Backup and Disaster Recovery: DIY or Buy?

Presented by: Stanley Louissaint
Presenter

Stanley Louissaint

• Principal and Founder, Fluid Designs
  ▪ Managed Service Provider
  ▪ Business Continuity Solutions
  ▪ Computer and Network Support/Consulting
  ▪ Computer & Mobile Forensics
  ▪ e-Discovery & Litigation Support

Phone: 908.688.2444
E-mail: slouissaint@fluiddesigns.com
LinkedIn: www.linkedin.com/in/slouissaint
Website: www.fluiddesigns.com
Introduction

• What am I talking about?
• What will I cover?
• What’s in it for you?
  • Insights into BDR options.
  • The impact that your decision has on your firm.
  • Q&A
  • Downloadable materials
Who Are You & What Have You Experienced?

• Firm size? Solo  2-10  11-30  30+
• Have you ever lost any files?
• You or someone you know hit by ransomware?
• Had a serious computer outage?
• Do you currently have a backup strategy in place?
• Do you currently have a disaster recovery strategy in place?
Subject: Invoice

To: GallagherBarrett@airtelbroadband.in

Dear Sir/Madam,

I trust this email finds you well,

Please see attached file regarding client's recent bill. Should you need further assistance, please feel free to email us.

Best Regards,

Barrett Gallagher
Community Health Systems, Inc.

www.chs.net
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so much time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Check Payment  Decrypt
Client Story

Your money or your data
That OMG moment!

- What went wrong?
- How does it feel?
- How do we fix it?
- What did we lose?
Disaster Strikes...

Are these your first thoughts:

• How old is our backup?
• Is it a good backup?

Did we lose everything?
Downtime

- Average company 10 hours of IT downtime per year\(^1\)
- 27% of users confident they can be back up after a disaster\(^2\)
- 75% of businesses have no Disaster Recovery Plan (DRP)

\(^1\)Source: CA Technologies 2012
\(^2\)Source: Information Week 2013
Downtime

• Root causes of unplanned outages
  • Hardware Failures – 35%
  • Natural Disasters – 10%
  • Human Error – 22%

*Source: 2016 Ponemon Institute Cost of Data Center Outages Report
It’s not about the technology.
It’s about keeping your business running.
Recovery Point Objective

• Often referred to as RPO
• How much data can your business afford to lose before negative consequences begin?
Recovery Time Objective

- Often referred to as RTO
- How long can you operate while your servers being offline?
# Recovery

<table>
<thead>
<tr>
<th></th>
<th>Best in Class</th>
<th>Average</th>
<th>Laggard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of downtime incidents in past 12 months</td>
<td>0.56</td>
<td>2.26</td>
<td>3.92</td>
</tr>
<tr>
<td>Average amount of downtime per event in last 12 months</td>
<td>0.16 hrs.</td>
<td>1.49 hrs.</td>
<td>17.82 hrs.</td>
</tr>
<tr>
<td>Longest downtime event</td>
<td>0.21 hrs.</td>
<td>4.78 hrs.</td>
<td>43.71 hrs.</td>
</tr>
<tr>
<td>Critical application availability</td>
<td>99.90%</td>
<td>99.62%</td>
<td>99.58%</td>
</tr>
<tr>
<td>Length of time to recover from last downtime event</td>
<td>1.13 hrs.</td>
<td>5.18 hrs.</td>
<td>27.11 hrs.</td>
</tr>
</tbody>
</table>
Backup

• “Data Backup”
• Process in which we duplicate data
• Allows for retrieval in the event of a data loss event
Backup Options

• Local
  • Data stored on internal/external media
    • Hard drive, optical discs, flash drives, network attached storage (NAS), tape drive

• Cloud
  • Data stored in cloud

• Local + Cloud
  • Data stored on internal/external media
  • Data stored in the cloud
Disaster Recovery

• The ability to bring your systems online through your platform
• Data backup AND servers are available
• Used for catastrophic events
Backup + Disaster Recovery = BDR
Why a BDR?

• Backup your servers
  • Image based backups

• BDR’s run as a replacement server
  • Backup images are run as virtual machines

• Minimize downtime

• Restore tests
A BDR is not...

- High Availability
  - Redundancy and no single point of failure
  - Doesn’t protect against data corruption
  - Handles physical failures
  - Can be used in conjunction with BDR but not a replacement for
Basics Components of Business Continuity

- Backup Software
- Backup Storage
- Failover Hardware
- Off-site Storage/Archiving
- Remote Failover
Business Continuity

Servers -> Physical Backup Appliance

TRANSFER via SSL VPN

Cloud Storage

Recovery

E-mail

Applications

Databases

File Systems

Screenshot Backup Verification
Business Continuity Methodology

• Business Continuity
  1. What is it?
  2. Why?
     • Fully Automated
     • Availability
     • Archiving
     • Multiple versions of backups
     • On & Off-site copies
     • Ability to run servers, hardware or location failures
  3. What is the frequency of the backup?
     • Continuous Backup
Key BDR Differentiators

- Agent or Agentless
- OS Support
- Chain Technology
- Data Encryption
<table>
<thead>
<tr>
<th><strong>Agent</strong></th>
<th><strong>Agentless</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Have to be installed on each server</td>
<td>• Nothing to install on servers</td>
</tr>
<tr>
<td>• Allows for multiple types of snapshots</td>
<td>• Reduces cost and simplifies administration</td>
</tr>
<tr>
<td>• No need for special credentials since services are running</td>
<td>• Centralized management</td>
</tr>
<tr>
<td>• Allows for granular restores of database servers</td>
<td>• Limited snapshot support</td>
</tr>
<tr>
<td>• Utilizes resources on server</td>
<td>• Must have a privileged username/password stored on backup server</td>
</tr>
<tr>
<td></td>
<td>• Lower impact on server</td>
</tr>
</tbody>
</table>
Key BDR Differentiators — OS Support

