COGNIZANT 20-20 INSIGHTS

10 Key Considerations for Disaster Recovery Planning

As IT infrastructure evolves from cost center to business enabler and a market differentiator, organizations must, more than ever before, embrace key tenets of disaster recovery planning to safeguard their technology jewels from disasters – both natural and man-made.

Executive Summary

The state of disaster recovery (DR) readiness at most organizations can be summed up in one of the following statements (or a combination of these):

- DR plans are mostly ad hoc.
- DR plans don't meet expectations when executed.
- DR plans are not kept up to date (if they exist in the first place).
- DR plans are not tested even once every year to know if they are working.

This results in most DR plans being, well ... a disaster!

With an eye on business continuity planning (BCP), DR planning needs to begin with business impact analysis. While most DR planning exercises require the business to clarify the recovery point objective (RPO) and recovery time objective (RTO), this white paper details ten key areas (in no specific order). that we believe an infrastructure architect needs to focus on, in any DR planning exercise.

Not all data in an enterprise is mission critical. It is important to classify data and define the associated metrics for retention, retrieval and archival. Missing this can increase costs.

1 CLASSIFY INFORMATION SYSTEMS

The key to success for any organization's DR planning lies in the classification of its information systems/applications. Business impact analysis must be carried out to clearly define the information systems as mission critical, business critical or business support. While the general tendency for any application owner/ business owner is to consider all systems as critical/important, the impact of these systems and the availability requirements will help to accurately classify the systems. This is where RPO and RTO metrics play a pivotal role.

Some companies simply classify information systems as gold, silver and bronze, emphasizing the top category for DR planning. Systems classification will help to define policies such as back-up, retention, archival, etc., and attach the same scheme to the associated Information systems. So, it is absolutely essential to get this right.

2 CLASSIFY DATA

Data is evolving from mere records (e.g., spreadsheets, computational data, etc.) to representing communication such as e-mail, SMS texts, etc. to acting as informational currency (e.g., the Internet of Things, blockchain networks, etc.). However, not all data in an enterprise is mission critical. It is important to classify data and define the associated metrics for retention, retrieval and archival. Missing this can increase costs (storage, backup, management, etc.).

Though this might seem like a simple step, it is often very hard to achieve given that many people within an organization believe that every piece of data is important and must be retained forever. Classifying applications that are mission critical (mandating a DR plan) will result in identifying the data associated with these applications, thereby narrowing down the actual data that needs to be transferred over the wide area network (WAN) for recovery in the case of a disaster.

> If the DR solution is cloud based, and the customer only pays for storage and one or two appliances (that manage replication from the primary site), the solution will be cost-effective and the business team will view the IT team as a transformational partner.

3 CHOOSE THE DR LOCATION WISELY

Standards such as ISO 22301, BS25999-2, NIST SP 800, ISO 27001 and others typically don't provide the actual distance recommended between the primary and DR sites. This is primarily due to the fact that the distance for a DR site can vary depending on the disaster – such as earthquakes, floods, tsunamis, forest fires, tornadoes, hurricanes, etc. That said, your organization should choose a DR location that fits its business model, regulatory requirements, and the way revenue is generated.

For companies that rely heavily on customer-facing online applications, it's better to look at larger distances between the primary and DR sites. Given the host of back-up vendors that typically provide disaster recovery solutions integrated with the cloud and disaster recovery as a service (DRaaS), this approach bodes well for those organizations as they pay only for services that they use (typically during DR drills or during an actual DR scenario). They don't have the overhead of managing the DR site to high standards, meeting various regulatory requirements. Furthermore, using cloud services for DR is generally the first step in an organization's utility computing journey.

4 MAKE THE BUSINESS SEE THE VALUE – NOT JUST THE COST

When you see the promise, you pay the price. This is so true in any organizational spend; expenditures for DR readiness is no exception. Given that there is no certainty around when a disaster can strike, most organizations are reluctant to spend on DR readiness. But in most cases, there is more value to be realized while undertaking the DR planning exercise – such as improving the robustness of the existing primary applications, business confidence and reduced costs.

