EQUINIX

WHERE OPPORTUNITY CONNECTS

SUCCESSFUL BUSINESS CONTINUITY PLANNING FOR FINANCIAL SERVICES

EQUINIX BEST PRACTICES GUIDE

Equinix.com

TABLE OF CONTENTS

SUCCESSFUL BUSINESS CONTINUITY PLANNING FOR FINANCIAL SERVICES IN THE 21ST CENTURY

If you are relatively new to business continuity planning (BCP), then you are likely gathering information from an array of sources in an effort to understand what is important to your company and where you should focus your attention first. As the host data center provider to many of the world's largest organizations, Equinix is in the business of helping its customers protect and connect their mission-critical applications and systems in the face of any type of event. This brief introduction to BCP is based on lessons learned by Equinix professionals across more than a decade of direct experience with our customers.

A Business continuity plan is a set of procedures that define how a company mitigates, reacts, continues or recovers its critical functions in the event of an unplanned interruption in normal operations.

THE SCOPE OF BCP

Drivers and Pressures

While prudent businesses have been practicing BCP for decades, today's major focus on BCP first began for many firms in the aftermath 9/11 when both companies and governments (via regulations) made significant investments in "disaster recovery" programs spanning catastrophic attacks to natural disasters. Additional high-profile events—including the US East Coast power outage in 2003, terrorist attacks in financial centers like London, and hurricanes, earthquakes and tsunamis—have occurred with such frequency in the past decade that the BCP manager's credo has now evolved to "expect the expected."

In 2008, the chaos, uncertainty, and disruptions of the financial crisis made clear that BC planners needed to focus on how to keep their operations running—and minimize business impact—in the face of a variety of disruptions involving people, technology infrastructure, and supply chains. In addition, the financial crisis led to significant new regulations in the financial services sector related to developing business continuity plans. Keep in mind the need to balance investment in BCP while tightening budgets—a juggling act to minimize spend, maximize value, and create an ROI model for your investment.

Holistic

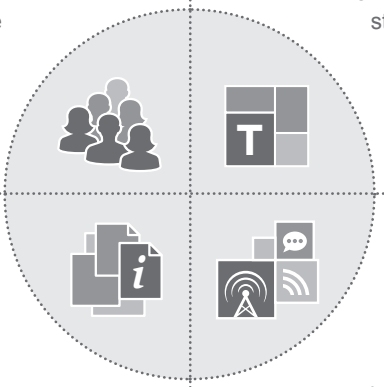
For BC planning to be successful—to ensure a business will keep running with a minimum of downtime—the plan must be truly "holistic" and encompass four key elements:

People

Where will people work? How will they get there? Do they know what their roles are in a crisis? Are there back-up assignments for each role? In the case of a longer term outage, how do you arrange to provide for normal creature comforts? Depending on the nature of the disruption, have healthcare or trauma related services been considered?

Technology

How much of the technology infrastructure needs to be reconstituted in what kind of timeframe? How will it be recovered? Will it adhere to all regulatory and compliance requirements in order to allow business operations to continue? How will access be guaranteed for staff, partners, and customers?



Information

Is all required digital—and paper—information currently protected and backed up so it will survive any anticipated threats? How will the digital assets be accessed by the recovered infrastructure? How will people be able to access the paper assets if necessary?

Communications

How will voice and data communications be restored and maintained? Should one platform have priority over the other? Does your data network have diversity in routes and carriers to ensure resilience? What corrective actions can you take if the cell phone network is down?

Trying to tailor your BC plan to address the specifics of every possible scenario can lead you into a bottomless pit of planning

Comprehensive

- **Risk Assessment: Plan for the Effect, Not the Threat** – A key BCP lesson that has been learned is that while it's very important to understand the potential risks inherent in your location and business, trying to tailor your BC plan to address the specifics of every possible scenario will lead you into a bottomless pit.

  Yes, you do need to make a risk assessment. What are the potential threats to your location? Are you in an area targeted by protestors or terrorists? Are you in a flood or earthquake zone? Is your area subject to hurricanes or heavy snow storms? Is your particular building located near other businesses that could pose a threat, such as hazardous chemicals? But since you can't anticipate all threats, your goal is to understand how any of the various scenarios will impact your building and area. Simply focus on the potential effect:

  How will your organization respond to unforeseen inability to access your production facility and connectivity services as a result of a local or regional event of a certain expected duration? How will your BCP be triggered? How will the immediate and longer-term impacts be assessed and handled?

