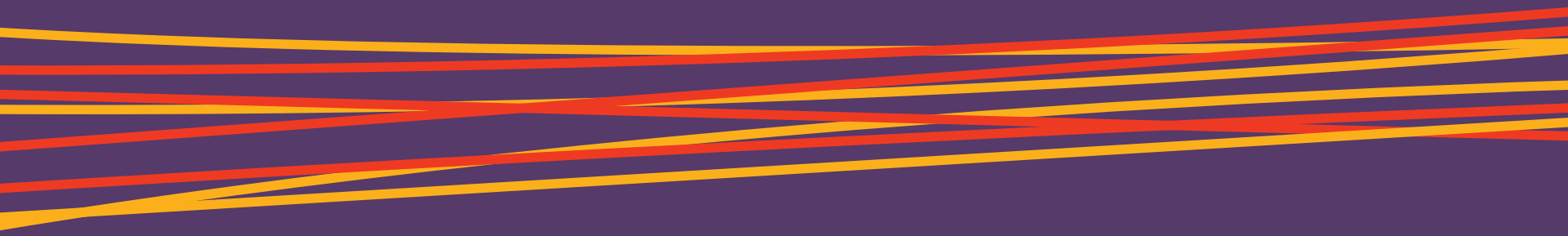
DISASTER RECOVERY : SERIES 1

HOW TO AVOID AN IT DISASTER

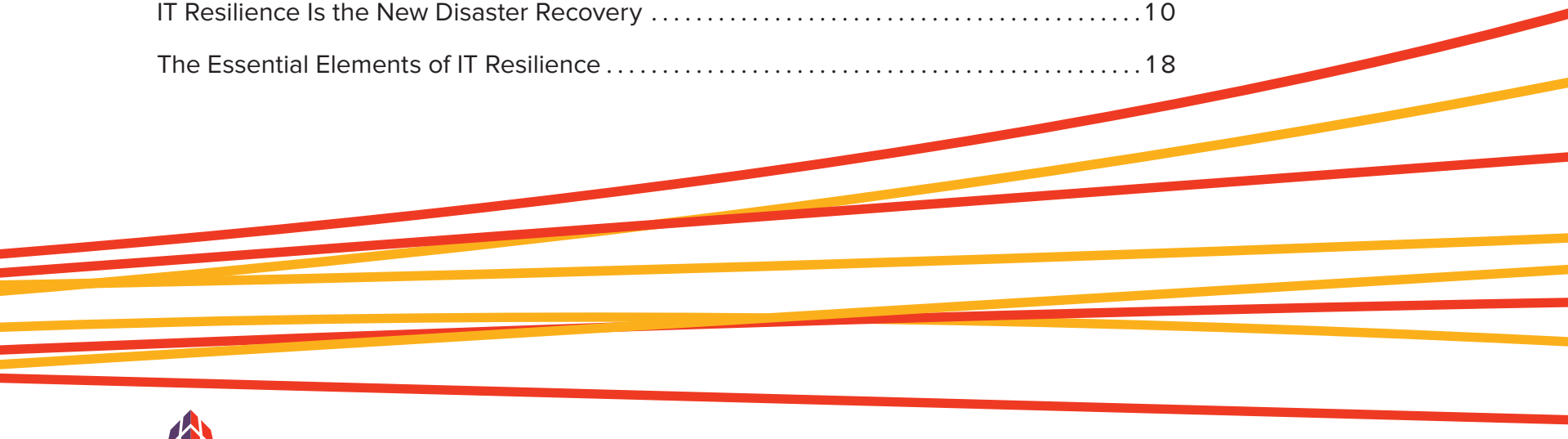
DC BLOX

"Business' steadily increasing reliance on technology as a competitive edge along with the growing complexity of IT environments demand proactive planning for disastrous events. Businesses simply no longer have the luxury of extended system downtime, no matter the cause. Data centers play a critical role in both disaster recovery and resilience strategies and we believe that there are important attributes of both that businesses need to consider as they evaluate their options."

— Kurt Stoever, Chief Product and Marketing Officer, DC BLOX



How to Avoid an IT Disaster



Business Continuity and Disaster Recovery Planning

The dizzying pace of technology innovation has given rise to possibilities unimaginable even ten years ago. Cloud services, big data, IoT, mobile apps, and others are providing enterprises new ways of improving their bottom line. What hasn't kept pace are the policy, people, process and technologies to keep it all running when unexpected events occur. What will you do when disaster strikes? Do you have a business continuity and disaster recovery plan for your business?

