White paper

Disaster recovery

5 questions to ask your managed services provider

October 2017

Introduction

Let's say a malicious hacker has gained control of your IT system and launched a ransomware attack, demanding an enormous payment within 24 hours.

All IT operations at your enterprise are completely shut down, as you prepare to respond. You are losing valuable data with each tick of the clock.

This is where your disaster recovery planning and preparation is seriously challenged.

Ideally, you have:

- Prepared a disaster recovery plan of action that kicks in immediately and accurately assesses the risks and costs of the downtime
- Designed a disaster recovery solution that recovers data to the cloud or to an on-premises data center (or both), and emphasizes business needs and priorities
- Established well-thought-out Recovery Time and Recovery Point Objectives (RTO/RPO) for all your IT assets, using an agreed upon rating system (e.g., Mission Critical, Operation Critical, Not Critical)
- Tested your disaster recovery solution and crisis communications plan
- Taken advantage of other, non-disaster uses for disaster recovery (see below)
- In the end, experienced minimal downtime, avoided the loss of any crucial data or revenue, and best of all, avoided paying a ransom of any kind

If this scenario represents your current situation regarding disaster recovery, congratulations. You deserve a bonus or reward of some kind.

But many, if not most, of you will not be so fortunate. Your disaster recovery plan needs work or is a non-starter at this time.

We'd like to say there's time to get it ready, but we can't. No one can predict when the next attack or disaster will occur. In fact, a sudden, unexplained power outage that lasts only a few hours and is not weather-related could prove to be devastating as well.

However, a serious discussion with your managed services provider (MSP) can at least help get you on the way. Here are things you will want to talk about with your MSP.

Question 1

So, why should I be meeting with you, an MSP, about disaster recovery?

Let’s discuss this. You want a disaster recovery (or cloud-based DRaaS) solution that is strategic, holistic, and in the best interests of your business. In today’s "do more with less" IT world, it is likely that a managed services provider is better positioned — than your own in-house IT staff — to give your business the full range of disaster recovery services and ROI it deserves and needs.

"The paradox is that to deliver on a more strategic outlook, IT leaders can no longer rely entirely upon internal resources," says Jeffrey Bannister, Executive Vice President of Global Enterprise Services for NTT America, in a July 2017 article he wrote for CIO.com.[1] "Achieving the right outcomes depends less on making up-front investments than on forging relationships with external partners who can deliver."

Bannister does note that IT departments must still retain "overall responsibility for the data and information that may constitute a corporation’s most valuable asset."

An MSP is also more likely to provide the end-to-end services involved with successfully integrating disaster recovery (DR) into your IT infrastructure. These include managing and monitoring the DR performance, and performing other related tasks, so that you, the client, can focus on the more strategic aspects of your business.

Disaster recovery solutions are not add-on or standalone tools, though they are frequently thought of as such, even by IT pros looking for a way to plug them in. Instead, they are important features of a broader platform, and must work well with your other IT components (cloud and/or on-premises). Your MSP is well-positioned to assess this, as well as factor in your specific RTOs and RPOs — and help you achieve these targets (more on this below).

The design, implementation, and testing processes for your DR solution are delicate but critical processes. Yes, you do want to test your system in advance. A strong understanding of the software tools and processes involved is a must to avoid unforeseen problems in testing.

Beyond this expertise, an MSP is also well equipped to:

- Supervise your entire IT environment and know what on-premises or cloud-hosted solutions might make your disaster recovery investment bring more value for the future
- Provide 24x7 access to highly trained and certified support technicians, as well as cutting-edge tools
- Offer global service coverage
- Apply expertise and experience to accurately budget for your project
- Give you peace of mind as well as time for your in-house IT team to focus on more strategic projects affecting business outcomes

Question 2

What is the best way to integrate disaster recovery into my company's IT environment, even with my legacy infrastructure?

Your IT environment and how it operates to serve your enterprise is unique. An MSP will seek to develop a broader business continuity management strategy that will guide how your disaster recovery solution is designed and implemented.

