Business Continuity Plan

Effective starting: April 20, 2024

Busch Technology Solutions, LLC (referred to as "BTS") is the owner and operator of BuschTechSolutions.com (referred to as "BuschTechSolutions") and BTSValidation.com (referred to as "BTSValidation"), including any related websites, sub-domains of BTSValidation, and pages. BTS takes business continuity very seriously. In order to ensure that we are prepared for any unforeseen circumstances that may occur to our physical location or virtual server, we have developed a comprehensive business continuity plan. This plan covers various topics and includes processes that can be implemented in advance to mitigate any negative impact that may arise from an adverse event.

It is important to note that the business continuity plan can be updated from time to time as lessons learned from any after action review (AAR). Any newly identified risk will need to be updated and the business continuity plan.

Topics:

- Organizational structure
- Scope of the plan
- Disaster response process
- Disaster recovery process
- Recovery process
- Preparation and training
- Notification list
- Time frames for action
- Additional information

Organizational structure

BTS is a small woman owned privately held company. In the event of a large scale outage of BTS validation, an emergency, or tragedy, Busch Technology Solutions, LLC. needs a way to continue operations. Because BTS it's such a small organization it's going to require all employees and contractors to help.

Scope of the plan

the following is a list of unwanted but potentially foreseeable adverse events that need a continuity response process:

1. An emergency situation requires the abandonment of the physical location of BTS.
    - In this situation, this could be a fire in the physical facility or a natural disaster such as an earthquake that would physically destroy or make uninhabitable the location where BTS operates. This situation could last hours, days, weeks, or a permanent state.
2. A complete collapse of the Microsoft Azure infrastructure
    - At the end of the day, this would be a huge event for not only BTS but a large piece of the World economy.
3. BTSValidation or BuschTechSolutions website being taken over or destroyed
    - This would most likely be related to adversaries using malware or hacking the BTS application intent to destroy the application.
4. Corruption or loss of BTSValidation data
    - From time to time, an application can be corrupted due to master data either missing or partially transacted transactions.
5. A loss of a key member, employee, or contractor
    - Out of all the potential foreseeable adverse events, this is the most challenging issue to handle for smaller companies.

Disaster response process

For each one of the potential foreseeable adverse events, BTS must develop an appropriate disaster response to mitigate the associated risk.

1. Abandonment of physical location
    - Step 1: Ensure the safety of all people in the physical facility of BTS. Make sure everyone has their medical situation taken care of within the limits of BTS's capability.

- Step 2: Using an Internet connection that can reasonably be considered secure, log in to the BTSValidation server and confirm that it is operational.
  - If the server is not operational, then attempt to start it using the Microsoft Azure admin console.
- Important Note: BTS staff all work and are given the capability to work remotely. Thus, physical location is not very important to our business model.

2. Collapse of the Microsoft Azure infrastructure
   - Step 1: If Microsoft's Azure admin console is not operational and Internet connectivity has been confirmed by connecting to another known operational public website, then contact Microsoft Azure at 866-425-4709 or 1-855-270-0615.
   - Step 2: If Microsoft Azure is unavailable due to a widespread outage, then the only alternative is to rebuild a temporary physical server and install the BTSValidation application on it.
3. BTSValidation or BuschTechSolutions website being taken over or destroyed
   - Step 1: Secure data from the backups. If online backups are not possible to be reached, then use offline backups.
   - Step 2: Rebuild BTSValidation on either a virtual machine or a physical machine for temporary use.
   - Step 3: redirect traffic from the destroyed or compromised virtual machine to the new BTSValidation server
   - Step 4: If it's determined that the BTS validation server has been compromised, then contact law enforcement. Ask the police to create an incident report.
   - Step 5: Contact our cyber security insurance.
4. Corruption or loss of client data
   - Step 1: Research the incident and determine the extent of the outage for the client due to corruption or loss of master data.
   - Step 2: Contact the client and inform the client of the corruption or loss of data.
   - Step 3: Determine if the data can be manually corrected within the tables to bring up the client.

    - Step 4: Pull backup data from the backups.
    - Step 5: Restore the client instance of BTSValidation by using a backups.
    - Step 5: Perform an after-action review (AAR) to determine what steps went well and which could have gone smoother.
5. Loss of key member, employee, or contractor
    - Step 1: Determine what type of loss this is:
        - Loss A: In the event the key member, employee, or contractor, is simply leaving the company, remove access to Microsoft Azure, GitHub, and O365 immediately.
        - Loss B: in the event of the death of a key member, employee, or contractor, first take care of the immediate family and the affected staff. Provide support to the extent that BTS can provide. After an appropriate length of time,
            - Perform all steps mentioned in Loss A (above)
            - Look for a replacement.

Preparation and training

To ensure that the business continuity plan is not just a theoretical document, it is essential to carry out regular preparation and training sessions at least once a year. An effective way to validate the recovery processes is by creating a BTSValidation template within BTS's own validation site and using it to confirm the mock execution of the recovery processes.

Notification list

As a part of our regular maintenance, we need to keep a notification list updated. Since the notification list contains confidential data related to our BTS classification, it will be managed separately from our business continuity plan. The notification list should include all members, employees, contractors, current client contacts, and terminated client contacts within a month of their termination.

The timeframe for action

The time frame for actions is proportional to the adverse event that necessitated the action to occur. There are two definitions that need to be defined:

- Recovery Time Objective (RTO)

    - RTO is the maximum time it will take to restore normal operations.
- Recovery Point Objective (RPO)
    - RPO Is the maximum amount of data that can be lost measured in time of the transaction (i.e. One hour’s worth of data).

1. Abandonment of physical location
    - RTO: 24 hours
    - RPO: 1 days’ worth of data
2. Collapse of the Microsoft Azure infrastructure
    - RTO: 96 hours
    - RPO: 7 days’ worth of data
3. BTSValidation or BuschTechSolutions website being taken over or destroyed.
    - RTO: 36 hours
    - RPO: 5 days’ worth of data
4. Corruption or loss of client data
    - RTO: 24 hours
    - RPO: 1 days’ worth of data
5. Loss of key member, employee, or contractor
    - Loss A:
        - RTO: 24 hours
        - RPO: 1 day’s worth of data
    - Loss B:
        - RTO: 36 hours
        - RPO: 1 day’s worth of data

Additional information

Regarding business continuity, this section covers additional information that was not previously discussed.

1. No additional information at this time