The Problem with Disaster Recovery

Business continuity and disaster recovery plans are the ginger haired foster child of IT. It's always invited last to the dinner table, ignored by the parents but yelled at loudest when it fails. The inconsistency in how companies and industries approach this is understandable. Think about it. It's hard to bring yourself to pay for something you hope you never have to use, and when you do, it's probably because of something awful. Expressing the Return on Investment for business continuity planning is really hard. Because of this, lots of organizations push off developing business continuity and disaster recovery plans to "later."

> *"Without question, the Federal Government has had the greatest impact on business continuity and disaster recovery."*

Requirements Driving the Need for Business Continuity and Disaster Recovery

Without question, the Federal Government has had the greatest impact on business continuity and disaster recovery. Through regulation and law, the Government has influenced the requirement for disaster recovery albeit with a noticeable lack of how. Entities and organizations that serve the "common good" are required to have measures that protect against and recover from disruption. Graham-Leach-Bliley, Sarbanes-Oxley, and HIPAA all use regulatory pressure to

CONTINUED | Business Continuity and Disaster Recovery Planning

mandate data protection, disaster recovery and business continuity policies and practice. The events of 9/11 were clearly a tipping point for the severity of disruption and how exposed certain industries were without continuity plans.

A Simple Approach to Business Impact and Risk Assessments

Your company or division has reached the point where an unforeseen event will affect the organization's core purpose. Not everything you do is core to your business. There are some activities you have to do, but they aren't why you exist. Have you performed a Business Impact Analysis (BIA) to understand the impact of a disruption on core (or critical) functions and identified potential loss scenarios (or hazards) through a modest Risk Assessment (RA)? Don't get fancy and try to apply statistical methods. Underwriting and insurance companies use the law of large numbers to create risk models. You don't have that.

Keep it simple and ask yourself:

1. What happens when this fails?
2. How long can I wait until it comes back?
3. What's the impact on the delay between failure and restore?

This is the BIA.

Staying with the simple theme, there is the risk (something happens good or bad), a cause (the trigger) and the impact (outcome). As a result of "cause," an "uncertain event" could happen which might lead to an "effect."

This is the RA.

Once you can establish a cadence, try to create an easily repeatable process for both BIA and RA. It's very important to identify and keep pace with changes to business processes and related impact.

CONTINUED | Business Continuity and Disaster Recovery Planning

Just because there's risk doesn't mean you have to create, maintain and test for every risk event. How far you decide to go should be based on how the outcome affects the organization's core purpose. Contractual and regulatory compliance requirements also dictate the degree of planning required for in-scope systems. A common nomenclature for risk management would look like this:

- Avoid – eliminate any impact of risk event
- Accept – if it happens, deal with it
- Transfer – move it somewhere else; e.g. the cloud
- Mitigate – take steps to reduce outcome should risk event occur

Have you evaluated the different risk handling alternatives (accept, avoid, etc.) available to you? Business continuity and disaster recovery planning isn't just IT. Sure, you may experience equipment or software failures and be aware of natural disasters like flood, hurricane and tornado. What about pandemic, cyber-hostage, or even key employee or supplier turnover? By thinking about the three simple questions you'll be able to consider all possibilities of disruption and be able to plan to respond.

Disaster Recovery Planning is Changing

Much of today's disaster recovery planning can be traced back to cold war Government preparedness. The secret bunker at the Greenbrier resort exemplifies the 1950's thinking of how to react to an apocalyptic event; bad things will happen, so you must duplicate as much as possible. When you think about IT business continuity planning, the historical mainframe mentality is not applicable to today's decentralization of business functions, IT delivery and outsourced services; "the stuff is everywhere."

Another problem with legacy disaster recovery and business continuity plans is that they are hard to test because the event is typically destructive or catastrophic. Because of this, if the plans are tested they may not fully expose the plan effectiveness. It takes imagination to create reasonable tests and plans for disasters. Business continuity and disaster

CONTINUED | Business Continuity and Disaster Recovery Planning

recovery plans have to change with the business and the technology that supports it. Have you considered how your legacy disaster recovery plan has scaled with your business. Do you have the necessary resources to execute TODAY?

Business Continuity in the Cloud

Yes, workloads are moving to the cloud which means that some risk is transferred to the provider. What does the provider do with that risk? What happens when the cloud fails?