To do this, an MSP will ask you a series of questions. Here are some examples:

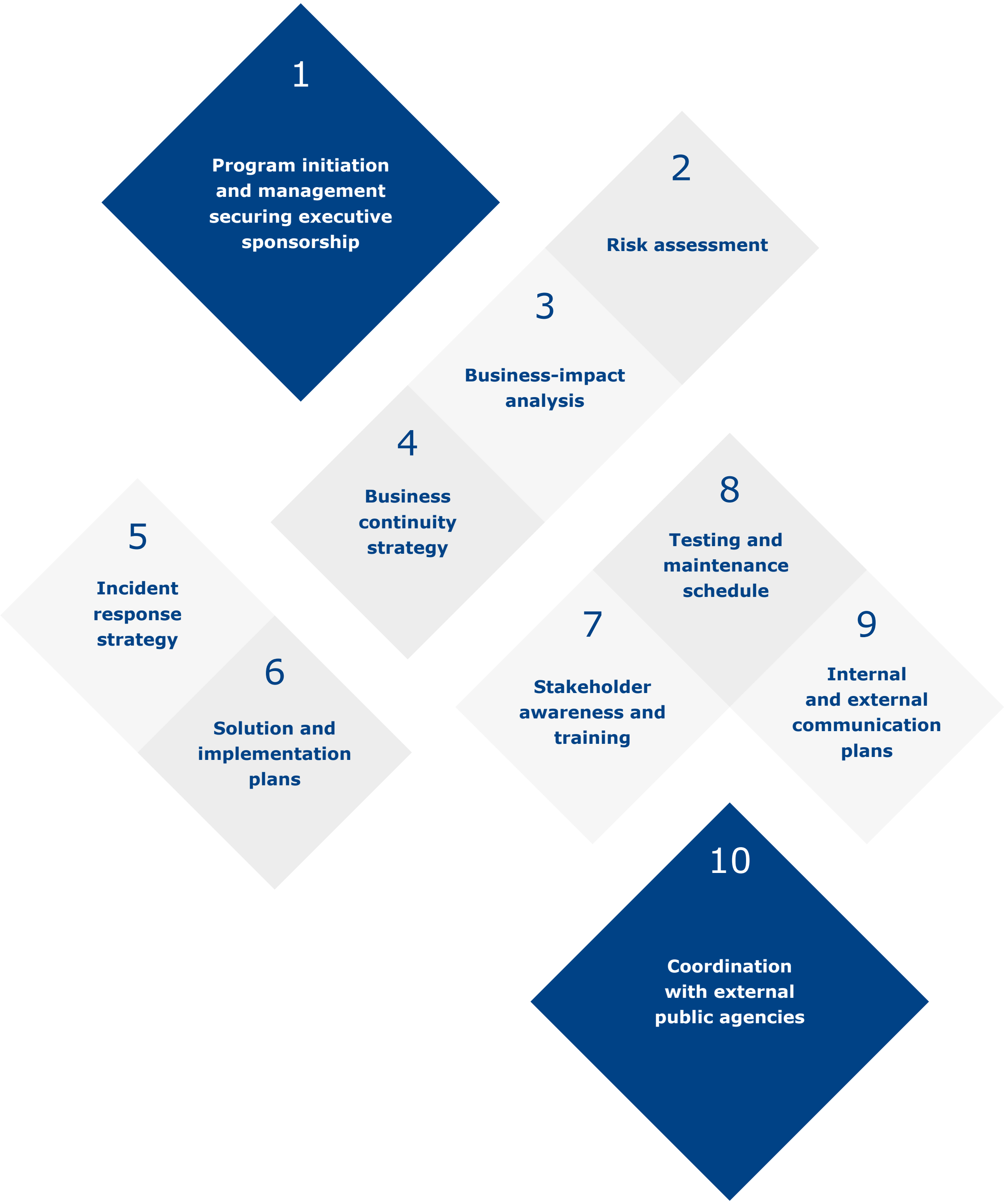
1. What are your RTOs and RPOs and what system was used to establish these targets — i.e., the levels of downtime your business could withstand? (Is it hours or minutes)?
2. How will your manufacturing operations be affected in a disaster?
3. How will your supply chain operations be affected?
4. Could you evaluate all your cyber and non-cyber threat considerations?
5. Can you utilize insurance as a risk-transfer tool?
6. What other risk-management concepts are in place?
7. How will any legal and regulatory concerns be addressed?
8. Can you leverage performance and cost savings with the latest advances in technology and cloud services?

