



---

***Remote  
Operations  
Business Plan***©

By David Dickson  
Managing Director  
Strategic Planning Consultants  
June 2, 2020  
305-773-8856

# TABLE OF CONTENTS

---

- 1. Executive Summary ..... 3
- 2. Technology ..... 4
- 3. Action Plan and Next Steps ..... 10

# 1. EXECUTIVE SUMMARY

---

The purpose of this paper is to outline a framework for setting up technology-enabled remote operations in time of crisis. It focuses on providing a high-level overview of the needs and processes involved in creating the final product: technology enablement of strategic and tactical plans for any disruption in the business operations.

The paper follows a common structure:

- **Opportunity:** Rapid deployment of disrupted or remote business operations
- **Mission:** Creation of a robust, tested remote operations plan
- **Solution:** Involve the business in a planning, design, implementation, testing and deployment process
- **Expected returns:** Creation of plans and environment(s) that have been designed, tested and ready to deploy for remote business operation

Recent research indicates that setting up remote operations is not new for many organizations; however, the recent events of COVID-19 have only emphasized the need for companies to develop and execute strategic plans to enable remote operations.

Some Key Metrics to consider about remote workers (OWL Labs Survey 2019):

1. Remote workers earn salaries higher than \$100,000/year, 2.2x more frequently than on-site workers.
2. 34% of U.S. workers would take a pay cut of up to 5% in order to work remotely.
3. Remote workers say they're happy in their jobs 29% more than on-site workers.
4. 68% of remote workers say they are not concerned working remotely will impact their career progression, while 23% say they fear it would.
5. 32% of employees report never or being unable to work from home.
6. Full-time remote workers are twice as likely to be individual contributors vs. people managers.
7. Those who work remotely at least once per month are 24% more likely to be happy and productive in their roles than those who can't or don't work remotely.
8. Companies that allow remote work experience 25% less employee turnover than companies that do not allow remote work.

## 2. TECHNOLOGY

---

Technology is the key to providing an emergency operation.” Business is the Driver; Technology is an enabler.” Business requirements dictate what is needed during the emergency to operate the business. Technology supports the business strategies and processes by enabling automation, technology platforms and other solution sets specifically relegated to a technology operation.



The following identifies likely critical areas that require solid technology enablement to support remote operations during a disaster or emergency:

# Remote Operations

## Business Plan

1. Contact Center:
  - a. Contact centers have several options:
    - i. Onsite operations –Critical in nature and may have high value assets or high security functionality that may be deemed high risk if remote.
    - ii. BPO (Business Process Outsourcing) - Partners that provide this capability to reduce costs, spread resources globally and provide a wider coverage of services.
    - iii. Remote- These resources can be either outsourced or in-house, but are not co-located with the organization.
2. Supply Chain:
  - a. Materials/Vendor/Suppliers – Most companies that have any substantial supply chain have to think about raw materials, component parts and manufactured goods to sell or use in their own manufacturing process.
  - b. Sourcing – There needs to be a robust and thorough process by which applications are selected to provide the supply chain process its needed inputs, capabilities, methodologies, etc.
  - c. Distribution channels – Organizations may need to develop alternate distribution channels for emergency or standby operations.
  - d. Tools/Capabilities – Technology tools are amongst the most valuable assets in a supply chain operation. The other aspect of tools, are the resources that manage and use these tools. Resources need to be able (and understand how) to operate under adverse or emergency conditions.
3. ERP/Financial:
  - a. Methodologies/Modeling – Financial modeling usually changes with market conditions, cash flow or other financial aspects of the company.
  - b. Financial Analysis/Cash Flow – Financial modeling along with the methodologies is important to determine cash flow and analysis and could be dependent on the technology and modeling/programming of the data for analysis.
  - c. Tools/Capabilities –The data ranks as one of the 3 most viable assets of the organization (Data, Products/Services, Resources).
4. HR:
  - a. Sourcing – Employees, Contractors, Vendors, Partners, etc.

## Remote Operations

### Business Plan

- b. L & M – Learning, Management, Training
- 5. Marketing/Sales – Plans also need to be developed so there is a migration from “Keep the lights on” to ramping up operations to resumption of a normal operations.
- 6. Security: For any operation, especially during a disrupted business operation, security is of prime importance. This includes the physical security of unused buildings and infrastructure as well as Cybersecurity.
  - a. Physical Security –There is a possibility that the physical property(ies) will need some added or modified level of security.
  - b. Cybersecurity – This aspect of enterprise security is always present on/offsite, day or night 24/7/365. Especially during emergencies or disrupted operations. Cybersecurity rules and procedures need scrutinization more so than under normal operations.
- 7. Data Warehousing:
  - a. In-house –This option is for an enterprise that has the resources (physical, financial and technological) to create and maintain its own warehouse either on site or offsite; single/multi and/or global sites.
  - b. Outsourced –This option is for enterprises that are too small to maintain their own sites, looking for an option of redundancy or looking to expand operations (possibly globally or over territory/regions).
  - c. Managed/Hosted – This option has several components:
    - i. Managed – Enterprise owned, on site but managed by an outside vendor/partner/3<sup>rd</sup> party.
    - ii. Hosted – Hosted by a vendor, 3<sup>rd</sup> party or partner in hosting site, but managed/maintained by enterprise (commonly call co-location)
    - iii. Managed/Hosted: A combination of the above 2 whereby the partner/vendor/3<sup>rd</sup> party both hosts and manages the data- warehouse operations
    - iv. Infrastructure/Software/Maintenance – In addition to Managed/Hosted options, enterprises can also select whether they want their physical infrastructure, software (applications, licenses, software) and maintenance capabilities installed, operated and maintained by the vendors/partners/3<sup>rd</sup> parties either offsite or onsite.

