Developing a Business Continuity Plan (BCP)

June 2019

Unexpected events such as terrorism can have a devastating impact on businesses. There will be damages to infrastructure and stocks, failure of IT systems, and loss of suppliers. Businesses are likely to collapse, and the aftermath makes it difficult for companies to resume normalcy.

However, when you take the effort to put in place a Business Continuity Plan (BCP), you will start to identify potential risks and create back-up plans. This enhances your company's resilience to disruptions and minimises the impact of such distractions. Your BCP should include the following steps:

Conduct Business Impact Analysis (BIA)

BIA helps to assign priority to critical business functions on both internal and external levels:

- Identify and prioritise factors that contribute the most to revenue, and/or factors that are essential to the continuity of the company's most profitable activities e.g. raw materials, a fully functioning website, etc.
- Assess the impact a disruption will have on business performance. Factors such as lost or delayed sales and income, increased expenses from overtime labour, outsourcing, regulatory fines and customer dissatisfaction should be considered.
- Evaluate how long the business can be sustained without certain services.

Create back-up plans for the following:

1. Employees

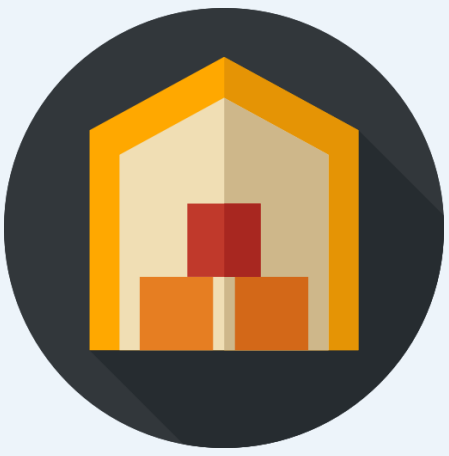
- Clarify the role of all employees as well as overlapping roles.
- Ensure that you have an updated list of employees' details and their next-of-kin.
- Standby a list of temporary and part-time staff to activate at short notice, in case your full time employees are affected by a terror attack.
- Create a call-tree so that it is easier to notify and coordinate staff in the event of a terror attack. Refer to the call-tree template on the MOM SGSecure@Workplaces website under 'Partner your Community'.

2. Internal and External Stakeholders

- Prepare a list of alternate vendors who can support your business operations if your current partners are affected by crises. This prevents a complete supply chain disruption.
- Reach out to stakeholders such as clients, suppliers and customers regularly to foster a strong community partnership, and thereby strengthening the value chain.
- Prepare a call-tree to notify stakeholders.

3. Inventory and Facility

- Identify temporary relocation options.
- Plan an alternative working arrangement in case a terror attack affects your current premises e.g. working remotely.
- Ensure that you have other essential equipment and supplies as back-up such as production equipment.



4. IT Systems

- Ensure that you archive and back-up important data for faster reinstatement of systems.
- Important data could include customers' information, emails, files and spreadsheets.
- Read more on cyber security here!

SGSecure@Workplaces Bulletin