  A focus on these fundamental questions will clarify your thinking about BC and help you deliver practical solutions for your particular operation. The ultimate goal is for you and your entire management team to understand how your plan is activated—no matter what the crisis may be—and how the immediate and longer-term impacts will be assessed and responded to. It is the business impact analysis (BIA) that will ultimately define the criticality of your applications and systems, and the priorities for a recovery, providing you with the response to any crisis with a minimum of disruption.

- **Business Impact Analysis** – It is important to compare the cost of downtime to the business with the cost of implementing the BCP. By doing so, you can demonstrate the need for additional investment in BCP or devise a less costly plan. As a part of the BIA, determine which people and organizations are most important to revenue flow and customer satisfaction. Can you continue operations if you have data access but not phones? What happens if some applications work but others do not? The recovery time objective (RTO) is the minimum time required for getting the critical production capabilities back online—e.g, 24 hours, 12 hours, or immediate. The recovery point objective (RPO) is the measure of how current the data must be in order to resume business operations. By establishing these metrics, you can measure the potential costs of recovery against the business impacts. You should also consider "tiering" your recovery. By bringing people, infrastructure, and applications back online in a phased approach, the most business critical take priority. For example, consider the 80-20 rule in financial services. If five trading desks out of 20 account for 80 percent of revenue, you can put those five desks into tier 1 and leave the other 15 in a lower tier to be brought back at a later time.

- **Business Continuity Plan** – As mentioned above, the business continuity plan itself must be holistic and comprehensive. It should also be auditable by all relevant organizations, including appropriate regulators (very important for financial organizations), IT, human resources, risk management, the executive team, the board of directors, etc. And it must be thoroughly tested using a variety of planned and surprise scenarios, with the results properly recorded and available for review.

- **Disaster Recovery Planning** – The disaster recovery plan is a critical subset of the BCP. This plan includes the specific procedures and requirements for the recovery of IT systems and bringing an alternate production site online.

- **Crisis/Incident Management** – This program focuses on people and communication. What are the roles and responsibilities in the event the BCP is set in motion? Who has responsibility for activating the plan? Who has backup responsibility if those individuals with primary responsibility are unavailable? How will people be informed that the plan has been set in motion? What if various communication platforms are not available?

- **Education, Training, Testing, and Reassessment** – A BCP will not be successful if people don't know about it, if they aren't trained to handle both their primary and backup responsibilities, if the plan hasn't been tested against a variety of scenarios, and if the plan isn't continually updated to account for changing business conditions and potential threats.

WORK AREA RECOVERY

Your BCP must take accountabilty for how and where an alternative production facility becomes live!

One critical aspect of BCP is work area recovery, and for financial services, the most critical work area is the trading room. What happens if the building that houses your production facility becomes inaccessible for an extended period of time? In this event, your BCP must dictate how, when and where an alternative production facility becomes live, how the required people will reach the facility, and how the critical IT infrastructure, applications, and communications capabilities will be channeled to the facility.

Facilities

Depending on the criticality of your production facility, your RTO/RPO, and your ROI analysis, you will need to decide between three basic options for your backup production facility.

Dedicated, Private Facility

A dedicated, private facility is the lowest-risk, fastest-recovery option. Such a facility is fully furnished, secure, and resilient. It is equipped with data and voice connections, includes a sufficient number of workstations for the number of people expected to work during the crisis and recovery, and provides access to all the mission-critical applications and materials they need to do their jobs.

Because you are designing this space for people, it should include access to conference rooms, general office utilities (copiers, fax machines, printers, etc.), and pantry/lounge area.

Finally, the facility should satisfy all legal, regulatory, and compliance requirements, and be scalable to accommodate evolving needs during a prolonged crisis.

For financial services firms, a dedicated, private facility should be equipped with the latest workstation technology, including:

- Dedicated trader/dealer desks
- Multiple monitors
- Dealer boards (turrets or VoIP phones) with voice recording and connectivity to access counterparties and research
- News and market data feeds
- Ticker plant
- Order/trade management systems

Shared Facility

A shared facility has the same capabilities as a dedicated, private facility, but the space is contractually shared with other companies. While less expensive than a dedicated, private facility, the space must be customized to the specific needs of each business at the time of a test or recovery (applications, access to private data, selected market feeds, etc.), which means that it will take longer for the facility to come online.

In addition, in a wider-area event, another business that shares the space may occupy the facility before you, pre-empting your progress toward recovery. If you choose this option, look at the other companies sharing your space to assess how likely it is that they will be caught up in the same event impacting your company.