Here are other considerations for you, as a client, in discussing specific disaster recovery services:

- Physical location of services
- Your MSP's network capabilities, security capabilities, and cloud options
- Achievable RTO/RPO targets
- Testing services and processes
- Delivery model — in-house vs. managed services
- Disaster recovery tools and reporting features available
- Platform interoperability — moving from another MSP or DRaaS solution can be difficult, but an MSP is your best bet to do so

From here, your MSP will develop a staged design approach.

Elements of Staged Design Approach[2]



1 Program initiation and management securing executive sponsorship

2 Risk assessment

3 Business-impact analysis

4 Business continuity strategy

5 Incident response strategy

6 Solution and implementation plans

7 Stakeholder awareness and training

8 Testing and maintenance schedule

9 Internal and external communication plans

10 Coordination with external public agencies

Having an MSP that offers flexible disaster recovery replication options is ideal. For example, NTT is partnering with Microsoft to offer NTT DRaaS with Microsoft Azure, which replicates to the Azure cloud, to another data center, or both, depending on your IT environment.

When a U.S. government agency (with an operating budget of more than $100 million) sought to upgrade its in-house disaster recovery solution and processes, it strictly needed a disaster recovery solution from an MSP: NTT Communications. The government agency's top priorities were to automate processes while increasing security and the restriction and isolation of data from other applications and third-party personnel.

In working closely with the agency's IT staff, NTT provided a solution that accomplished that, including:

- Automating failover and 24/7 management and monitoring services, which previously had been multiple, extensive manual tasks — saving time and eliminating security and performance risks
- Enabling users to interact with the replication services and schedule operations directly from the management portal
- Helping the agency in an additional, unexpected way: NTT's disaster recovery solution is now being used as a fast, secure file-transfer service between operations on East and West coasts[3]

Question 3

What are my RTO / ROP needs and objectives, and how best can I determine them?

Helping clients meet their Recovery Time and Recovery Point Objectives is the essence of a disaster recovery solution. What is the business impact if you have downtime? What is an acceptable amount of lost data? How long can you withstand the loss of data — a few hours? A few minutes?

"Clients understanding these metrics will lead a provider to the right conversations," says George Rigby, Senior Solutions Director for NTT's managed services.

Here are the definitions:

- **Recovery Time Objective (RTO)**. This is a service-level agreement (SLA) setting the maximum time that an application will be unavailable in a downtime situation. The shorter this time period, the faster the recoveries will need to be. Generally, this SLA covers the operating system and configuration data, as well as the application data.
- **Recovery Point Objective (RPO)**. This is an SLA setting the maximum amount of acceptable data loss to occur in a downtime or data loss scenario. Frequent backups or near-continuous replication is required to reduce the amount of data loss.

RTO and RPO are key components of any disaster recovery solution design. As such, **having a clear understanding of how these targets are established** — and making them a true representation of business importance — are crucial. A quality MSP will discuss the options, trade-offs, and factors to help you arrive at this most important determination.

Some common problems:

Enterprises **frequently underestimate their needed recovery time**, which is often realized too late. A common occurrence is a business, to save money, focusing its business continuity efforts on protecting backups of critical data by storing them in an offsite facility. However, they may fail to consider how to recover the data under a variety of scenarios, a costly oversight.

For example, a large geographical area is affected by a major weather event, such as a hurricane. Simply having a copy of the data offsite does not guarantee that you can access the data quickly, acquire the equipment needed to recover the data (tape drives, for example), or restore the data and rebuild application systems fast enough to satisfy the needs of the business. Each of these unknowns must be considered, as they will clearly result in increased downtime and inevitable cost to the business. Understanding the effect of recovery time on the business, and all factors that influence recovery, may prompt you to make different technology and service provider choices.

On the flip side, many other enterprises **set unrealistic recovery objectives**. While it’s understandable that you want a high bar for your recovery goals, it’s important to know that your level of redundancy and ability to recover are directly tied to your budget for recovery services. Many organizations have a false expectation that disaster recovery solutions operate like an insurance plan: maximum replacement at a minimal cost. But this isn’t the case. In general, the more you budget for disaster recovery, the more resilient your applications and data become.

Perhaps as big a mistake as any is having **unclear Recovery Time and Recovery Point Objectives**. Each business application will have a different tolerance for downtime and data loss caused by a disaster. This often reflects the importance of the application to the business. For example, it might be possible to recover data lost from a system that processes supplier invoices by having suppliers resubmit documentation, but data lost from an online customer order system may be gone forever.

