Best Practices for COVID-19 Preparedness

Introduction

COVID-19 may increase existing risks to your staffing, office access/availability and IT. Below are ideas and best practices for preparedness and how to adapt to maintain business continuity.

Mitigating risk to staffing

Avoid business processes that put an entire team covering a key function at risk. For example, if a few team members become ill or are unable to work for any reason, there should be ample time before there is risk to the rest of the covering team.

- Implement policies that allow for ample flexibility and coverage among team members. Develop a contingency plan in case employees in a region suddenly become unavailable.
- Build contingencies that may include extending work hours in other regions and/or splitting shifts among distributed teams.
- Communicate with employees and give them training before the other region is unavailable if possible.
- Consider the impact on working time: illness or other unplanned events (e.g. being a caregiver) may remove some amount of productive work for every employee. Expect other preparations outlined in this guide to generally consume additional time.
- Defer technical goals not aligned with business continuity by a month or quarter, whatever is appropriate. Prioritize carefully.

Managing office closures

Your needs are likely to change due to Working from Home (WFH).

- Prepare for working hours to change when not subject to commute delays.
- Anticipate that peak service load may move and become more sudden and taller. Have a company-wide WFH day test, asking everyone to practice video conferencing, and other core collaboration tools, as some people may not have used them in the last few months.
- Fix equipment, update software and address any issues in the office after the test to prepare for a WFH requirement when fixes could become much harder.
- During a mandatory evacuation of all commercial buildings in a city or county, computer repairs cannot happen. This could cause a loss of capacity as computers cannot work from home.
- Ensure your Disaster Recovery (DR) sites are working.
- Review your physical data center DR plans; sites should not be too close together.
- Assure that your cloud virtual data center has its DR in a different region.
- After everyone has demonstrated WFH collaboration, ask every team to test their hardest procedures (that typically take place in the office) and capture urgent bugs for problems. Fix those bugs and mitigate VPN or Zero Trust issues before mandatory WFH. If factories and manufacturing plants close or slow production, inventory for a variety of products could be impacted.

Reviewing IT tools, resources & capacity

Revisit all capacity planning to make sure there is headroom for growth.

- Anticipate that some usage patterns might change dramatically for your users. Remote management only gets you so far.
- Implement and test graceful degradation or another popularity mitigating measure.
- Understand the impact of delays in your supply chain - whether it be slower delivery of products to your shelves, or inability to provide new hires with laptops.
- Review policies for virtualization and cloud pre-purchase and reservations.