Business Continuity Planning

Defining and creating a recovery plan for business outages that impact your operations

Cyberattacks | Government Shutdowns | Natural Disasters
Overview

Business Continuity Planning (BCP) practices have been around for many years; however, unless required to by a specific management action, customer mandate, or applicable regulation, many have dragged their heels when it comes to implementing formal business continuity processes across their organization. Organizations that have not adequately planned for disasters are often forced into reactionary efforts and not able to prioritize clients, employees, and revenue-based focuses. Only after an earthquake, data breach, government shutdown, or similar disruptive event occurs do companies find themselves asking: “How can we verify the safety of our personnel and assets? Who do we need to contact? What are our immediate next steps within the next 48-72 hours? How do we resume business as usual?”

Answers to those questions require taking a holistic view of your organization and gathering data across all business lines, including executing detailed assessments across the organization, identifying roles and responsibilities, providing education and training for personnel, reviewing information technology (IT) infrastructure, and most importantly gaining management buy-in.

In short, BCP encompasses what actions your organization takes in order to be prepared in the case a business disruption event occurs and how to recover efficiently, effectively, and securely.

BCP Best Practices

In order for your BCP to be effective during a disaster, you should have immediate short- and long-term action plans. BCP considerations should be built into business processes, facilities, information systems, organizational structure, and strategy. Personnel must be educated on their BCP plans, know where and how to reference approved documented plans, and how to execute plans based on prior testing. With the right BCP structure and education, you can protect your company’s assets, keep your business functioning, and keep revenue coming in the door.
BUSINESS CONTINUITY PLANNING INCLUDES:

- Creating standards
- Documenting plans (at business line and/or site level)
- Educating personnel on those plans
- Testing plans on a periodic basis
- Continuous monitoring and refreshes of risk identified and addressed via BCP documentation

Crafting of the overall BCP process will differ based on risk appetites, industry, compliance requirements, and management approved standards.

BCP STRUCTURE

Senior management is traditionally responsible for setting the tone and standards your organization will employ during business continuity initiatives. These are documented and distributed to personnel via formal policies, procedures, and training. Your organization’s senior management or dedicated risk management personnel should be responsible for oversight of BCP processes. However, all business units should be responsible for applying the appropriate detail and due diligence in crafting and assisting in the BCP process.

DISASTER RECOVERY PLANS

A disaster recovery (DR) plan should accompany your BCP. In order to resume digital operations, a disaster recovery plan defines how information systems are configured, used, and how they should be restored during a disaster. IT teams are normally heavily involved in crafting DR plans, but business lines utilizing those tools are responsible for establishing which data and systems are critical to operations and must be restored.

In summary, to get your business back up and running in a timely, secure manner after a significant disruption—including having all the tools, software, and data needed to do your job—a robust DR program is your key tool.
Who Needs a BCP?

In short, everyone. Even the smallest businesses could benefit from having Business Continuity and Disaster Recovery plans to recover from a disruption. For instance, if a power outage hits your physical office and there is no emergency backup power, personnel who have already been trained on business continuity planning know the following:

- Processes for checking in with management, and downstream communication processes with customers and clients during outage if necessary
- Steps needed to maintain productivity, connectivity, and access to redundant information systems (e.g. Cloud backups)
- Processes and tools to track employee time used and charged during the length of the disruption
- How to coordinate and communicate with management and IT resources to determine next steps and when resumption of normal operations can be expected
- Processes to check for adherence to contractual obligations and communications processes for handling customer updates
- Any steps required on their part to help return to normal operations

If properly implemented BCP or DR processes are in place, business and customer impacts will be minimized. BCP and DR plans should be crafted at a level that covers any general business disruption and also addresses key scenarios that could impact your organization, with special considerations based on corresponding industries, geographical location, and more, including:

- Natural Disasters (Earthquakes, Tornados, Hurricanes, Flooding)
- Government Shutdowns
- Cybersecurity Incidents (Data breach, Ransomware, Virus)
- Facilities and Infrastructure Outages
- Key person dependencies/Loss of key personnel/Loss of key vendor
Privacy regulations such as HIPAA and GDPR, or organizations like FFIEC or NIST, require companies to be compliant in corresponding industries and to have suitable contingency plans in place. Companies that are not required to create and maintain BCP should develop plans to ensure protection of personnel and assets.