- March 2017, a typographical error by cloud provider technician disabled hundreds of thousands of customers for hours. A month earlier, the same provider had a 4-hour storage services outage.
- August 2017, an interactive cloud-based online gaming environment was unavailable preventing login, multiplayer games, and even login for single-player games.
- October 2017, during routine data center maintenance, an accidental activation of a fire suppression system created a sequence of cascading failures that resulted in a loss of cloud-based compute, storage, backup/recovery and reporting for over 8 hours.

Just because you've moved workloads to the cloud doesn't mean you are insulated from failure. You still must assess the risk, create a plan, practice, test and update.

Can your Data Center Deliver Business Continuity?

Despite highly advanced engineering and N+ "whatever" designs, the data center industry still experiences business affecting failures. Causes range from "faulty UPS," "generator failure" and "poorly manufactured switch gear" to "squirrel in transformer." 77% of 200 CEO's surveyed by the Marsh Group in 2015 expected a failure in their data center.

Time will tell how the data center hubs of Ashburn, Atlanta, Chicago, Dallas and Santa Clara deliver reliability and redundancy for the emerging needs of IoT, IIoT, mobility and service needs on the Edge.

CONTINUED | Business Continuity and Disaster Recovery Planning

In summary, nothing's failure proof. We can't predict or control nature and whenever there's a human involved, there's a possibility of a mistake. Look at the fundamental purpose of your business and begin to build a list of exposure. Prioritize your list and decide how you would treat each risk and then create a budget. Don't forget that business continuity and disaster recovery plans require update, test and practice. Ultimately, you will weigh the costs of the risk event against the cost of having a plan to address it.

IT Resilience Is the New Disaster Recovery

Given the financial and reputational threats of unplanned data center outages, it's time to start thinking about IT Resilience, an approach that John Morency, Research Vice President at Gartner, has described as "the new disaster recovery." With IT Resilience, CIOs and IT staff evolve from Disaster Recovery, Business Continuity and Continuity of Operations models which are inherently reactive to one that is preventative and proactive, and designed and executed for organizations to be able to ride through an adverse event.

Make no mistake. The IT decision-maker that interprets the difference between IT Resilience and Disaster Recovery as merely a question of semantics does so at great peril to his or her organization.

A 2016 Ponemon Institute report estimated that the mean cost of an unplanned data center outage is $740,000 with a maximum of approximately $2.4 million. Crunching numbers further, a study by the Aberdeen Group found that the cost of downtime per hour for medium-sized companies was $216,000 and for large enterprises $686,000.

If these statistics fail to grab your attention, you are not alone. Despite the economic fallout caused by unplanned outages due to natural or man-made catastrophic events, the Disaster Recovery Preparedness Council found that nearly three-quarters of organizations worldwide aren't adequately protecting their data and systems.

But you might also want to consider this: According to the Federal Emergency Management Agency (FEMA), more than 40 percent of businesses never reopen after a disaster, and of those that do, only 29 percent were still operating after two years. As for those that lose their information technology for nine days or more after an adverse event? These companies enter bankruptcy within a year.


FINANCE
COMMERCE

CONTINUED | IT Resilience Is the New Disaster Recovery

Business disruption, lost productivity and lost revenue, to say nothing of the injury to brand reputation compounded by 24-hour news cycles and social media, are all too frequent outcomes even when a company does manage to stay viable following an unplanned outage. When an 11-hour IT system outage occurred last December at Atlanta's Hartsfield-Jackson International Airport, the mishap not only cost the affected airline $50 million, but forced it to cancel some 1,400 flights and lose an incalculable number of brand champions whose loyalty will likely never be recovered.

But whether caused by equipment failure, cyberattack, extreme weather events, human error, or power outage, many companies have poor insight into whether they can fully recover from extended outage, because their Disaster Recovery plan is rarely tested or scores low marks in preparedness.

According to a Disaster Recovery Preparedness Council Survey:

- 73% of survey participants worldwide scored ratings of either D or F in disaster readiness
- 60% surveyed do not have a fully-documented Disaster Recovery plan
- 40% admitted that the Disaster Recovery plan they currently have did not prove useful

And even if your firm does have a well-planned and rehearsed Disaster Recovery plan, Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) can be damagingly expensive if not targeted within the optimal parameters.

Given the above-mentioned stakes, liabilities and pressures, it's high time that CIOs prepare for unplanned outages and adverse events from a position that is both proactive and preventative. It's time to implement a strategy of IT Resilience.