Again, RTO measures the amount of downtime the business can withstand during an application outage, without incurring significant loss. This can be measured in minutes for mission-critical applications to hours or even days for secondary applications. RPO measures the business’s tolerance for data loss during application downtime. The aforementioned online customer order system might have an RPO measured in seconds, whereas applications using data that can be easily recreated may have a much longer RPO.

If the business is to avoid losses following a disaster, applications with smaller RTO and RPO must be recovered faster than those with longer RTO and RPO.[4]

Question 4

What value is there in an MSP being cloud-agnostic and vendor-neutral?

Gone are the days when MSPs and other providers of technology services worked largely on the behalf of their technology manufacturer partners, and new offerings were quickly evangelized. Today, the bigger focus is on delivering business outcomes for the client.

The research firm Gartner, in its June 2017 "Magic Quadrant for Disaster Recovery as a Service" report, defines DRaaS as "a service offering that includes replication of server workloads and recovery of such workloads, as needed, to a cloud with which the provider ultimately has fiscal responsibility." As stated in the 2016 iteration of this Magic Quadrant, DRaaS is "now a mainstream offering. In fact, Gartner estimates it to be a $2.02 billion business currently, and it is expected to reach $3.73 billion by 2021."[5] We calculate this as an increase of nearly 85 percent.

If your organization seeks to migrate more workloads to the cloud, implementing a new disaster recovery solution may be an opportune time to upgrade your IT environment. Fortunately, leading cloud providers such as Microsoft Azure have compelling offerings with innovative features. You can't really lose.

But, you need the flexibility to choose new cloud and data center technologies that fit with your existing infrastructure and your budget. That may mean the ability to continue to use a certain cloud platform — say, PaaS and SaaS services from the same IaaS provider you currently use. It may also mean customizing with a mix of cloud offerings and/or on-premises technologies.

A disaster recovery solution, from an MSP with a consultative, vendor-neutral approach, can help you configure a complete business continuity and disaster recovery solution, plus any new cloud services you'd like to integrate, that offer the best business outcomes.

Some additional considerations:

- Service-level commitments, test-recovery schedules and other details involved generally vary per MSP and cloud services provider. You want terms that you can work with.
- Hybrid recovery configurations often require a custom service agreement, especially for the SLA definitions. Again, the terms here are important.
- Integrating a new solution doesn't mean your in-house IT team has completely turned over responsibility and accountability to the MSP or cloud services provider. Internal IT teams still must work with providers to manage recovery assurance, so you want a partner you can work with.
- Managing and predicting your monthly cloud spend in the era of consumption-based IT models can be challenging. This ongoing process involves everything from selecting the right cloud and cloud instance sizes for your applications to being able to understand the various delivery models available from the different major cloud providers.
- Navigating the ever-evolving changes in public cloud capabilities is almost impossible. By working with an MSP with certified engineers and operations professionals in the different cloud platforms, you can optimize costs and IT service management by utilizing new cloud capabilities as soon as they are available.

Question 5

How can a disaster recovery solution help my organization with its digital transformation?

1. Moving data to the cloud for disaster recovery

Replicating your applications and data to the cloud, rather than to another data center, is more efficient and ultimately more cost-effective. You avoid the need to replicate your entire production system in full at a secondary data center, with disaster recovery available on demand in the cloud. Replicated virtual machines can be copied to locations globally, for quicker, more efficient access in the event of a disaster. More significantly, system downtime can be reduced to minutes, as a result. In addition, cloud-based systems enable enterprises to replicate virtual machines to storage in multiple regions, for greater protection and redundancy. (NTT DRaaS with Microsoft Azure enables global service coverage, as well as other benefits of Azure, the world’s fastest-growing cloud platform).

2. Using your disaster recovery environment for sandbox testing

Maintaining a separate test environment can also be expensive, especially when you want to test against full production data. Your DRaaS environment can be used as a sandbox for production testing, since it already contains replicas of your data. Once all the applications are operational, your MSP can perform your regression tests in this sandbox against a fresh copy of your production data. When you’re satisfied with your testing, you can collapse the environment. You only pay for the resources needed while you are doing the test; no need for a huge capital investment in test equipment. Also, your normal data replication can continue during the testing to keep your protection within your desired RTOs and RPOs.