The DR planning exercise will uncover many issues that have typically been "swept under the carpet." Addressing them will improve the robustness of the existing application's landscape. When IT and business teams collaborate effectively to produce the necessary documentation (including technical recovery plans for each key business application), it improves business owners' confidence and helps them to see how IT can rescue the business in the event of a disaster. If the DR solution is cloud based, and the customer only pays for storage and one or two appliances (that manage replication from the primary site), the solution will be cost-effective and the business team will view the IT team as a transformational partner.

A survey that Forrester/DRJ conducted in 2017 found that only 18% of organizations use either DRaaS offerings or public cloud IaaS offerings.[1] On the other hand, Gartner estimates that the size of the DRaaS market will exceed that of the market for more traditional subscription-based DR services by 2018.[2] Clearly, the industry is moving towards DRaaS. Our recommendation: Evaluate the offering thoroughly and decide before it is too late.

5 IMPROVE PROTECTION AGAINST MALWARE

Disaster comes in many forms. Ransomware can be one such instance, in which hackers attempt to extort money from users via various Trojan Horse techniques, such as CryptoLocker, CryptoWall, Wannacry, Petya, NotPetya, etc. The malicious code injected encrypts data, files or even entire systems by generating a private-public pair of keys. It is impossible, or very difficult for any typical IT user, to decrypt the data without the private key, which is stored on the attacker's server until the ransom is paid.

Many companies across industries have suffered major losses due to these malware attacks. Reckitt Benckiser, a consumer goods firm specializing in health, hygiene and home products, estimated a drop in quarterly revenue growth by approximately 2% due to cyber attacks.[3] Courier delivery services company FedEx incurred costs of over $400 million through December 2017 in dealing with a NotPetya malware outbreak.[4] Pharmaceutical company Merck reported that revenue in both the fourth quarter and the full year of 2017 was unfavorably affected by approximately $125 million and $260 million, respectively, from lost sales in certain markets related to the cyber attack that occurred in June.[5] Many other enterprises such as Maersk, WPP and NHS have incurred huge costs in dealing with such malware attacks.[6, 7, 8] Worst yet, security software vendor Kaspersky reported in 2016 that one in five (20%) of ransomware victims who paid never got their data back.[9]

While the best way to protect businesses against these threats is to keep systems patched, use up-to-date anti-virus (with latest definitions) and

In the unfortunate case where a business becomes the victim of a ransomware attack, efficient DR solutions that replicate from the primary site to the DR location almost continuously (or at regular intervals) can help the business revert back to the state before the "attack" happened. Coupled with "awareness" communications to educate users about phishing e-mail, this could go a long way in securing the IT landscape.

Many organizations have a DR plan that will help them recover the individual servers. They then feel that as long as the servers are recovered, they should be able to recover the applications (business services). Most often than not, this is the perfect recipe for disaster.

security software, a robust DR plan can come to the rescue, too. In the unfortunate case where a business becomes the victim of a ransomware attack, efficient DR solutions that replicate from the primary site to the DR location almost continuously (or at regular intervals) can help the business revert back to the state before the "attack" happened. Coupled with "awareness" communications to educate users about phishing e-mail, this could go a long way in securing the IT landscape.

DOCUMENT THE DR PLAN

A 2016 survey that Zetta conducted revealed that two in five companies still don't have a documented DR plan.[10]

When it comes to DR planning, we cannot overemphasize the importance of documentation. It should cover all details such as physical and logical architecture, dependencies (inter- and intra-application), interface mapping, authentication, etc. Application dependency matrix, touchpoint diagrams, interface diagrams and application to physical/virtual server mapping play a significant role in defining how enterprise applications interact with each other to deliver various functionalities.