CONTINUED | IT Resilience Is the New Disaster Recovery

Let's Level Set

Broadly defined, IT Resilience is an organization's ability to maintain acceptable levels of service regardless of what challenges may occur. But before we look at IT Resilience in greater depth, let's establish some agreed-upon definitions concerning Disaster Recovery, Business Continuity and Continuity of Operations to better understand where IT Resilience fits.

- **Disaster Recovery (DR)** is a set of policies, procedures and physical assets deployed by an organization that enable the recovery or continuation of vital technology infrastructure and systems following a disaster or negative event.
- **Business Continuity (BC)** as defined by the Business Continuity Institute is a plan to deal with difficult situations so an organization can continue to function with as little disruption as possible. A key component is the Business Continuity Plan, or BCP, which sets forth the policies, processes, procedures and instructions that enable a business to respond to a disaster.
- **Continuity of Operations (COOP)**, which was developed in accordance with presidential and U.S. Department of Homeland Security directives, is an effort within individual executive departments and federal agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of adverse events, including localized acts of nature, accidents and technological or attack-related emergencies. The concept of COOP has since evolved beyond federal agencies and adopted by non-governmental organizations and institutions, such as hospitals and colleges and universities.

In this framework, both Disaster Recovery and Continuity of Operations are considered to be subsets of Business Continuity.

IT Resilience, a Paradigm Shift

Be assured, unplanned data center and system outages and other adverse events are not a question of if, but when. That said, by implementing a carefully and intelligently designed

CONTINUED | IT Resilience Is the New Disaster Recovery

IT Resilience strategy that integrates distributed data centers, the physical security of the properties on which they sit, low latency network connectivity, and data replication capabilities, these events needn't become debilitating to an organization's ability to continue doing business.

But IT Resilience isn't just about implementing geographically diverse colocation sites for failover and deploying automated network configuration backups. It's also about integrating data centers and advanced technology solutions with policies, processes and people working in concert at any point in the crisis cycle.

A useful analogy to better understand the differences between traditional Disaster Recovery and IT Resilience is to consider the difference between brittle materials and ductile materials. When a low load is applied to a brittle material, such as glass, the material will come back to its original shape after the load is lifted, but at moderately high loads, the fracture is permanent – glass breaks. In contrast, ductile materials, such as aluminum or steel, will go through various stages before fracture and can be bent or stretched into wire while maintaining elasticity.

The goal of IT Resilience is to factor in data from Business Impact Analysis (BIA) and determine the risks and relative costs associated with anticipated threats, and then design organizations and systems that can withstand an adverse event and thus avoid recovery. While no system has unlimited elastic resilience, the new paradigm is to enable people, processes and technology to undergo stress, stretch and "bend to the event," but not break and cause permanent damage to the organization's ability to continue doing business.

Another way to look at the difference between IT Resilience and Disaster Recovery is to consider these concepts in relation to the building engineering sector. With resiliency, engineers employ earthquake-resistant construction methods and materials to withstand seismic events, while recovery involves

earthquake response teams scouting and assessing structural damage. IT Resilience, therefore, is prevention and the ability to ride through unexpected events when they occur. So, let's take a look at some of the cornerstones of a resilient organization.

IT Resilience Closes the Gap Between Business Continuity and Disaster Recovery

An effective IT Resilience strategy guides CIOs and their IT teams to close gaps in existing BC and DR plans across various components of IT, from networks to data centers to applications, in a more deliberate, methodical and constructive approach. Defending systems entails more than merely securing them, it also means taking measures that can reduce the probability of system failure. These steps could include load balancing servers to prevent an overload, or providing redundant systems that can prevent single points of failure.

Other proactive and preventative measures that improve resiliency include real-time traffic analysis that allows IT to spin up workloads and draw down capacity on demand, container movement to protected service regions, and deploying VMware VMotion, which enables the live migration of running virtual machines from one physical server to another with zero downtime, continuous service availability and no disruption to end users.

Early Detection Is Critical to Data Center Resilience

Many organizations have no effective tools or processes in place to alert IT staff of service disruptions in the data center. This is a major but remediable flaw, because the faster that IT members are alerted that a system has gone down, the faster it can remediate the problem. Beyond reporting a system outage, implementing a monitoring solution that gauges the performance of physical servers and their specific applications and services can assist IT staff to understand and address problems before they can cause a full disruption.

