



# Protecting Oneself: Backing up, Archiving and Restoring Data

Sean Costello

IronGate Server Management & Consulting  
[Sean@IronGate.ca](mailto:Sean@IronGate.ca) • @SeanInMotion

# What is backup?

# What is backup?

- Backup is what we can restore in a crisis
- Backup is not having to say “I’m sorry”
- Backup is feeling safe at night
- Backup is a way to protect your investment of time in a project
- Backup is not Archive

# Backup vs. Archive

- Backup is all about being able to quickly resume use of data that you are still in the middle of (or were very recently) using.
- Archive is being able to go back to old work we weren't sure we were going to need, or wasn't worth keeping in our live systems.
- The kicker? You must backup your archives.







# Restoration

# Restoration

- When disaster strikes, how far back in time are you willing to travel?

# Restoration

- When disaster strikes, how far back in time are you willing to travel?
- How much time will rebuilding the system take?



# Restoration

- When disaster strikes, how far back in time are you willing to travel?
- How much time will rebuilding the system take?
- How much will the restoration downtime cost?

# Restoration

- When disaster strikes, how far back in time are you willing to travel?
- How much time will rebuilding the system take?
- How much will the restoration downtime cost?
- Schedule a monthly restore test. Discuss the results with your clients.

# Requisite spaceflight slide:



© Getty Images



# Planning the Backup

# Planning the Backup

- Data Source



# Planning the Backup

- Data Source
- Backup Destination

# Planning the Backup

- Data Source
- Backup Destination
- Transport Medium (Software)

# Planning the Backup

- Data Source
- Backup Destination
- Transport Medium (Software)
- Backup Frequency

# Planning the Backup

- Data Source
- Backup Destination
- Transport Medium (Software)
- Backup Frequency
- Defining layers of protection

# Planning the Backup

- Data Source
- Backup Destination
- Transport Medium (Software)
- Backup Frequency
- Defining layers of protection
- Method & speed of restoration







First Published: 19:36 IST(29/8/2011)  
Last Updated: 19:38 IST(29/8/2011)

## Branson loses autobiography in blaze

Airline tycoon Richard Branson has lost his autobiography and 15 years of handwritten notes after his British Virgin Islands house caught fire.

Actress Kate Winslet and 20 other guests were holidaying at the billionaire's home when lightening hit the wooden property and set it ablaze, reports [contactmusic.com](http://contactmusic.com).

"My office was in the house and I lost everything in it. I'd got a long way into writing my autobiography and it's lost. Fifteen years of handwritten notebooks went and photographs and so on," Branson told Britain's The Sunday Times.

"Running a business, we have a meticulous computer backup system so I'd assumed all that was completely safe. But it turns out the backup was also in the house.

"Everything filed on the computers there in the past few years is lost, both business-related and personal... But these are things. And as long as you have your family and friends around you, they're not that important," he added.

<http://www.hindustantimes.com/StoryPage/Print/739287.aspx>

© Copyright © 2011 HT Media Limited. All Rights Reserved.

# The case for backup

- “Can you afford to lose everything you’ve done since your last backup?”
- Focus on the restoration when discussing options with clients.
- Let the client imagine the alternatives to backup, while trying not to resort to scare tactics.
- When a client doesn’t seem open to the idea, draw out the real reason why.
- Will a hold harmless agreement work?

# What to back up?

- Bootable or user data only?
- Databases will have to be addressed specially
- Consider how you are backing up your large files, IE Entourage Databases and Virtual Machines.
- How to keep track of your backup status.

# Where to backup to?

- Disk-based media
  - Plain hard drives
  - Drive cartridges
- Tape drives / libraries
- Network Attached Storage
- Storage Area Network
- Continuous onsite/offsite solutions
- Backing up the backups
- Encrypting the backup media



# Thieves hit radio host's home, steal precious laptop

DOUG HEMPSTEAD, OTTAWA SUN

FIRST POSTED: THURSDAY, JULY 29, 2010 07:01 PM EDT | UPDATED: FRIDAY, JULY 30, 2010 06:55 AM EDT

Lowell Green wonders if he was the target of a random robbery, or if thieves to his west-end home **knew exactly what they were looking for.**

Wednesday, the local radio talk show host and author discovered his home had been broken into, and **the only thing stolen was his HP laptop computer.**

The machine was stored in Green's home office and contained all the research for his upcoming book, which will be about immigration and multiculturalism. He **hadn't backed up much of the data** and didn't store it anywhere else. A rough draft of the book has already been sent for editing, but **all the background work is lost.**

# Encrypted drive options

- Apricorn Aegis Padlock
- Data Locker
- LaCie SAFE hard drives
- MXI Stealth Bio hard drives and flash drives
- RadTech's Impact enclosures
- RocStor's Rocbit FXKT and Rocsafe MX
- SecureDisk enclosures
- any drive with full disk encryption - PGP, Truecrypt, WinMagic & others

# The backup software

- Time Machine
- Carbon Copy Cloner / SuperDuper!
- Crashplan / CrashPlan PRO / PROe
- PresSTORE
- Retrospect 8
- Rsync & other scripted solutions

# Monitoring the backups

- Why wait until the monthly restore test?
- Built in email notification
- Monitoring Products
- Client Education

# Testing the Restore

- Document the restore process as a part of the backup planning.
- Schedule the test restores in your calendar, make that a repeating task.
- Great for client education & empowerment
- Talking about the results, good or bad, will foster a deeper sense of trust.



Thank-you for coming to join us today!

Any questions?