The key to getting the documentation right is to have a holistic view and focus on recovering the application services — not just servers. This is where sequence of the activities to be performed for restoring the service plays an important role. The technical recovery plan for each application/service needs to document all the details of the activities that need to be performed along with the sequence of the activities. Many organizations have a DR plan that will help them recover the individual servers. They then feel that as long as the servers are recovered, they should be able to recover the applications (business services). Most often than not, this is the perfect recipe for disaster.

TEST THE DR PLAN

The previously cited Forrester/DRJ survey found that 17% of the organizations conduct a full test of the DR plans less than once a year while 21% do not test their DR plans at all.[11] Meanwhile, the previously cited Zetta survey revealed that only 40% of the companies surveyed test their DR plans once a year.[12]

Most organizations have a DR plan (of sorts) and feel that they can recover key business applications in case of a disaster. The main issue is that these plans are not tested to identify gaps or challenges. Thoroughly testing the DR plan is the only way to unearth issues such as hard-coded IP addresses, host file entries, license file/ key, configuration details, dependency on other applications/ services, etc., resulting in the need to update the DR plan to make it robust. While it might not be possible to test all key business applications during a DR drill, it is important to focus on recovering the application(s)/service(s) and not just on servers. In essence, an untested DR plan is only a strategy.

8 AUTOMATE THE DR PLAN

The ability to orchestrate and automate a DR plan as well as successfully test that plan frequently will significantly improve confidence in it. One of the myths surrounding automated DR solutions is that they are not customizable or cannot work with a combination of physical and virtual servers. Nothing could be further from the truth.

While there can be exceptions, in general, automated DR has matured significantly, providing options for customizing and scripting. Companies should examine offerings such as Zerto Virtual Replication, Azure Site Recovery and others that provide these functionalities (i.e., automation and orchestration) and are cost-effective; we estimate that they'll save at least 20%, though actual savings vary among organizations.

9 EVALUATE AND CHOOSE AN OPTIMAL SOLUTION

Just because a product is number-one in the market or the most acclaimed does not necessarily make it the best fit for your organization's DR needs. While it might seem wasteful to invest in a "passive" data center, distributing the workload and having an "active-active" data center strategy might work well depending on the location of the users.[13] Organizations should consider taking this one step further by examining DRaaS

> Thoroughly testing the DR plan is the only way to unearth issues such as hard-coded IP addresses, host file entries, license file/key, configuration details, dependency on other applications/services, etc., resulting in the need to update the DR plan to make it robust.

> If there are key limitations that result in increased complexity or cost of the DR solution, take this opportunity to highlight the implications. This can pave the way for re-platforming/migration/upgrade activities that can remove these limitations.

solutions that incur costs based on usage and are usually less expensive when using the right toolset. It may be that DRaaS is, after all, not ideal for your enterprise given the limitations that exist in the current IT landscape. However, you can only know by trying. Before your organization finalizes its selection of a DR solution, it must ensure that the solution (via a proof of concept) is functional and fit for purpose. After all, the proof is in the pudding.

Beware of replication solutions in which the entire logical unit number (LUN) hosting multiple VMs needs to be replicated. The DR solution must be hypervisor/hardware agnostic so that choosing a specific hardware/hypervisor does not impact the overall DR plan. Solutions that provide the granularity not just in terms of recovery but also in terms of what is replicated will result in significant savings (i.e., bandwidth, storage and management costs).

10 SET EXPECTATIONS WITH BUSINESS OWNERS

It is important to get an official sign-off on the DR plan from the business owners and other key stakeholders. Rather than just giving them a document, schedule a meeting to take them through the plan, provide an overview and highlight the scope of the applications and services covered under the DR plan. This presents an opportunity to set expectations about what the business pays for and what it gets in return.

If there are key limitations (e.g., the existence of legacy servers/applications, physical servers, etc.) that result in increased complexity or cost of the DR solution, take this opportunity to highlight the implications. This can pave the way for re-platforming/migration/upgrade activities that can remove these limitations.