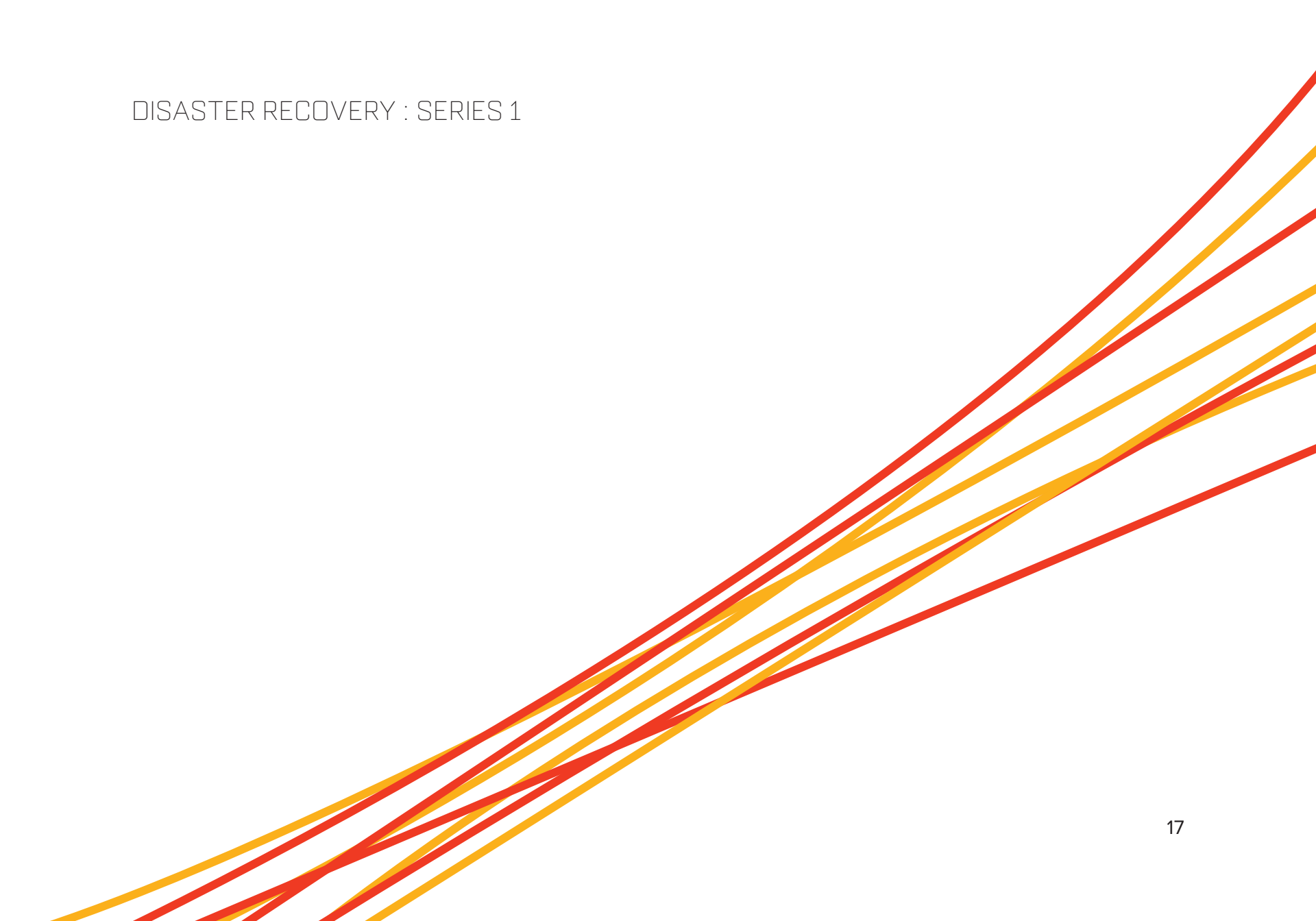
CONTINUED | IT Resilience Is the New Disaster Recovery

Moving Beyond Recovery to Ride Through

A detailed plan for addressing the effects of a disruption provides the foundation of IT Resilience. Historically, the focus of BC has been on IT Disaster Recovery — how to restore in the event of failure. But the ultimate goal of resilience is to ensure that when systems fail, IT can still provide essential services. Today, technology has evolved so that the focus is no longer on how to restore but how to ride through events. As some industry experts have recognized, advanced solutions such as data replication, continuous data protection and snapshotting can assist organizations to enhance resiliency and proactively avoid recovery situations.

