10 CRITICAL QUESTIONS TO ASK YOUR DISASTER RECOVERY PROVIDER

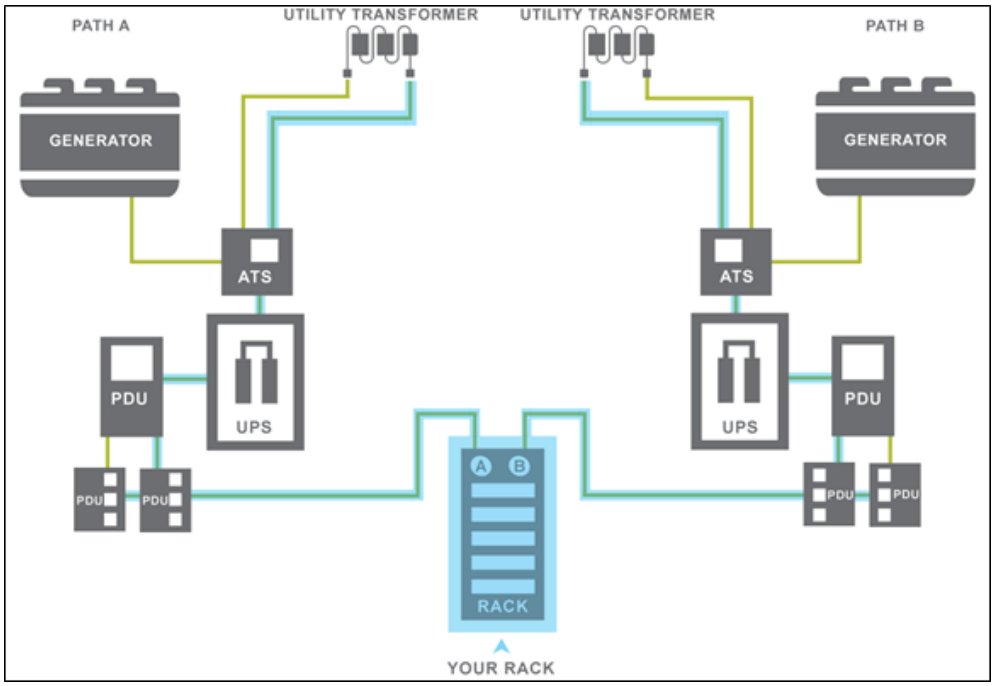
onramp

TOP 10 CRITICAL QUESTIONS TO ASK YOUR DISASTER RECOVERY PROVIDER

Whether you're moving your IT infrastructure to a disaster recovery provider for the first time or looking to switch to a new provider, finding the right partner to keep your operations running 24/7/365 is a critical piece of the puzzle. A disaster recovery partner offers you benefits like lower operational and personnel costs, increased reliability, better performance and additional resources. This whitepaper guides you through some of the key questions to ask when conducting your search.

1. How redundant is your data center?

The redundancy of a data center's critical systems is a critical factor for ensuring its uptime. And the most important critical system is power. Data centers with the highest levels of redundancy provide at least two totally independent, parallel paths of power all the way from the utility to your racks. We call this a redundant isolated path power architecture (diagram below).



A data center with a redundant isolated path power architecture maintains redundant sets of equipment that deliver reliable, protected and conditioned power along an isolated path from the utility to the data center rack. Each path has dedicated equipment including emergency power generation, independent fuel storage, uninterruptible power systems and power distribution systems, all of which remain isolated from equipment along other paths. Using this model, if anything were to happen with any individual piece of equipment, it would affect only one single path.

However, most data centers electrical systems fall short of truly redundant power availability. Some data centers will claim to operate in a redundant way, but are in fact using paralleling technology in their critical subsystems. In a paralleled system, the uninterruptible power supply (UPS) and generators are connected together so that the load can be shifted back and forth, to equalize stress, in the event of a failure in a single device. The problem with this system is that it introduces complexity, which could ultimately harm the whole system. For example, in the event of a lightning strike, the disruption can cascade across the entire infrastructure, bringing down the entire power system.

Additionally, truly redundant data centers operate only online UPS systems. "Online" means that the computers protected by the UPS are always powered directly by the UPS, which offers a more stable method of power conditioning and delivery. A very redundant version of online UPS system is a double conversion online UPS system.

A double conversion means that the utility power, which is alternating current (AC), is "rectified" into direct current (DC) and then is "inverted" back to AC power. By going from AC to DC and back to AC, the power has been put through a double conversion. This double conversion means that the output power of the UPS system is completely clean, computer grade power that has been generated inside the data center.