LOOKING FORWARD

When it comes to DR planning, it typically makes sense to start small (i.e., the application level) and then build the big picture. Focus on the technical recovery plan for a key business application. When your organization has completed a few of them, it will clearly see the overall DR plan unfolding. In many ways, having a functional DR plan is an organization's insurance plan to eliminate costly downtime during a disaster and prevent lost market share or reputational damage.

Sure enough, DR planning is painstaking. But the only thing harder than DR planning is explaining why your organization didn't do it.

FOOTNOTES

[1] Stephanie Balaouras, Forrester/DRJ, "The State of Disaster Recovery Preparedness 2017," www.drj.com/journal/spring-2017-volume-30-issue-1/the-state-of-disaster-recovery-preparedness-2017.html.

[2] Gartner Research, John P Morency, Christine Tenneson and Ron Blair, "Gartner Magic Quadrant for Disaster Recovery as a Service (2016)," www.gartner.com/doc/3350217/magic-quadrant-disaster-recovery-service.

[3] Update on cyber-attack – and estimate of financial effect, Reckitt Benckiser Group plc, www.rb.com/media/2989/rb-rns-6-july-2017.pdf.

[4] "NotPetya's Cost to FedEx: $400 Million and counting," https://securityledger.com/2017/12/notpetyas-cost-fedex-400-million-counting/.

[5] "Fourth-Quarter and Full-Year 2017 Financial Results, Merck," http://investors.merck.com/news/press-release-details/2018/Merck-Announces-Fourth-Quarter-and-Full-Year-2017-Financial-Results/default.aspx.

[6] "NotPetya ransomware attack cost us $300m – shipping giant Maersk," www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/.

[7] "Largest advertising company in the world still wincing after NotPetya punch," www.theregister.co.uk/2017/07/07/ad_giant_recovering_from_notpetya/.

[8] "NHS WannaCrypt postmortem: Outbreak blamed on lack of accountability," www.theregister.co.uk/2017/06/29/nhs_wannacry_report/.

[9] Kaspersky Security Bulletin 2016, https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf.

[10] "State of Disaster Recovery 2016," www.zetta.net/resource/state-disaster-recovery-2016.

[11] Stephanie Balaouras, Forrester/DRJ, "The State of Disaster Recovery Preparedness 2017," www.drj.com/journal/spring-2017-volume-30-issue-1/the-state-of-disaster-recovery-preparedness-2017.html.

[12] "State of Disaster Recovery 2016," www.zetta.net/resource/state-disaster-recovery-2016.

[13] An active-passive data center refers to an environment that only uses the passive data center in the case of a disaster. At all other times, the active data center will handle all requests. On the contrary, in an active-active data center, during business-as-usual operations, both the data centers handle requests, thus balancing the load and reducing impact during a disaster scenario.

ABOUT THE AUTHORS

Sudharson Aravamudhan

Senior Infrastructure Architect, Cognizant Infrastructure Services

Sudharson Aravamudhan is a Senior Infrastructure Architect with Cognizant Infrastructure Services. He has over 14 years of experience in the IT industry and has consulting experience at several leading companies across numerous industries, focusing predominantly on infrastructure consulting, data center migration, cloud and architecture. He holds a master's degree in human resource management from Pondicherry University and a bachelor's degree in electronics and communication from Madurai Kamaraj University. Sudharson can be reached at Sudharson.AN@cognizant.com.

Alec Selvon-Bruce

Director and Practice Lead, Enterprise Computing Practice, Cognizant Infrastructure Services, EMEA

Alec Selvon-Bruce is a Director and Practice Lead for Enterprise Computing Practice at Cognizant Infrastructure Services in EMEA. He has over 23 years of professional services experience across leading system integrations and technology providers. Alec drives the innovation councils that provide guidance on infrastructure and transformation strategy. He holds a master's degree in political studies from the University of Aberdeen. Alec can be reached at Alec.Selvon-Bruce@cognizant.com.

ABOUT COGNIZANT

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 205 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

Cognizant

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters
1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters
#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060