Temporary Space
Many companies rely on temporary spaces for their recovery options; however such an approach carries a significant risk of a very slow time to recovery. In addition to the need to equip such a facility with the required furniture, technology, and connectivity—at a time when vendors may be overwhelmed by other requests stemming from the crisis—there may be issues related to security and meeting legal, regulatory, and compliance requirements.

Some companies' work area recovery schemes rely on working from home or local cafes offering Wi-Fi, but such an approach carries the highest level of risk. While these sites may be sufficient for individuals needing to make phone calls and write reports, they are insecure, lack access to mission-critical applications, and especially for companies in financial services, put companies at risk of significant legal, regulatory and compliance violations.

However, it is possible to address the inherent lack of security and resiliency in the "work from home" approach if it is carefully developed to account for physical and data security, backup power, access to mission-critical applications, and legal, regulatory, and compliance requirements. Note that by the time all these aspects are managed for a sufficient number of people, it may be far more logistically complex and expensive to implement and manage than the dedicated, private approach, not to mention the inherent reduction in efficiency and ability to collaborate when taking a centralized people function and geographically dispersing it.

People

No matter how sophisticated and fully equipped the backup production facility is, it's of no value if the required people can't get there in a crisis or are unable to work. And their ability to get to and effectively use the backup facility depends on a number of factors depending on the type of event:

Commuting pattern – How far are employees currently traveling to work? How far would they have to travel to the backup facility? Is the facility close enough to be practical but far enough away to minimize the likelihood it would be caught up in the same event? Would the employees need to stay in hotels?

Dependents – Do the employees have dependents that need to be accounted for during a crisis? What happens if the plan trigger is a snow storm or flood that closes local schools? How will the employees manage childcare and pet care? Are there childcare and kennel facilities located near the back-up facility?

Safety and comfort – Is the backup facility in a safe area? Does it provide creature comforts (access to food, clean restrooms, etc.) that will support sustained work effort?

Crisis management – Will crisis management phone trees be operational? Will management be able to check in on employees to ensure they are safe and accounted for?

Backup roles – "Eliminating a single point of failure" is an established practice for the IT infrastructure, but it is also important when it comes to people. No one person should be so vital to business operations that his or her lack of availability would prevent recovery. This requires that multiple people be trained for each critical operational role.

It is vital that the backup network infrastructure be as robust and reliable as your primary network infrastructure

Data Services

In bringing data services to the backup facility, it is vital that the backup network infrastructure be as robust and reliable as your primary network infrastructure. It should be fully redundant and continuously monitored, and it should have no single point of failure. It should rely on multiple paths and multiple providers, so that if one provider is affected by the crisis or overloaded during the recovery, you have access to a second or third provider. To do this, make sure your backup infrastructure is located in a network-dense facility that provides the maximum options for connectivity.

Numerous options exist for ensuring application and data availability. These options are driven by three factors:

1. Recovery targets (RTO/RPO), technology in use, and budget.
2. Data replication technology and network bandwidth requirements vary greatly. For example, a company running a mission-critical trading application in production may choose to employ a geographically load-balanced active/active solution for its backup platform. This solution can instantly failover without a service interruption thanks to synchronous data replication over very high-speed data circuits. While a very low risk-option, it is quite expensive and technically complex. By contrast, a company with a less critical email system to protect may choose periodic file "snapshot" replication running on a much slower network connection. Today many people are looking at the services offered by the burgeoning cloud market as a way to balance recovery targets and budgets.
3. Ultimately, the difference in cost and technology used should be a cooperative effort between the business unit and the IT department under the guidance of the business continuity organization.

Financial services firms must maintain access to diverse market feeds. Just as you plan for a network-dense facility with the maximum options for network connectivity, make sure your backup facility can provide access to all the required market feeds.

Voice Services

Voice services are critical both to continuing business operations and to communicating during the immediate response to the crisis. Ensure your backup facility provides access to multiple telecom providers, and consider leveraging voice over IP (VoIP) services, which can provide voice communications over the more robust and flexible internet network in the event that the telephone system is not operating.

BEST PRACTICES

Here are 10 best practices that will help focus your thinking and guide you toward a more successful BCP effort.

1

Get Management Buy-in

A must for every large-scale project that cuts across departments is broad management buy-in as it is crucial for BCP because it is essentially an investment in something you hope you'll never use. To encourage buy-in, go beyond presenting the mere potential damage by not being prepared for a disaster, include RIO benefits of implementing the plan. These include using the backup infrastructure for other purposes, such as training days or development testing (as long as these are pre-emptible), identifying obsolete or unneeded applications during the prioritization process, and having more flexible employees who are better trained in more activities vital to the organization, thus reducing recruiting and job transition costs.