Many data centers often run an "offline" or "line interactive" UPS system, which means that during normal operation, they really aren't powering the computers connected to them. During normal operation, an offline or line interactive UPS system only protects against extreme surges or failures of power. Many distortions not in these extreme ranges, including damaging "harmonics," are allowed to get through to the computers. Harmonics are transient radio signals that are generated by the noise of solar interference or motors using the same power lines and are proven to shorten the life of computers and interrupt their operation.

Data center redundancy should also be built into the telecommunications infrastructure. The data center should have a minimum of two internet backbones, each with individual, redundant connections. For

more information about data center connectivity, please reference question #4.

2. How secure is your data center?

A data center should employ comprehensive security measures, from the physical environment outside of the facility to the details on the inside—like individual cameras in the data room and locked cages.

A. Location and Structure. The data center should be constructed in a low traffic, non-descript setting, set far off any major road or highway, but still be easily accessible. Review the physical location of the building to ensure that it is in a geographically stable location with stable weather patterns, far from any natural environmental dangers such as floodplains, landslides and seismic faults. Hurricanes and tornadoes can dramatically impact the facility and the utilities and services around the facility. High winds, random acts of violence and other natural disasters can have an impact on the facility, so make sure there are no outward facing windows from the data center rooms. All critical outside critical systems should be fenced off and monitored.

B. Physical Security Systems. All entrances and externally located critical equipment should be alarmed, caged and surveilled by cameras that feed into the network operations center (NOC), which should be manned 24/7/365. All doors should require dual factor authentication for entrance. All rooms and equipment inside the data center should be monitored 24/7 by cameras that feed images to monitors in the NOC. Recordings of these images should be stored for no less than 90 days and accessible on-demand. Each rack or cage should have individual locks, and those keys maintained in a separate, lockable location accessible only by authorized data center personnel. Advanced systems should be in place to continuously report the status of the electrical and mechanical infrastructure to the NOC staff. The following is a suggested list of items to ask the data center provider if, and how, they are monitored:

• Intrusion	• Temperature / Humidity
• Fire	• Breaker trips
• AC power failure	• Leak detection
• Generator failure	• UPS failure

C. Logical Security Systems. Data centers that undergo a SSAE 16 SOC 2 Type II and SOC 3 audit will have controls over information technology and related processes, policies and procedures, including operational activities that validate performance at optimal standards regarding security, availability and operating integrity. The SSAE 16 SOC 2 Type II standards dictate certain procedures that a data center

must adhere to with regard to authenticating customer access requests as well as procedures for controlling hard drives or tapes in the event that they are damaged, necessitating their removal from the customer's environment.

***D. Creating a Culture of Security through Systems and Processes*.** A critical component of a truly secure facility is the creation of a culture that emphasizes and embodies the ideals of security. When selecting a data center partner, pay special attention to the measures taken by the data center personnel to authenticate visitors to the facility by key card, biometric access systems or a combination of both. Only authorized visitors should be granted access to their own, dedicated equipment in the facility after surrendering a government-issued ID to the onsite personnel. Phone based authentication is also critically important. You need to feel safe that you are working with a partner who values your security and has built the systems and processes for ensuring it. External audits are one way to measure the ongoing effectiveness of a data center's security policies and procedures. All security systems should be monitored 24/7 and activities logged according to stringent controls and audited by a third party. These third-party auditors will issue opinions on whether or not that data center has met the standard of security. The highest is SSAE16 SOC 2 Type II and SOC 3. You need to ensure that you are working with a partner who has met these standards.

3. What certifications and audits does your data center have?

A data center must have controls in place that comply with industry recognized standards. Standard audits and certifications for data centers include: SSAE 16, PCI (payment card industry) HIPAA (Health Insurance Portability and Accountability Act for protection of sensitive electronic protected health information), SOX, FISMA, FERPA, GLBA and FACTA.

Data centers that host systems relevant to their customers' financial reporting are responsible for certain controls over those systems, such as physical and environmental security. The Statement on Standards for Attestation Engagements no. 16 (SSAE 16) is the new "attest" standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants. A SSAE 16 SOC 2 Type II audit is widely recognized because it represents that a service or outsourcing organization has been through an in-depth audit of their control activities. This audit generally includes controls over information technology and related processes, policies and procedures, including operational activities and validates everything is performing at optimal standards regarding security, availability and operating integrity. Internet service providers must demonstrate that they have adequate controls and safeguards when they

host or process data belonging to their customers. A third party that conducts a SSAE 16 audit reviews numerous processes and controls related to:

