What Every Business Owner Should Know About Protecting Their Data

Presented by

Mitchell Romm

Managing Partner

Dr.Backup

www.drbackup.net

(301) 560-4534

support@drbackup.net

Dr.Backup™ online backup service

we've got your BACK

Climbing the Mountain

- These days, it seems that running a business is like trying to climb a steep mountain
- It's a challenging world out there and danger confronts us daily
- What if you slip while climbing and fall? ...all the way to the bottom
- We all need a reliable "safety line" to help protect us

Dr.Backup™ online backup service

we've got your BACK

What If You Came Into The Office Tomorrow Morning And All Your Data Was Gone – Without Warning?

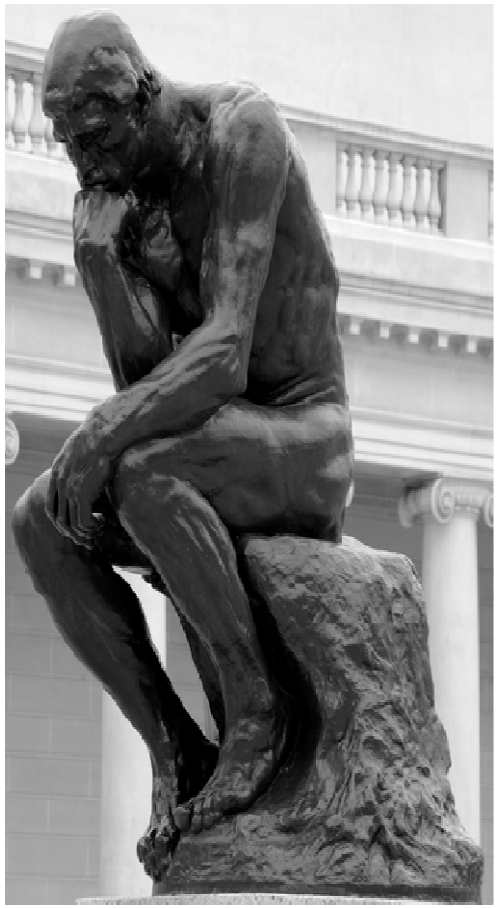
This is not fiction or a rare occurrence.
It happens **every day** to businesses everywhere.

Dr.Backup™
online backup service

we've got your BACK

Businesses Run on Data – But Have You Ever Tried To Locate All **Your** Critical Information?

- What you must have back within 24 hrs of a “fall”
- Your “Tier-1” operations data
  - Financial (invoices, AR, payroll, etc.)
  - Customer service/ordering systems
  - Work-in-progress (projects and schedules)
  - Sales, marketing and customer communication tools
- Important: Have each worker compile a written list of files, folders and applications they use regularly – these are needed to configure data protection technology
- Business owner should personally oversee Tier-1 analysis process - delegate analysis of less critical data



Dr.Backup™ online backup service

we've got your BACK

The “Dark Side” of Information Technology– Named Perils

(When you’re a computer, it’s a dangerous world out there...)

Technical Perils	Virus, ransomware, file corruption, hardware failure, software bugs, failed patches or upgrades
Human Perils	Accidental file delete/overwrite, sabotage, fraud, spilled coffee, theft, hackers, unknown event
Natural Perils	Fire, flood, hurricanes, tornado, earthquake, lightening strike, sprinkler malfunction, power surges

Darth Sidius
Star Wars
(villain)

The majority of small-mid size businesses are vulnerable to unexpected data loss.

Dr.Backup™ online backup service

we’ve got your BACK

Hard Disk Drive Failure Rates
Source: Google (large scale failure analysis)

- Don't believe the 1.2 million hour MTBF figures disk drive manufacturers publish. These are just simulated failure intervals!
- Realistically, expect 1 in 14 hard drives will fail within the first year of service. 1 in 4 will fail within three years!!
- How old is your computing equipment?

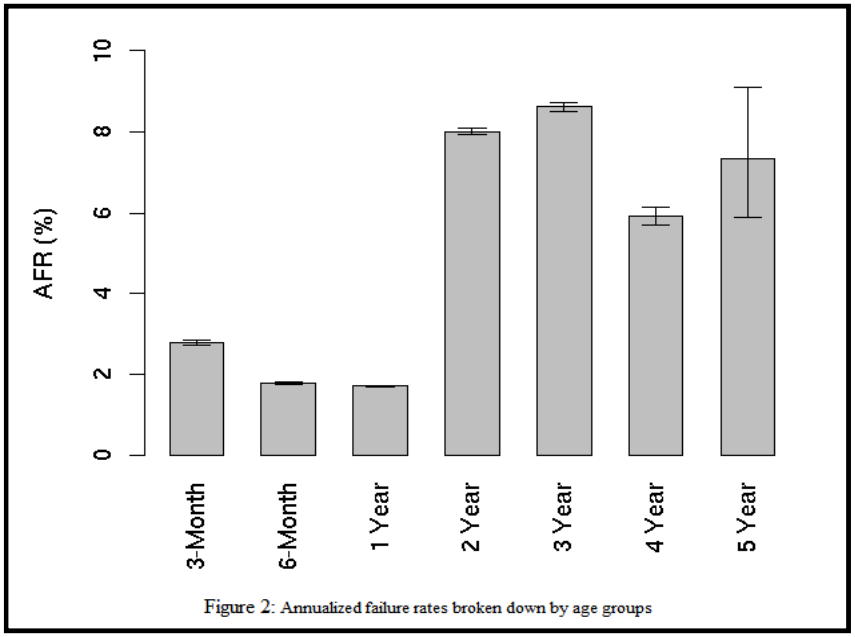


Figure 2: Annualized failure rates broken down by age groups

The Likelihood of Your Business Suffering a Data Disaster Sometime In the Near Future is High. What are you going to do?

