

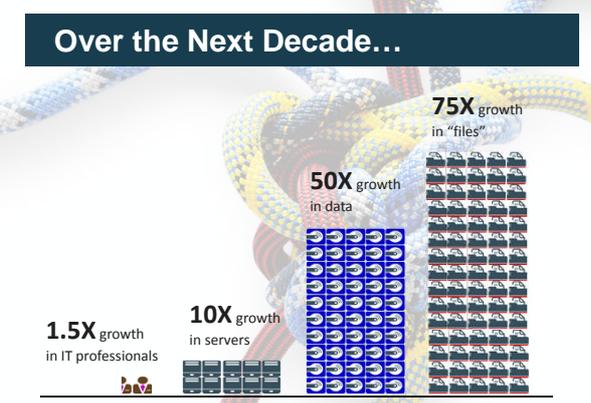
Disaster Recovery Planning Best Practices



Mohammad Alshafie, Systems Engineer | mo@unitrends.com
Harold Schmoecker, Regional Sales VP | harold@unitrends.com

UNITRENDS
Unified Data Protection, Without Limits

Over the Next Decade...



1.5X growth in IT professionals

10X growth in servers

50X growth in data

75X growth in "files"

[Source: The 2011 IDC Digital Universe Study]

Page 2

Why the information explosion?

"Why is the amount of data stored by your firm increasing?"



Reason	Percentage
Business is growing, so there's more data generated by existing systems	46%
We are capturing more data per business activity than before	32%
Regulatory compliance and auditing requirements require us to keep more data than before	29%
We have increased our replication and disaster recovery capabilities	28%
We are generating more data warehousing, reports, and analytics on existing business data	26%
We have increased use of audio and video data	22%
We haven't defined a data retention strategy, so we just save everything	21%
We just don't want to throw anything away	21%
The retention period for key business data or backups has lengthened	16%

Base: 1281 Server decision-makers with X86 servers at North American and European enterprises and SMBs
Source: Forrester's Technology Foresights For Hardware, Q3 2012

Consequences of downtime

Industry	Hourly Cost
Brokerage Services	\$6.8M
Energy	\$2.8M
Telecom	\$2.0M
Manufacturing	\$1.6M
Retail	\$1.1M
Health Care	\$636K
Media	\$90K

Industry Average Cost of Downtime, US \$
Sources: Network Computing, the Meta Group and Contingency Planning Research



Consequences of data loss

- 93% of companies that lost their data center for 10 days or more
 - filed for bankruptcy within one year of the disaster.
 - Source: National Archives & Records Administration in Washington
- 94% of companies suffering from a catastrophic data loss do not survive
 - 43% never reopen
 - 51% close within two years.
 - Source: University of Texas study on catastrophic data loss
- 30% of all businesses that have a major fire
 - go out of business within a year
 - 70% fail within five years
 - Source: Home Office Computing Magazine



Consequences of data loss

- 77% of companies who test their tape backups found back-up failures.
 - Source: Boston Computing Network, Data Loss Statistics
- 7 out of 10 small firms that experience a major data loss go out of business within a year.
 - Source: DTI/Price Waterhouse Coopers
- 96% of all business workstations are not being backed up.
 - Source: Contingency Planning and Strategic Research Corporation
- 50% of all tape backups fail to restore.
 - Source: Gartner



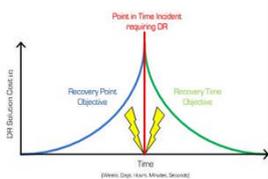
Agenda

- › *The evolving role of backup as part of disaster recovery*
- › *Using hybrid strategies to find the right fit for your environment*
- › *Recommendations and next steps*



RTO and RPO

- Recovery Time Objective (RTO):
 - Fancy definition (from Wikipedia): Duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
 - Simple definition: Acceptable length of time without service and data being available
- Recovery Point Objective (RPO):
 - Fancy definition (from Wikipedia): Maximum tolerable period in which data might be lost from an IT Service due to a Major Incident
 - Simple definition: How much data (past and present) must be restorable in the RTO



Considering your IT environment

- Few mid-market IT shops are 100% virtualized
- However, over 60% have some level of virtualization
- Top reasons for virtualization:
 - Server and storage consolidation
 - Hardware and infrastructure cost savings
 - Heating/cooling and power
 - IT Staff productivity



Stuff to think about data protection and DR

- What's your budget vs. your SLA's?

- ✓ Recovery point objectives
 - How much lost data can you afford?
 - Data size/change rate
- ✓ Recovery time objectives
 - How long can you afford to be down?
- ✓ Backup windows
- ✓ Cloud for DR
 - Public or private
- ✓ IT administrators
 - Capacity
 - Expertise
- ✓ IT environment topology
 - Physical servers
 - Virtual servers/hosts
 - Storage
 - Applications



Unifornds Confidential

Page 10

What Causes DR Epic Fails?

1. Malfunctioning Backup Technology
 - Backup Technology FIRST
 - Backup & Replicate, Archive, Bare Metal
 - Planning comes second
2. Neglecting to Plan
 - Detailed Guideline Documentation
 - Identify key people
 - Identify key systems
 - Process: Step-by-Step Guidelines
3. Failing to Test, Test, and Test AGAIN!
 - Fundamental Mistakes:
 - Fail to test plans on a consistent basis
 - Fail to test real world scenarios
 - Change rate of data is a good benchmark for DR test frequency

Unifornds Confidential

Page 11

What Causes DR Epic Fails?