- Logical and Physical Access
- Security of Environment and Information
- Backup/Recovery
- Secure Storage

The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, ATM and POS cards. The standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Because data centers provide facilities for companies and merchants to house servers as they conduct their business, the data center provider has specific responsibilities that must follow PCI compliance. A merchant or company that is located within a PCI compliant data center is not automatically PCI compliant. Each merchant or company claiming PCI compliance must have and be able to provide their own attestation of compliance, detailing their sensitive information procedures as they follow the PCI standard. A data center provider that claims to be PCI compliant should be able to assist in accomplishing PCI-DSS requirements 1 through 12, thus assisting customers in passing the PCI audit and responding to security alerts. Working with each customer data center providers can ensure a safe, compliant and successful hosting experience.

Companies that deal with sensitive patient data are required by law to secure that data in accordance with HIPAA rules and regulations. HIPAA compliance rules apply to both Covered Entities (any healthcare provider, health plan or health care clearinghouse) and Business Associates (any company that comes in contact with electronic protected health information [e-PHI]). Whenever a data center's services are used by healthcare companies or their Business Associates, that data center is required to enter into a cooperative relationship to ensure that the appropriate measures are taken to protect the availability, integrity and confidentiality of the customer's sensitive patient data. Few data centers will sign business associates agreements due to the liability risks associated with a security breach. A data center that claims it is HIPAA compliant must have certain administrative, physical and technical safeguards ensuring HIPAA data security in place.

4. How connected is your data center?

The connectedness of a data center is an important indicator of the reliability of its network and the flexibility you will have as a customer to find a network solution that works best for your business needs.

A data center should provide bandwidth from multiple tier-1 backbone providers. While bandwidth built on two of these provider backbones is acceptable, bandwidth built on three such backbones is truly enterprise class. This bandwidth should be multi-homes and the data center should employ specific routing technologies that optimize and route traffic in a way that ensures network speed and ongoing connectivity. At the core layer, Border Gateway Protocol version 4 (BGP4) is the industry standard routing technology to automatically route traffic most optimally. By having multiple backbones and using BGP4 to decide how to send traffic to those backbones, the data center is making internet access much more reliable. If either backbone or any router fails, the network automatically routes traffic around the interruption. During normal operation, the routing protocols ensure that packets are routed along the best path across the Internet on a route by route basis.

A well-connected data center's network should be built on best-in-class, enterprise equipment, incorporating a core, an aggregation and an edge layer, deployed in a full mesh for the utmost redundancy. The core of the network is comprised of a series of routers that connect directly to major internet backbones. Each of the connections should be fiber-based Gigabit Ethernet lines, capable of transmitting 1 Gigabit per second (Gbps) or 1 billion bits per second. The backbone connections should connect to their own backbone using SONET rings, which are miles long strands of fiber laid in a ring fashion so that if the fiber is cut in any place, traffic can automatically re-route around the other direction to the ring.

At the Edge layer, a data center should be able to provide a dual drop to connect customers using Hot Standby Router Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP) routing technologies to provide fault tolerance from the facility's networking equipment to the rack. A dual drop adds an additional layer of redundancy from the customer's rack to the Edge layer. While most customers will use a "single" drop or a single wire to connect the Edge layer, those that cannot risk the possibility of an outage, due to a failed switch/router will request a dual drop. With a dual drop, the data center adds another protocol or language into the customer connection to mediate the interaction of the two drops.

A well connected data center should also offer you options to connect directly, with the telecom provider of your choosing, for point to point or private connections. In order to provide the most possible selection, (and the most efficient market for you as a consumer of telecom services), a data center should have many different options. Enterprise class data centers have over 10 fiber providers in their facilities. However, in reality, as long as there is an ILEC (Incumbent Local Exchange Provider) in the facility, you can connect across that ILEC's network to a wide variety of providers.

Finally, it is important to ensure that you have the flexibility to start small, with room to scale as you grow. Before you sign any contracts, make sure the data center provider can accommodate the installation of additional equipment and networking capacity, on demand. Does the data center have the flexibility, in their contract terms, the design of their facility, and the responsiveness of their support group to accommodate that need quickly and effectively? How do they handle overage charges? It is important to be working with a data center partner that is truly flexible in their approach to best supporting your business' telecom needs as you scale and grow.

5. What level of support does your data center provide?

Make sure that your data center's NOC is staffed 24/7/365 by onsite engineers that can actually provide hands-on help in the event of a problem or emergency. While you might not foresee the need for help inside your rack, consider the benefits that an experienced network engineer can provide in the way of remote hands when you need a server reboot or technical support above the hardware layer at 3AM.