3. Using your disaster recovery environment for upgrades and patches

Scenarios here include your company undergoing a hardware refresh, moving data between infrastructure solutions, or simply upgrading or "patching" your production environment. This has usually meant planned downtime — in the middle of the night or on weekends. However, this has become harder to do, as today's businesses are 24/7 operations, with no tolerance for downtime, planned or not. With your DRaaS solution, you can failover your production environment to your cloud provider and run your production operations from the cloud. Once running in the cloud, an MSP can perform the upgrade or refresh to your production equipment. Next, instead of replicating to the cloud, shift the replication from the cloud to your production data center and perform a "failback."

4. Using your data center environment for security incidents

Yes, disaster recovery can be used as mitigation for a number of security incidents. Not only will you have tools to prevent ransomware or malware attacks via your security strategy, but with DRaaS, you also have a mitigation strategy in case of an attack. By using backups for long-term data storage and a replication solution for real-time changes in the cloud, you can rest assured that during a security incident, you won't lose crucial data or revenue due to extended downtime. In such an event, you just invoke your disaster recovery plan to bring your applications live in the cloud using the most recent, clean copy of your data. When you have cleaned your production systems from the attack, you can replicate your cloud versions back to your data center.[6]

Got more questions? See your managed services provider and be confident you will get answers.

Footnotes

[1] Jeffrey Bannister, "Managed services and strategic outcomes," CIO.com, July 10, 2017

[2] Disaster Recovery Institute International framework

[3] From the NTT case study, "Business Impact Summary: U.S. Government Agency"

[4] NTT white paper, "Top 10 Disaster Recovery Pitfalls," 2017

[5] Gartner, "Magic Quadrant for Disaster Recovery as a Service," Ron Blair, Mark Thomas Jaggers, June 19, 2017

[6] Jeffrey Ton, "Disaster Recovery: It's Not Just for Disasters Anymore," Forbes.com, July 12, 2017

Next steps

NTT Communications' Disaster Recovery as a Service (DRaaS) portfolio, including NTT DRaaS with Microsoft Azure, provides cloud-based services including cloud recovery and cloud backup. These can serve as a key element of a company's overall disaster recovery plan, allowing a business to operate as normal during planned or unplanned outages.

Features include:

- 24x7 fully managed and monitored DRaaS services
- Users can define, configure, and monitor virtually any level of service
- Customizable SLA targets to meet the most stringent DR requirements
- Global support for hybrid configurations
- Full suite of business continuity, disaster recovery and security professional services

NTT's DRaaS offering also includes multiple public and private cloud resource options, all with the goal of delivering each customer the best disaster recovery and business continuity program for their business.

Through NTT's dynamic and scalable hybrid cloud options, top-tier global internet backbone with a private network in more than 196 countries, and one of the largest global data center footprints (140+ data centers), customers can leverage NTT's expansive managed infrastructure capabilities to deploy a robust and secure DRaaS program.

Interested in a free assessment of your disaster recovery environment?
We will provide a free assessment to qualified candidates.

Contact us today to get started.
Dial: 1-888-341-7867
Click: www.us.ntt.com
Email: NTT_America_Team@ntta.com

About NTT Communications

NTT Communications provides consultancy, architecture, security and cloud services to optimize the information and communications technology (ICT) environments of enterprises. These offerings are backed by the company's worldwide infrastructure, including the leading global tier-1 IP network, the SD-WAN Service Portfolio reaching 196 countries/regions, and 140 secure data centers worldwide.

NTT Communications' solutions leverage the global resources of NTT Group affiliate companies to enable digital transformation journey for enterprise clients.

- Comprehensive product and service portfolio spanning data centers, network services, hybrid cloud and pure cloud services
- Offering one-stop enterprise ICT solutions from the NTT portfolio of companies
- Major offices and data centers in key technology locations worldwide for business agility and lowest international latency — including the U.S. West Coast (Silicon Valley) and U.S. East Coast (Northeast Corridor)

NTT's core capabilities:

1. Professional/Advisory Services
2. Managed Services (infrastructure and application level)
3. Data Center and Network Services
4. Collaboration Services
5. *All services governed* by Enterprise Security and Compliance

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.