Additionally, organizations can achieve continuous availability even in the face of an unplanned outage by running “active-active” data centers, whereby two data centers can service business-critical applications, and databases, storage and security policies are synced in both facilities. If a server at a colocation site in the Atlanta data center goes down, failover to a backup server at a data center facility in Chattanooga can take over almost instantaneously.

In an upcoming article, we’ll explore the essential elements of IT Resilience in both broader and more granular detail. We’ll also examine how DC BLOX leverages its colocation facilities, intelligent high-speed network, Cloud Storage and Cloud Ramp solutions to fortify IT Resilience, enabling our customers to effectively ride through an adverse event and carry on with their businesses.



The Essential Elements of IT Resilience

In a previous article we examined organizations' need to evolve from Disaster Recovery (DR) and Business Continuity (BC) models to a strategy of IT Resilience. As discussed, while DR and BC solutions are inherently reactive responses to unplanned outages, IT Resilience is preventative and proactive, and designed and executed for businesses to be able to ride through an unplanned outage or adverse event.

Today, we'll explore IT Resilience in more detail. We'll also examine how DC BLOX leverages its colocation facilities, intelligent high-speed network, and Cloud Storage and Cloud Ramp Solutions to enable customers to maintain acceptable levels of service, regardless of what challenges may occur.

Geographically-Distributed Data Centers: The Cornerstone of IT Resilience

IT Resiliency and high availability go hand in hand. End users, including your customers, partners and staff care little about the resiliency of your systems — whether theoretical, tested or proven under fire. They are only concerned with the availability of their data, app, service or transaction. Can you answer in the affirmative that faced with an unplanned outage or adverse event, they will still work?

Traditionally, we conceive of Disaster Recovery and Business Continuity in the data center as founded on the use of redundant components, systems or subsystems. When one component or system fails or experiences an outage, the redundant element takes over seamlessly and continues to support computing services to the end-user base. The same concept extends to the physical facilities. For example, an organization may power its data center with two separate utility feeds from diverse substations so that a backup is available when the first utility feed fails. Additionally, a traditional approach to DR and BC incorporates protective measures such as fire detection and suppression systems, as well as redundant UPS, back-up generators and redundant chillers.

CONTINUED | The Essential Elements of IT Resilience

It's important to recognize that not every data center is equal with respect to these fundamentals. As a Tier III data center operator, DC BLOX incorporates all of these protective elements at its facilities and more.

> *"DC BLOX's data centers are an example of IT Resilience founded on geographically-distributed colocation facilities."*

To achieve higher levels of resilience for mission critical computing platforms and systems, strategically-located, geographically-distributed colocation facilities in a region connected by a high-speed private network enables applications and data to be distributed or replicated across data centers with low-latency synchronization between them. This geo-dispersed data center approach means that in the event of an unplanned outage or system failure at one facility, applications or data will remain available at a site or multiple alternate sites within the footprint.

DC BLOX's data centers are an example of IT Resilience founded on geographically-distributed colocation facilities. With more than 100 miles between data center locations, they meet an essential best practice that includes geographic diversity as a bulwark against potential natural or manmade disasters and unplanned outages. If something happens in one location, an organizations' data and applications are secure in an alternate location. The key enabler is DC BLOX's high-speed network whose performance allows the application to replicate great quantities of data over a large geographic area. We'll discuss the importance of our resilient network in greater depth later.

While DC BLOX data centers are far enough from each other to avoid a common impact such as a power outage or tornado, they are also close enough that IT staff can easily

CONTINUED | The Essential Elements of IT Resilience

travel to each location for equipment installation and updates. DC BLOX data centers can also support remote infrastructure from an enterprise-owned data center.

How Much IT Resilience, Where and Why?

After gathering data from a Business Impact Analysis (BIA), DC BLOX recommends that CIOs, COOs, and Chief Information Security Officers (CISOs) consider their organization's business objectives and the criticality of an immediate or near-immediate resumption of operations in relation to the continued viability of their business. Financial institutions, healthcare organizations, and government public safety agencies engaged in time-sensitive computing activities are just a few of the types of entities that would experience even a few hours of downtime as completely unacceptable as compared to other environments.

For this reason, the IT Resilience strategies employed in a data center will vary with the importance of the respective workloads or application availability. Organizations with mission-critical workloads will utilize more resiliency techniques at greater levels within the data center because the cost of not preserving critical computing services is more expensive or debilitating than the fallout of an unplanned outage. Conversely, nonessential workloads that can tolerate some level of disruption may receive less resiliency or simply remain offline until they can be restored.