## Remote Operations

### Business Plan

8. VPN/Remote Access:
  - a. VPN – VPN (Virtual Private Networking) is probably the most secure way to allow access from remote or offsite employees/resources. This level of security involves setting up access for each and every user and allows access to specific applications, websites, databases, technology platforms, etc.
  - b. Remote Access – This option is less secure, but allows for quicker and wider access by allowing access and login via the internet (i.e. anywhere globally with internet access). Security is provided by login and passcode access to websites, applications and partners.
  - c. Code security – This type of security is compatible with both remote and VP access and provides for 1 more layer of secure remote connectivity. A key FOB or software application that has a continually changing access number/alpha that changes on a 30 sec to 1-minute routine. (RSA is market leader)
9. Analytics/Reporting:
  - a. Analytics – Metrics need to be established (probably from normal operations) for both normal and current conditions.
  - b. Reporting – Reporting needs to be modified to meet needed conditions.
10. WEB/eCommerce:
  - a. Web – Web access is usually for employees/authorized resources access to the infrastructure and applications of the enterprise via a login or username and password/passcode protection.

eCommerce – This capability is generally for the public at large to conduct business (shopping, banking, bill payment, order status, etc.)
11. Mobile/OmniChannel:

This technology offers the opportunity for the enterprise to combine all of the above technologies into a Customer centric application. Combining Web, Mobile, Voice, Video, Chat, Fax, Social Media and other applications within the enterprise framework, the customer experience is greatly enhanced.
12. Cloud & Communications (VoIP, email, Chat, Social, fax, etc.):

The cloud is particularly useful in emergency operations. Most large enterprises have some if not all application in a cloud environment (either

## Remote Operations

### *Business Plan*

Hosted/Managed/Maintained; Owned/Outsource; Onsite/Offsite), as well as redundant sites (either co-located or owned).

TCO (Total Cost of Ownership) can be very competitive if multiple sites, applications and infrastructure types are required

The cloud can offer capabilities that the enterprise may find too costly, time consuming or cumbersome to operate. Most cloud/hosting sites have licensing/software applications that can integrate a multitude of different applications, OEM software, Middleware integration, infrastructures and medium (telecom lines: fiber, microwave, satellite).

### PROPOSAL OUTLINE FOR EMERGENCY/REMOTE OPERATIONS

---

1. Video and telephony conferencing vendors:

- |                  |                    |
|------------------|--------------------|
| 1. Zoom          | 6. 8x8             |
| 2. Cisco Connect | 7. Nice-In Contact |
| 3. Ring Central  | 8. WebEx           |
| 4. Five 9        | 9. GoToMeeting     |
| 5. Owl Labs      |                    |

2. Short, mid, long-term technology solutions identified

3. Data Warehouse, RSA (Remote Security), VPN, Connectivity, AI (Artificial Intelligence), RPA (Remote Process Automation)

4 Understand players-in remote space operations:

- a) Contact centers-traditional capabilities
- b.) Enterprise
- c.) Other stakeholders, partners, suppliers
- d.) Enterprise customers / clients

5. The short mid and long-term solutions from the vendors

6. Technologies:

- a.) Contact centers
- b.) Enterprise capabilities
- c.) Web, chat, email, telephony, video
- d.) DW (Data Warehouse), VPN (Virtual Private Network), Security, Data Mining, MDM (Master data Management)
- e.) AI (Artificial Intelligence), RPA (Robotic Process Automation)
- f.) Social Media
- g.) Remote capabilities

7. Operational Aspects:

- |   |   |                               |
|---|---|-------------------------------|
| a.) Remote Ops overview -   | } | 1.) strategy/goals/objectives |
| c.) Emergency Deployment  |   | 2.) Roadmap                   |
| c.) Business continuity at contact centers only - technologies  |   | 3.) Plans:                    |
| d.) Routing + flow of existing calls contacts via web/mobile<br>- standby capabilities in non-emergency situations (i.e. - phone@40% cost per month from 8x8) |   |                               |
| e.) Asset + identity management from mobile/personal assets.  |   |                               |
| f.) Data Management   |   |                               |

8. Training and Learning:

- a) Establish/create training documentation
- b) Conduct training sessions

9. Remote Support options (Centralized, decentralized, outsourced, independent per user)

### 3. ACTION PLAN AND NEXT STEPS

---

We have come to the point where the organization needs to take action. Most enterprise organizations have some remote operations capabilities. However, since most organizations typically do not need, or have built capabilities around these plans, they are seldom used, and even less reviewed on a regular basis.

Remote operations (specifically workers not onsite) utilize technology to a great extent. Rarely does a remote worker **not** utilize a computer, internet, videoconferencing, telephone technologies. It is for this reason this paper was created.

Specific steps to achieve desired goals stated in this paper include (but are not limited to):

1. Assessing needs of plans
2. Determining timeframes for each plan/process
3. Determine resources required to create each plan
4. Determine costs factors for each plan
5. Prioritize the required plans
6. Decide on/if planning process needs to start
7. If the decision is to start the planning process, then start discussions with resources (internal, external, consultants, etc.)

EXPECT RETURNS:

- **Opportunity:** Business operations continuation/resumption
- **Mission:** Business continues via remote operations
- **Solution:** Strategy and processes identified, remote capabilities deployed and operating