SAI360

Risk | Learning | EHS | Sustainability

PRIMER

SAI360's Top Nine Best Practices for Successfully Navigating a Long BC Emergency

Once upon a time, an IT Business Continuity (BC) plan consisted of how to restore the backup tapes at a hot site after a server room fire. Those days ended in the last millennium. Beginning with 9/11, the 2008 financial crisis, and now the COVID-19 pandemic, companies have to routinely plan for a diverse range of long-term IT emergencies. These nine tips for BC planning in the 21st century will help you design for long-term resilience rather than short-term recovery.

1. START WITH RISK MANAGEMENT

This means identifying critical business services, assessing risks to those services, and focusing resources on the most likely disaster scenarios that have serious business impacts. There are six key steps to this process:

A. LIST CRITICAL ASSETS

List the critical assets that are essential for continued operation.

B. IDENTIFY RISKS

Identify risks and rank them by probability, from accidental errors to national emergencies.

C. SEARCH FOR WEAKNESSES

For each identified risk, search for weaknesses that can cause processes to fail, such as 2FA depending on a single cloud provider.

D. ASSESS POTENTIAL CONSEQUENCES

Assess potential consequences, such as estimating financial losses for each risk.

E. PRIORITIZE RISKS

Use these priorities to assign planning effort going forward.

F. DOCUMENT RESULTS

Document results and perform multiple all-hands reviews.

2. IDENTIFY KEY PERFORMANCE INDICATORS (KPIS)

Every business has a set of KPIs that signal imminent failure. These KPIs measure business metrics, such as customer orders, supply margins, and economic metrics, that provide advance warning of tipping-point stressors. Define those limits in advance for your enterprise, and establish baseline values and normal ranges. Monitoring these KPIs can then give your BC plans enough lead time to be effective.

3. DEVELOP DISASTER SCENARIOS

These scenarios are of foreseeable events, which unfortunately today include weather-related disasters, terrorist attacks, and pandemics. Identify must-have critical resources necessary to continue day-to-day operations, even with degraded performance.
For example, after COVID-19's initial weeks of lockdown, when restaurants re-opened many pivoted to pickup and delivery operations. Not all succeeded, though, because few had the foresight to planning for this emergency.

4. PLAN MULTIPLE LEVELS OF SERVICE DEGRADATION

For restaurants that lost the ability to provide indoor service, advance planning could have helped many establishments survive government-imposed restriction. You should estimate maximum acceptable impact tolerances for multiple staffing and service delivery levels. According to foodservice research firm Datassential, 10% of US restaurants had closed permanently a year into the pandemic.[1] The problem is even worse worldwide. OpenTable's State of the Industry site, which tracks how COVID-19 has impacted restaurants worldwide, shows that some countries, such as Canada, still have more than half of impacted restaurants still closed, possibly to never re-open. Advance planning could have saved these businesses. You can still save yours.

5. MAINTAIN IT SECURITY

During an emergency, it's easy to overlook IT security in the name of expediency. But this is a false economy, as businesses are most vulnerable to attack during an emergency, something hackers readily exploit. The single most common IT security failure during the pandemic was the loss of *multi-factor authentication* (MFA).

People get lax, especially in times of stress, and many IT administrators discovered their MFA

[1] https://www.nrn.com/fast-casual/datassential-more-10-us-restaurants-have-closed-permanently

depended on a third party that stopped operating. So these administrators disabled MFA temporarily, to keep operations running. Many healthcare companies sustained data breaches as a result.

Now is the time to identify single points of failure in your authentication processes, and provide backup mechanisms. For example, most MFA systems support the use of a series of *one-time passwords* (OTPs): backup credentials that users can store securely on a mobile device, for user when MFA control flow is interrupted. Usable only once, these cannot be used by a hacker in a replay attack.

6. COMMUNICATE STATUS WITH YOUR CUSTOMERS

Ensure that your public-facing business interfaces are pre-configured to communicate emergency status information. You should consider a backup web hosting service to deliver this emergency status information. Also, set up in advance alternative communication channels for customers and business partners.

After making sure all of your staff members are safe and know their roles during the emergency, it's critical to reach out to all others who might be affected. In addition to your customers, this includes vendors, stakeholders, board of directors, and possibly even social media and local or national media. Your BC plan should assign key responsible contacts in advance to keep these information channels updated.

7. USE IT AUTOMATION TOOLS

On the back end of your business, IT automation tools can help ensure that BC processes go smoothly, both by limiting opportunities for human error, and by providing an audit trail of completed tasks. You likely already use these tools in your day-to-day operations. Exploit that existing capability to design emergency automation workflows today, before the emergency happens, to execute critical BC functions when the time comes. This will reduce labor, and staff stress in the bargain.

8. DOCUMENT EVERYTHING

Document the processes, strategies and systems to support key business services in a long emergency, and be sure to record the rationale for each BC process. Consider using purpose-built BC documentation systems, which are designed to facilitate review, be used during live testing, and provide collaborative editing.

9. "FAIL BACK" IS NOT AN OPTION

In today's BC planning, a long emergency is likely to impose equally long changes to your business and its operations. Be prepared for the long haul. Even with "traditional" disasters, such as fire or flood, failing back is usually not advisable. Given the transition to Cloud-first services, it's more important that you can fail over to equivalent services and plan to stay there.

With these nine best practices, you'll be prepared to transform from a "failover/failback" Business Continuity practice from the last century to a modern "persevere through the many faces of adversity" approach of today.