Essential business services such as transaction processing software or database systems may require more comprehensive data center and IT Resilience measures, including clustering, snapshots, virtualization and container movement.

> *"DC BLOX's network is resilient itself, and its high-speed connectivity allows an application to replicate great quantities of data across facilities."*

CONTINUED | The Essential Elements of IT Resilience

The caveat in all of this is to carefully determine which systems, services and applications are mission-critical to business viability and which are less essential. At first glance, an organization may consider a business function as simple as email to be non-essential. However, if the staff of an eCommerce business or even a B2B firm was unable to communicate with its customers or partners for an extended period of time, the results could prove dire.

High-Speed Network Connectivity Is Essential to Resilience

Now that we've explored IT Resilience in the data center, let's examine the importance of high-speed network connectivity linking an organization's data centers. DC BLOX's network is resilient itself, and its high-speed connectivity allows an application to replicate great quantities of data across facilities.

DC BLOX's meshed fiber optic network infrastructure has the capacity to deliver 8.8 terabits per second (Tbps). This capacity provides customers at our data centers with fast, low-latency connectivity with geo-redundant paths. Providing carrier class network service, average latency between DC BLOX's Atlanta data center and the ATL1 Internet Exchange at 56 Marietta Street is 0.103 milliseconds, while Atlanta to its Chattanooga facility is only 1.71 milliseconds.

Why is fast, low-latency connectivity so important to resilience? Because you need to continuously replicate or synchronize data in real-time across data center locations, so that in the face of an unplanned outage or service disruption at one data center site you can quickly access applications and data at the other facility in order to maintain operations.

From DC BLOX's perspective, there are at least three components that comprise a resilient network.

- IT resilience at the network level requires adequate performance to ensure that there is enough capacity to avoid network

CONTINUED | The Essential Elements of IT Resilience

bottlenecks. Optical transceivers of 100Gbit/s are now common in enterprise networks, driven by a combination of internet traffic, online commerce, streaming video, social networking and the increased use of cloud and SaaS platforms. DC BLOX uses multiple 100Gbit/s connections from its Atlanta and Chattanooga data centers to the facility at 56 Marietta Street. Our network is intelligent and capable of managing and orchestrating the large volumes of data that pass through our facilities every second.

- It's also important to monitor WAN bandwidth consumption. A key component of DC BLOX's approach to IT Resilience is that our software-defined network allows network routes to be established and modified as network traffic patterns require.
- Lastly, a resilient network requires redundancy. The DC BLOX wholly owned fiber network uses Ciena's converged packet optical and packet networking products to provide fully protected and redundant routes with unprecedented scale and performance. In the event that one network route is compromised, traffic will automatically be rerouted over different network connections. Ciena's 6500 and 8700 platforms add greater network automation, control and service delivery for customers in the Southeastern United States.

The Cloud and IT Resiliency

The cloud offers both a preventative and proactive means for riding through an unplanned outage or adverse event. Customers can access our Cloud Storage Solution to backup and archive data in any DC BLOX data center directly from their business premises or from a colocation space. Additional copies of the data can be replicated to another DC BLOX data center over our high-speed, private network for enhanced data protection through geographical diversity. Beyond reducing the cost and complexity of managing storage infrastructure, our Cloud Storage Solution eliminates the need to modify applications because we support standard file system interfaces. So, when a data storage component of a company's IT infrastructure fails, backed-up data stored in DC BLOX's Cloud Storage solution can be easily mounted to resume normal operation.

