through use of using deceptive e-mails and websites).

As an organization, it will be critical to account for this likelihood and re-assess the organization's cybersecurity plan and reinforce it with employees. The organization can aim to sensitise their employees regarding such attacks and undertake protective measures such as thorough screening of emails, firewall maintenance, etc.

Remote Working and Capacity Stress Testing

The organisation must ensure that the remote working interfaces employed by them are not only user friendly but reliable and secure. The objective should be to reduce the learning curve for employees while using the new interface and create a secure platform for business operations.

Additionally, in order to facilitate the various employees working remotely, a dedicated and experienced IT team must carry out load testing and any changes in the system as suggested by them must be carried out. The organization

may also consider increasing its bench strength of qualified IT personnel as a BCP strategy.

Real Time Vulnerability Updates

The organisations must consider employing full time dedicated IT teams for monitoring and maintaining the virtual framework of the organisations and undertaking on-spot maintenance practices to ensure confidentiality of the sensitive data held by the organisation.

It is crucial that the organisation seriously considers increasing their security levels so as to avoid any data breaches in the current atmosphere of increased virtual attacks.

Assessing Impact – Key Strategies

- Review your BCP and determine whether a stress test for your technical infrastructure is required.
- Revisit your cybersecurity plan to ensure the additional risks created from work from home is accounted for.
- Reinforce and train employees on any changes to the BCP and/or cybersecurity plan and any new deployment of software.
- Re-assess capacity of the infrastructure being used to support work from home – whether it is technology, servers, or human resources.