4. Assuming Homogeneity
 - Simplifying IT infrastructure is always a good thing.....until it isn't!
 - Maintain flexibility in order to maximize ROI

Unifornds Confidential

Page 12

Agenda

- › *Industry trends on Disaster Recovery integration with the backup process*
- › *Cloud disaster recovery options and alternatives*
- › *On-premise, off-premise and hybrid approach to disaster recovery*



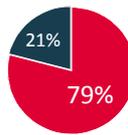
Agenda

- › *Industry trends on Disaster Recovery integration with the backup process*
- › *Cloud disaster recovery options and alternatives*
- › *On-premise, off-premise and hybrid approach to disaster recovery*



Industry Trends on Disaster Recovery and Backup Process

2013 Disaster Recovery Current Landscape



- Have Tape Backup, Disk Backup or another form of backup
- Have HA Automated DR Technologies

Future of Disaster Recovery

Automated Backup with replication	39%
Other	25%
Array-based Replication	11%
Tape Backup	10%

Why should your DR start with your Backup?

— Because we are simply Human

- 43% of companies have experienced at least one incident of data loss in the past year
- 65% of companies report that a significant portion of all plans rely on manual process
- 67% of companies state that loss in productivity is most common consequence of data loss

Source: Disaster Recovery Fitbit and Metrics Survey, IDC Technology Survey



Eliminate Complexity

By 2016, one-third of organizations will change backup vendors due to frustration over **cost, complexity, capability**

The fourth and fifth Cs of backup concerns: **completeness and scale, customer support**

Source: Gartner, Best Practices for Addressing the Broken State of Backup, Dave Russell, August 27, 2010

Agenda

- › *Industry trends on Disaster Recovery integration with the backup process*
- › *Cloud disaster recovery options and alternatives*
- › *On-premise, off-premise and hybrid approach to disaster recovery*

Cloud Considerations

- Blended systems with local backup plus cloud becoming common
 - Take advantage of cloud economies and flexibility
 - But
 - Add another layer of management
- Service provider risks
 - SLAs
 - Never put all eggs in one basket
- CAPEX benefits
 - Significant savings DR
 - Facilitates backup of remote sites
- WAN Latency may be acceptable for secondary storage
 - When cloud is an alternative
 - Compare existing storage costs to cloud offering(s):\$/GB/month



- ### How do you decide which is best?
- Disk-to-Disk-to-Cloud considerations:
- How much CapEx are you saving vs monthly cloud service fees?
 - Are you comfortable with the manageability and control of your data?
 - Are you able to **seed** the cloud with any sort of direct access?
 - How (and how quickly) can you recover from a real disaster from the cloud?
 - How much "trust" do you have in your cloud service provider?
 - Could you pass a compliance audit of your data in the cloud?

- ### "Seeding" Data Strategies
- How quickly can you get your data protected?
 - 1TB → T1 = 30-60 days
 - Do you have any form of "direct access" to the cloud for fast uploading?
 - What happens if the data you're protecting changes by a great degree?
 - Policy change requires all data to be encrypted
-

How do you decide which is best?

Disk-to-Disk-to-Disk considerations

- Should you use rotational disk drives?
- Saving copies of your data to removable disk drive
- You could have a pickup and storage service (something like Iron Mountain) to handle rotational disk drives
- Should contain enough data and information to completely rebuild your primary site in the event of a disaster
- Should you use Attached Storage
 - Long-term retention on premise
 - Storage pool can be extended to accommodate retention needs
 - Secondary storage pool can be setup in an DR location for replication target



How do you decide which is best?

Disk-to-Disk-to-Tape rotational archiving considerations:

- You can have a pickup and storage service like Iron Mountain secure your tapes
- Minimally have someone on your IT staff responsible for taking tapes off premise regularly
- Your solution should ensure your tapes contain enough information to rebuild your entire IT environment in the event you experience a true disaster



Agenda

- › *Industry trends on Disaster Recovery integration with the backup process*
- › *Cloud disaster recovery options and alternatives*
- › *On-premise, off-premise and hybrid approach to disaster recovery*



On-Premise and Off-Premise Disaster Recovery

On-Premise DR Strategy

- Data kept on premise
- Can you recovery objectives in the event of a site failure?

Off-Premise DR Strategy

- Data replicated off premise
- Can you meet Recovery Objectives and SLAs?

UNITRENDS logo 25

Hybrid Disaster Recovery Strategy

Hybrid DR Strategy

- Data kept on premise
- Data replicated off premise
- Meet recovery objectives
- Minimize outage and unplanned down time

UNITRENDS logo 26

Recovering from Real Disasters

No matter which Disaster Recovery method you choose, you want to ask these questions:

How quickly can you recover your data?

How quickly can you recover your system?

How quickly can you recover your premise?

UNITRENDS logo 27

What Did We Learn?

- › *BR/DR are increasingly converging to one automated process*
- › *Chose which method is optimal for your environment*
- › *On-premise, off-premise and hybrid approach to disaster recovery*



Conclusions

- Know your business requirements
 - SLA's
 - RPO's & RTO's
 - Compliance regulations
- Know your budget
- Plan for disaster
- Test to your plan



Unifrends Confidential  Page 29