While most data center companies like to talk about support, they actually provide very little in the way of real, hands-on help. A data center that is strictly a "ping, power and pipe" facility may not even touch your equipment regardless of the situation. And, if a data center says they can help you in the event of a problem, ask them to define their meaning of "help." Do they provide server reboots or can they go deeper? Do they stop at the network layer or can they provide help all the way through layer 7, also known as the application layer, of the Open Systems Interconnection (OSI) Stack? Who staffs their data center after hours: a security guard or onsite engineers? Consider the travel time it will take for you or your team to make a special trip to your data center in the event of an emergency. Can you afford downtime in the event of a hardware failure? Ask your data center how trouble tickets are handled, how problems are escalated and what staff members are on-call both during and after business hours. Is everything automated or do actual human beings answer the phones, respond to tickets and troubleshoot problems in your rack?

A data center that boasts about its support department should be able to back it up with technicians that are experienced, onsite and available by e-mail and phone in the event of any problem 24/7/365. Moreover, they should have the certifications and technical expertise to help you where you will need it most: inside your rack.

Also, data center that operates all the way through layer 7 of the OSI Stack provides several unique advantages, even if a customer doesn't foresee a need for support. To begin with, a data center that is

capable of application layer support will have the deep experience in application development to be able to diagnose, troubleshoot and remedy problems at the application layer. In most cases, data centers that offer this level of support will have an onsite development team skilled at developing front and back-end application functionality giving them the distinct advantage of speaking the same language as their data center customers. As such, they will have the necessary tools and resources onsite for their customers to be successful. A data center that is engaged with each layer of the OSI Stack can supplement a customer's capabilities, whether something is tangential to their knowledge or they need immediate onsite support.

6. What, if any, supplementary services does your data center provide?

Ask your data center provider if they can provide managed hosting services and/or managed security services, in addition to colocation. A data center that only provides colocation services may lack the flexibility to meet the rising demands of many companies. Managed servers are single or multiple server installations with dedicated power and bandwidth, hosted within the data center. Managed servers are best suited to customers who would prefer that the data center own, operate and monitor the equipment on which their applications are running. If a data center can provide both colocation and managed hosting, they should have the ability to augment a customer's hardware infrastructure with resources on-demand. This hybrid hosting solution enables significant flexibility to grow and scale of resources. When a layer of virtualization is added to a managed hosting configuration, the customer can reap the benefits of cloud computing in what is known as a private cloud. In today's world of cloud computing, the ability to scale and provision services on-demand is a critical component to growing your business.

In addition to managed hosting options, ask the data center provider if they can support other managed services including managed storage, managed backups and managed devices. If you require a great deal of data storage, can the data center support you with a storage area network (SAN)? Some data centers will offer "managed storage" or SAN disk space by the Gigabyte (GB) where disk space is accessible either across a dedicated Ethernet network using a technology called ISCSI or using a dedicated fiber connection. In this arrangement, the customer is charged a set fee for each server connection to the SAN and charged per GB of storage used.

It is standard practice to regularly make backup copies of data and to store those copies offsite to protect against the case where a physical disaster destroys the only copy of data. Inquire as to whether the data center provider can help customers accomplish backup needs, including encrypted backups for compliance. All of the backup tapes should be stored offsite in a protected environment. If a data center

provides backup services, how are they deployed and what is the fee structure? Overall, you are more likely to be successful if you have the flexibility of many supplementary services at your fingertips.

7. Does your data center help with compliance, such as HIPAA and PCI? If yes, at what level?

If your business interacts with sensitive customer data, whether that is financial, or health related, or any other kind of sensitive data, it is important that your data center can help with ensuring your business is compliant with rigorous and consequential compliance standards. Two such standards are HIPAA and PCI. Many data centers will tout that they are HIPAA and/or PCI compliant, but few truly have the competency, capabilities and compliance standards in place to ensure that your critical data meets the security and regulatory standards defined by law.

There are 12 PCI-DSS requirements for compliance and a data center that boasts PCI compliance should be able to help customers configure their network to accomplish requirements.

Similarly, if a data center is truly your partner in HIPAA compliance, they will work with you to build a comprehensive, fully-compliant solution that addresses the confidentiality, the availability and the integrity of e-PHI. Ask the data center provider if they can help with a risk assessment to diagnose, assess and manage any threats, vulnerabilities and risks to your IT infrastructure and then work with you to design and implement systems and applications to meet HIPAA's privacy and security standards and related administrative, technical and physical safeguards.