CONTINUED | The Essential Elements of IT Resilience

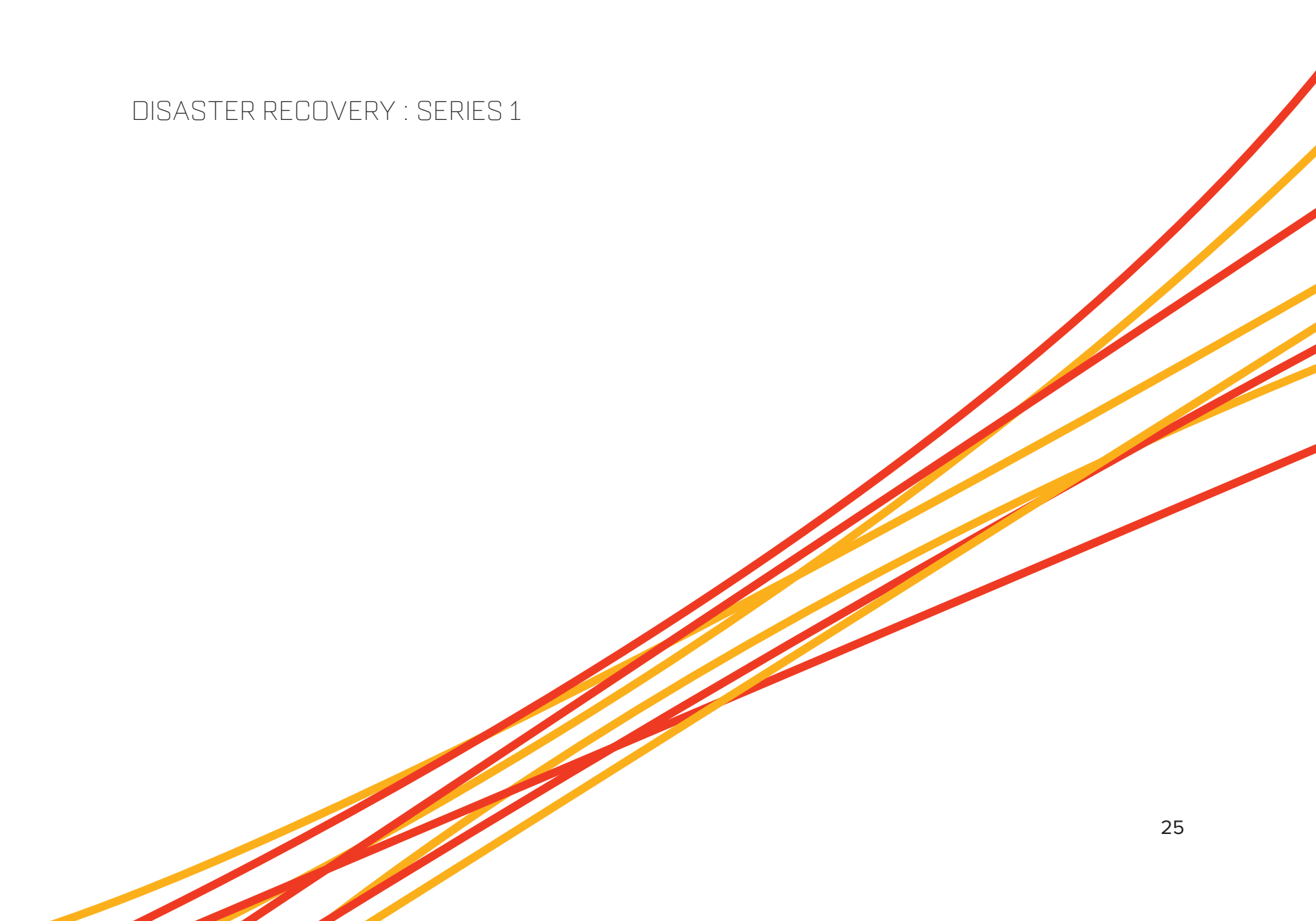
Many companies increase their IT resilience by leveraging public cloud providers to provide redundant on-demand compute or storage resources in the event that their primary systems become unavailable. They may even only use the cloud for certain critical components of their infrastructure. These hybrid IT environments require high-speed private network connections to ensure continuous communications during normal operations and disaster situations. DC BLOX's Cloud Ramp facilitates hybrid IT environments where some infrastructure runs in a DC BLOX data center while connecting to additional compute or data storage resources in a public cloud provider.

Let's Step Back and Look at the Big Picture

You've built redundancy into your servers and storage arrays. You've placed them in a DC BLOX data center that has redundant power, cooling and network connections. The data center itself can be redundant with another data center less than 100 miles away that contains replicated or synchronized data. And the high-speed network that facilitates data center-to-data center communications has built-in resilience through redundant connections and dynamic routing. This is a practical approach to increasing your company's IT resilience!

By now, we trust it's apparent that developing an IT Resilience strategy is neither a siloed nor one-size-fits-all exercise, but a holistic methodology integrating technology, sound decision-making, and a proactive and preventative mindset that prepares for the unexpected.

The stakes are high — the success and long-term viability of your business – and DC BLOX is here to assist you.



ATLANTA
6 West Druid Hills Dr., NE
Atlanta, GA 30329

HUNTSVILLE
333 Diamond Drive NW
Huntsville, AL 35806

CHATTANOOGA
807 East 16th Street
Chattanooga, TN 37408

BIRMINGHAM
6th Street South
Birmingham, AL 35233

DCBLOX.com