Data cybersecurity continues to be an area of concern and scrutiny. According to Norton, the U.S. is No. 1 for targeted cyberattacks. Taking a proactive approach to business continuity planning can ultimately save and protect your information assets, client data, resources, finances, and reputation.

The U.S. is the #1 target for cybercriminals

According to a study by Juniper Research, cybercriminals will steal an estimated 33 billion records in 2023. Jupiter expects more than half of all data breaches globally to occur in the United States by 2023.

How to Get Started

These steps can help businesses of any size build out a business continuity program:

**IDENTIFY KEY BUSINESS AREAS AND CORRESPONDING RISKS**

Without determining the key business areas across your organization, continuity and data recovery will not be effective. Areas to examine are processes and procedures, roles and responsibilities, and business critical operations. A business impact assessment (BIA) is conducted to identify business areas, as well as provide information about risks specific to each area. The BIA will also determine potential organization-wide impacts, roles and responsibilities, key person dependencies, third-parties relied on, and supporting information systems/IT resources required.

**DEVELOP AND STANDARDIZE POLICIES AND PROCEDURES**

This is key in setting the tone for your business. Senior management must ensure that the importance of these efforts are communicated consistently across the organization and enforced. Creating and distributing a formal document to personnel is an effective way to educate employees about how to incorporate BCP considerations into everyday tasks.
CONTINUOUSLY MONITOR BCP AND DR PROCESSES

BCPs and DR plans should reside in living documents, requiring periodic reviews and updates based on changes to your organizational structure, business processes, and IT environment. These documents should be reviewed on an annual basis or when significant changes occur. Employees should be informed of any key updates during annual training sessions on general BCP processes and security awareness. BIAs may be re-performed on a periodic basis as established by management, which will in turn feed updates to BCPs.

Finding the Right Strategic Partner

Determining what to do next depends on the maturity of your business’s current BCP plan, and finding the right partner for your organization is key. You can get a jumpstart on this process by hiring individuals familiar with implementing and governing a BCP/DR program, as well as working with an experienced third-party to get your initiatives on the right track. Many BCP consultants can offer services in the form of a proposal.

An investment of time and resources upfront can yield powerful return when a disruption arises. A solid BCP plan provides management and customers with peace of mind that your organization is equipped to handle a crisis, without compromising the quality of service your internal and external partners are accustomed to.
As outlined in this document, the effort required to implement BCP and DR processes can be significant. Evaluating your existing environment and existing gaps can be an intimidating task, especially if you need to also undertake appropriate and feasible remediation actions. Aronson’s Risk Advisory team has decades of experience in dealing with BCP evaluations, assistance with BIA, drafting BCP/DR policies and procedures, and consulting on remediation actions to get your organization BCP ready. We offer a wide range of services designed to assist you in achieving your BCP/DR needs.

Let us help get you started on your business continuity endeavors. For more information or to discuss a BCP/DR consultation, contact:

LEXY KESSLER
Partner
lkessler@aronsonllc.com
301.231.6218

RENZO PORTELLA
Manager
rportella@aronsonllc.com
301.231.6657

About Aronson LLC

Aronson LLC provides a comprehensive platform of assurance, tax, and consulting solutions to today’s most active industry sectors and successful individuals. For more than 55 years, we have purposefully expanded our service offerings and deepened our industry specialties to better serve the needs of our clients, people, and community. From startup to exit, we help our clients maximize opportunity, minimize risk, and unlock their full potential. For more information about Aronson LLC, please visit www.aronsonllc.com or call 301.231.6200.