2

Think Globally

As you develop your BCP and design your backup production facility, consider the ability to replicate the process globally to avoid having to start from scratch in each market. Are your key vendors available where you need them?

3

Think Ecosystem

When it comes to your trading room, think about how you connect to your ecosystem of critical data sources, counter parties and service providers. Ideally you will want to connect to as many possible inside the same facility to minimize network costs. At the same time, look for a backup site that has density of network providers as well, for connections that go outside the building.

4

Prioritize

Simplify recovery by taking a tiered approach. Prioritize the processes and applications that must come online first, and design your plan so that the supporting infrastructure for these processes and applications become available first.

5

Regulatory or Audit Review

Ensure the recovery infrastructure will be consistent with all legal, regulatory and compliance requirements. This is especially critical for financial services firms that face mounting and evolving requirements.

6

Evangelize

As your plan takes shape, distribute it widely and make it available in multiple formats, including paper, PDF and web. Develop a system (e.g. regular meetings, email updates) to ensure that executives and managers are familiar with the plan, know how to access it, and understand their roles in triggering the plan and responding to a crisis.

7

Train

Today, a variety of resources exist that can provide additional information on BCP. These include articles, books, conferences, and local and global trade organizations. You can also consider enrolling in a certificate program.

8

Test

Design and run a variety of announced and surprise test scenarios. For example, you can regularly run through "tabletop exercises," where you sit in a room, propose a disaster scenario, and discuss each person's response activities. Better perhaps to initiate a surprise scenario? For example, announce that a bomb has just gone off in the basement, designate a number of people who are on vacation and hurt in the explosion, and then have everyone else implement the plan.

9

Plan Maintenance

People, business requirements, business facilities, partners, vendors, and regulations all change over time, resulting in the need to update the RTO, RPOs, recovery tiering strategy, roles and responsibilities, etc. You should design and maintain a rigorous reassessment schedule and update the plan accordingly.

10

Personnel Plan B

Make sure you have a second and third backup person trained for each critical response and recovery function (including yours) in the event that a primary individual is unavailable (i.e. out of town, on vacation, affected by the crisis). These functions include making the decision to trigger the plan, leading the internal communication effort, contacting vendors, and responding to the media.

Equinix—A Critical Business Continuity Partner

Through its global footprint of provider-dense data centers, Equinix offers robust and reliable backup infrastructure—both dedicated and shared—along with state-of-the-art business continuity trading rooms equipped with the latest workstations, dealer/trader desks, multiple monitors, VoIP phones or trading turrets with voice recording, and various market data feeds. This backup infrastructure service includes all the people-related features to operate a mission-critical trading function, such as furniture, communications equipment, conference rooms, utility rooms and a pantry area.

Equinix high performance data centers create a dynamic partner ecosystem, connecting more than 1,400 network service providers, more than 2,500 IT and cloud service providers, and more than 1,000 financial services firms, including more than 475 buy/sell firms and more than 175 exchanges. Equinix operates 145+ data centers in 40 strategic markets across the Americas, EMEA and Asia-Pacific.

For more information about an Equinix Business Continuity Trading Room, visit http://www.equinix.com/solutions/by-services/business-continuity/overview/ or call +1 (201) 422-6695.

Corporate HQ

Equinix, Inc.
One Lagoon Drive
Redwood City, CA 94065
USA

Main: +1.650.598.6000
Email: info@equinix.com

EMEA

Equinix (EMEA) BV
7th Floor Rembrandt Tower
Amstelplein 1
1096 HA Amsterdam
Netherlands

Main: +31.20.754.0305
Email: info@eu.equinix.com

Asia-Pacific

Equinix Hong Kong Limited
Units 6501-04A & 6507-08, 65/F
International Commerce Centre
1 Austin Road West
Kowloon, Hong Kong

Main: +852.2970.7788
Email: info@ap.equinix.com

About Equinix

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners inside the most interconnected data centers. In 40 markets across five continents, Equinix is where companies come together to realize new opportunities and accelerate their business, IT and cloud strategies.

In a digital economy where enterprise business models are increasingly interdependent, interconnection is essential to success. Equinix operates the only global interconnection platform, sparking new opportunities that are only possible when companies come together.

Business Continuity Planning White Paper v0816 WP-EN NC-LK
Q216