And ask whether the data center will sign a Business Associates Agreement (BAA), the agreement between a covered entity and a business associate or between two business associates that clearly defines the roles and responsibilities of each of the parties to the agreement regarding the protection of e-PHI. Covered entities are required to execute a BAA with anyone who may come into contact with e-PHI that is not directly employed by the covered entity and who does not otherwise have the right to access the e-PHI in accordance with the HIPAA Privacy Rule. In addition, anyone who is a BA is required by HIPAA to execute a BAA with anyone else that might come into contact with the e-PHI due to their relationship with the BA.

8. What level of support can you provide for disaster recovery and business continuity?

A data center partner that is a disaster recovery site should have the highest levels of security, redundancy, reliability and infrastructure necessary to house your servers. But it is also critical that your disaster recovery partner be able to support you remotely. After all, by definition your disaster recovery site will be located remotely from your business operations. It is important to make sure that your disaster recovery site has experienced personnel onsite to facilitate the installation, monitoring and maintenance of your equipment. It is also important to make sure they can provide remote hands for customers that aren't able to travel and require immediate assistance to maintain online operations. And if travel can't be avoided, your disaster recovery site should provide dedicated workspaces, seats and conference rooms.

A data center partner for disaster recovery should also work with you to help identify your recovery time objective (RTO) and recovery point objective (RPO). RTO is the maximum length of time that a system can be down after a failure or disaster occurs before the company is negatively impacted by the downtime. RPO specifies a point in time that data must be recovered and backed up. The RPO determines the minimum frequency and at which intervals backups need to occur, whether every hour or every 5 minutes.

Cloud-based disaster recovery is a good choice for companies that need a secondary infrastructure where they can spin up resources on-demand or replicate their data in the event that they need to failover to the disaster recovery site in an emergency. When the emergency is over, operations can failback to the primary site. As referenced earlier, information that resides in a cloud environment should ideally be stored on dedicated equipment, devoted solely to the use of one customer.

9. What kinds of resources and tools are available to help me be successful as a customer?

Whether or not you plan on making regular trips to your data center, it is best practice to find out what tools and resources the data center makes available to customers and whether these tools are accessible and available for use 24/7/365. Most data centers require customers to bring everything they need to work in their server cabinet or rack. But a true data center partner should have many of these tools and resources onsite.

Emergencies rarely happen during regular business hours. If you experience a hardware failure or server emergency at 3AM, consider the feasibility for you or your IT manager to drive to your data center and troubleshoot the problem. As a data center customer, you are more likely to be successful choosing a data center whose technical staff have deep experience at every layer of the OSI stack, regularly work on server and networking hardware and have the ability to assist you on-demand. A top tier facility that has an onsite, experienced technical support staff, will not only have a complete supply of tools, on-hand, for customer use, but they will also have staging areas, diagnostic equipment, office space and conference areas enabling you to host a meeting or just take a break. Moreover, the data center should have spare servers, hardware and software available for customer use in the event of a failure or other emergency. Below is a checklist of resources that a data center should have on-hand for customer use:

- Spare servers
- Spare software media from Microsoft/Redhat/VMware/Citrix
- Spare firewalls
- Spare content switches
- Spare routers
- Spare KVM switches
- Spare Ethernet wire
- Spare caged nuts
- Spare cable ties
- Tools
- Cable testers

10. Have other customers been successful in partnering with your data center?

Learning how other customers have been successful in partnering with the data center is of critical importance when choosing a data center partner. Is the provider implementing new facility design elements and integrating technologies that increase power and cooling capacities to support higher density rack configurations? Determine whether the data center environment can provision flexible solutions, on-demand. What is the average tenure of the data center's customer base? How can the data center accommodate current and new customer growth? What is the average customer size or footprint? Customer references and case studies are a strong indication of how the data center goes about solving unique challenges and delivers on what was promised. Have a list of questions to ask the data center's references.

About OnRamp

OnRamp was founded in 1994 in Austin, Texas. As one of Texas' first Internet operations companies, its history is rooted in providing reliable and secure connectivity that enables distributed computing. Today, OnRamp is a data center operations company that delivers a comprehensive suite of services.

As an SSAE 16 SOC 2 Type 2 and SOC 3, PCI-DSS certified and HIPAA compliant company, OnRamp operates multiple enterprise-class data centers in Austin and Raleigh, N.C., to deploy hybrid solutions built on cloud-delivered computing capacity, managed hosting, disaster recovery and colocation services. OnRamp specializes in working with companies with high security needs, helping them meet the rigorous compliance requirements associated with HIPAA, PCI, SOX, FISMA and FERPA.

For more information: www.onr.com | 888.667.2660