- What type of physical machines are supported?
  - Microsoft Windows Server
  - macOS Server
  - Linux Server

- Are virtual environments supported?
  - Microsoft Hyper-V
  - VMWare
  - Citrix XenServer
Key BDR Differentiators – Chain Technology

- Traditional Chain Technology
  - A full backup and subsequent backups are incremental, all points are needed for full recovery

- Inverse Chain Technology
  - All recovery points are image-based backups can be fully constructed
  - Ability to delete backups without resetting the backup chain

- Chain-Free
  - No dependency on other backup points
  - Each backup point stands on its own
Key BDR Differentiators – Encryption

• Can you encrypt the local data?
• Can you encrypt the cloud data?
Pre-Packaged Solutions

• BDR Appliance – Local
• BDR Appliance – Local + Cloud Storage
Pre-Packaged Solutions - BDR Appliance — Local

• Data stored on BDR
• Ability to spin up virtual machines on BDR locally
• No off-site copy
• BDR but not true business continuity since no off-site option
  • Down location no way to spin up cloud option
Pre-Packaged Solutions - BDR Appliance — Local + Cloud Storage

• Data is stored on BDR
• Data is also stored in the cloud
  • Most providers have multiple data centers
  • Some providers allow for use of third party data centers
• Ability to spin up virtual machines on BDR locally
• Ability to spin up virtual machines in the cloud
  • Used when you have a physical issue in your location
• Most solutions can also archive your data and retain it for a period of time – days, years, infinite
Pre-packaged Solutions – Pros

• No guess work
• Faster implementation
• Hardware & Software tightly integrated
• Leverage the expertise and support of the vendor
• Benefit from any upgrade or enhances that are rolled out
• Most meet compliance requirements
• Service Level Agreements
• Multiple data centers
• Ease of cloud launch in the event of disaster
Pre-packaged Solutions – Cons

• Hardware options limited by vendors
• May not have ability to upgrade
• Security concerns w/ data access
• Recurring monthly costs/subscription based
Build Your Own

• BDR Appliance – Local Backup
• BDR Appliance – Local Backup + Cloud Storage
Build Your Own — BDR Appliance — Local Only

• What’s needed?
  • Hardware
    • Server
      • Motherboard
      • Processor
      • RAM
      • Hard Drives/SSD/Flash Storage
    • Case
    • Power Supply(s)

• Software
  • StorageCraft
  • Replibit
  • Cloudera
  • Macrium
  • Quorum
Build Your Own — BDR Appliance — Local + Cloud

• What’s needed?
  • Hardware
    • Server
      • Motherboard
      • Processor
      • RAM
      • Hard Drives/SSD/Flash Storage
      • Case
      • Power Supply(s)
  • Software
    • StorageCraft
    • Replibit
    • Cloudera
    • Macrium
    • Quorum
  • Cloud Storage
    • Amazon S3
    • Microsoft Azure
Build Your Own – Pitfalls

• Not sizing your device properly
  • Lack of storage space, memory or CPU

• Unforeseen labor costs
  • What did it really cost you to build?

• Failure to test backups
Build Your Own – Pros

• Can pick your hardware and software
• Upgradeable
• Non-recurring fees on licensing
• Control costs
Build Your Own – Cons

• Expertise is needed for configuration and setup
• Expertise is needed for compliance requirements
• Lack of vendor support
• No Service Level Agreement (SLA)
• Lack of integration
• Have to manage backup chains and test


**Let's Compare**

**Pre-Packaged Solution**

- Intel Xeon D-1541 8-Core 1U Rackmount 2 x 10GbE, 32GB ECC, 128GB OS SSD & 2-1TB Hard Drives w/ Software and Unlimited Agents - **$2,500**
- Monthly Recurring Service w/ 1 Year Data Retention - **$275**

**Build Your Own**

- Intel Xeon D-1541 8-Core 1U Rackmount 2 x 10GbE, 32GB ECC, 128GB OS SSD & 2-1TB Hard Drives - **$1,750**
- (1) ShadowProtect SPX Annual License - **$657**
- Amazon Cloud Storage 2 TB – **$70+**
Let's Compare

Pre-Packaged Solution
• $2,500 One-Time Costs
• $275 Monthly Recurring Costs

Build Your Own
• $2,407 One-Time Costs
• $70+ Monthly Cloud Storage Costs
• Unknown management costs
Downloadable Materials

Free downloads at:
www.fluiddesigns.com/aba

“THE LAWYERS GUIDE TO RANSOMWARE”
&
RECOVERY TIME & DOWNTIME COST CALCULATOR
Presenter

Stanley Louissaint

• Principal and Founder, Fluid Designs
  ▪ Managed Service Provider
  ▪ Business Continuity Solutions
  ▪ Computer and Network Support/Consulting
  ▪ Computer & Mobile Forensics
  ▪ e-Discovery & Litigation Support

Phone: 908.688.2444
E-mail: slouissaint@fluiddesigns.com
LinkedIn: www.linkedin.com/in/slouissaint
Website: www.fluiddesigns.com
• YOU play the most important part in keeping TECHSHOW exciting. Please complete the Speaker evaluation before you leave.

• Reserve the dates!

TECHSHOW 2019: February 27 – March 2, 2019