OR

Stick your head in the sand and hope it doesn't happen to you

Raise your head, snarl, and come up with a contingency plan

Dr.Backup™ online backup service

we've got your BACK

Contingency Plan Goal

Protect your business against loss by regularly making copies of important data and securely transferring the copies to a "threat-safe" location from where they can be readily retrieved and used if necessary.

Dr.Backup™
online backup service

we've got your BACK

Action Plan: Implement These Data Safeguards

(Do You Have A Realistic RPO and RTO?)

- Mirrored Disks (RAID)
  - Protects against drive failure
  - **BUT**: Can mask equipment problems unless monitored
- Local backup (redundancy)
  - Fast backup/restore, bulk data storage, programs and data, “bare metal” restore (virtualization possible)
  - **BUT**: Subject to many of same threats as primary storage
- Online backup (physical protection)
  - Offsite backup means full threat protection – including physical
  - **BUT**: Limited upload speeds, higher cost per storage unit (start with mission critical data first)

All technology products require some management and oversight. There is no such thing as a “set-it-and-forget-it” product.

Dr.Backup™ online backup service

we've got your BACK

Technology-Threat Analysis
How Well Are You Protected?

Threat	RAID	Local Backup	Online Backup
Hardware Failure	Yes	Yes	Yes
Software Bug	No	Yes	Yes
File System Corrupt	No	Yes	Yes
Accidental Deletion	No	Yes	Yes
Virus Infection	No	Yes*	Yes
Human Error	No	Yes	Yes
Employee Sabotage	No	No	Yes
Natural Disaster	No	No	Yes
Equipment Theft	No	No	Yes
Power Surge	No	No	Yes

* Partial Protection

If possible, protect your business using all three approaches.

Dr.Backup™ online backup service

we've got your BACK

What Happens If Computer Equipment is Stolen?

- Yes, you can replace the physical assets and recover data from your backups...in theory. BUT...
- You must assume that confidential information about your clients has been compromised. The bad guys don't need your Windows password to see your data.

- In many cases you are required to disclose this information to your clients and to your insurance company. You may ultimately be responsible for remediation steps/costs. UNLESS...
- Consider employing full disk encryption protection on all your systems – especially any laptops or portable devices. Makes it virtually impossible to access stored data without entering encryption password at boot time – before even Windows starts!

It's An Ongoing Process…Keep it Going with Periodic Review & Update - Don't Take Your Eye off the Backup

- Perform periodic fire drills to restore random key data
- Adjust configuration of backup technology whenever changes occur – watch the updates!
- Review product log files, emails, etc. to find out if backups are occurring and are error free
- Educate employees on the importance of ensuring their data is backed up

Don't choose a self-service product if you don't have the time or expertise to manage it yourself.
S.M.A.R.T. = Setup, Monitor, Alert, Restore and Test

Dr.Backup™ online backup service

we've got your BACK

Bonus Tips

- Get professional (vendor) help to backup SQL, Exchange, Databases or other proprietary applications – if possible, avoid backing up a backup
- Best to backup data when it's in a closed and quiescent state on the hard disk. Open file backups are sometimes necessary (crash-consistency)
- Convert any software distribution CDs to (.iso) images and backup. Name the file with the product key and keep with data for easy recovery
- When backing up products that use multi-file databases (index sequential), always create a FULL backup to get all database files as a compete set
- Always have an offsite backup of your Tier-1 data – lower priority data can sometimes be backed up less often and stored on low cost media
- Begin integrating SSD technology into your computer systems – everything runs faster (including backups) and productivity gains are real

Benefits of Choosing **Dr.Backup**
S.M.A.R.T. Online & Local Image Backups

SSAE 16 TYPE II Certified

- Serving small businesses since 2001 – Backup is our only business!
- "Done-For-You" (Managed) cloud backup service with fully assisted setup & data restores PLUS daily monitoring and alert notification
- Generous storage packages – based on compressed data size
- Backup: MS-SQL, Exchange, Open files, Active Directory & more
- Local Image Backup to customer-owned onsite media for blazing fast restores, system virtualization and "bare metal" restore capability
- Average client invests just $2 /day – isn't your business worth it?
- HIPAA compliance for medical professionals
- 100% Customer Satisfaction Guarantee – no offshore call centers

30-Day Risk Free Trial – Ask your IT professional about **Dr.Backup** or call us today at **(888) 716-5816 or email support@drbackup.net**

Dr.Backup™ online backup service

we've got your BACK