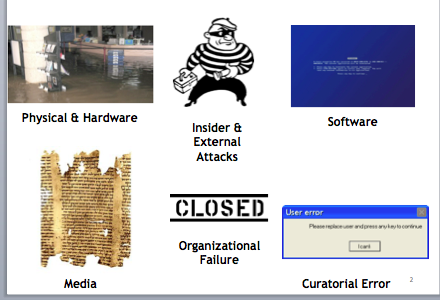
## Introduction

-- Durable Bits are not a Solved Problem

-- Importance of long term access

## Classes of Threats



Approaches to Mitigating Bit Level Risk

Personal examples 7 PLAGUES 1 COMPUTER CENTERq

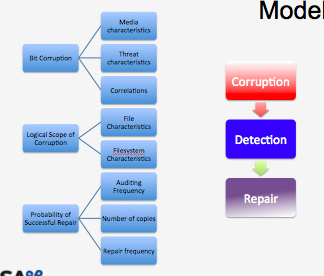
- airplane crashes - impact, fire & flood

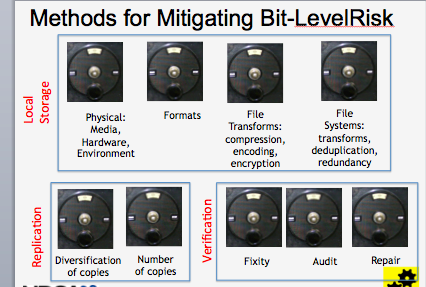
- rats

- regular 3PM thunderstorms 100’s of miles away

- quarry blasting -

- CRICKETS





## Model

Keeping risk of object loss fixed

-- what choices minimize $?

Modeling risks and controls overall structure

- Problem defined

“Dual problem”

Keeping $ fixed, what choices minimize risk?

Extension

For specific cost functions for loss of object:

Loss(object\_i), of all lost objects

What choices minimize:  
  
Total cost= preservation cost+ sum(E(Loss))

- Event based

Actors

- content owners

- auditors

- storage providers

Objects

- Shelves

- Blocks

- Documents

- Collection - treated as one

Messages:

- Silent failures

- Communication costs

Base Model/Extensions

We've modeled block-level errors as poisson distributed (no correlated failures, no bathtub curve -- which implicitly assumes disks are burned-in elsewhere, replaced regularly, and swapped out after early signs of block-level failures), and are adding shelf-level and institutional failures, and auditing / repair.

The idea is to use a block-life-error rate consistent with the ex-post rate of failure on ia RAIDed system, rather than model the RAID & filesystems mechanisms explicitly.

At this point, our plans for these extensions are:

- Shelves fail noisily (no audit needed to detect), and failures are exponentially distributed. Some positive level of correlation among shelves within an institution.

- Institutions may fail noisily or silently, based on a normal distribution, with some positive level of correlation among institutions.

- Auditing is either based on use of object (Zipf distribution); random sample (uniform), or is periodic -- per collection, per institution, or complete. Audit time is proportional to size of collection.

- Repair time is proportional to size of object (different factor than auditing). Repair is more costly if less than a quorum (default majority) remains -- since assume manual intervention is required to determine correct copy.

# Calibration Assumptions

- Google High Replication Datastore, AWS

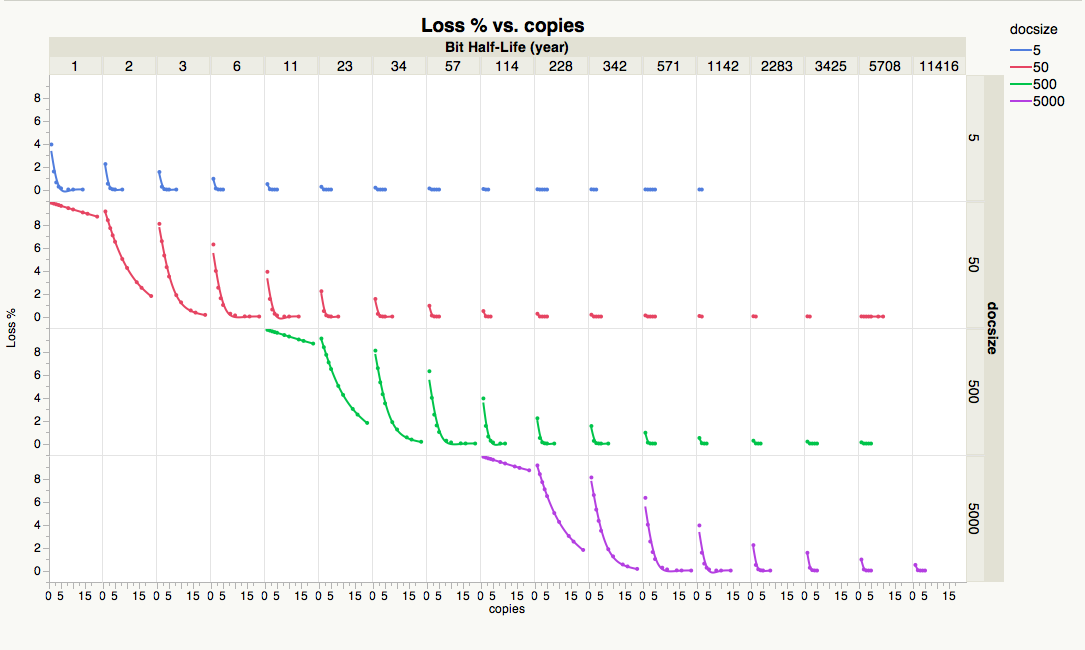
- Preservica background

- DPN

- Failure rates from Internet archive, Google studies, Backblaze

# 

# When is replication alone enough? A simple case.



- Low block error rate, no correlated failures, no bathtub curve -- which implicitly assumes disks are burned-in elsewhere, replaced regularly, and swapped out after early failures

**- Small document size relative to error rate:**

***formula for doc size, error rate, and copies?***

# Example: Amazon Glacier…

[Refactor Glacier blog post, in light of simulation approach]

# How does auditing help?

Compare auditing & repair strategies

Floor on half-life employs auditing

Auditing is worth the cost of XX additional copies.

# How concerned you should be for institutional failure?

**- If you’re risk tolerance for block level failure is X -- you should store in at least Y institutions**

**- If you’re willing to pay X for an additional copy, you should be willing to pay Y to have them institutionally diverse**

# Modeling Other Choices

- Correlated shelf failure

- File formats

- for bit-level concerns, file format affects the ability to repair failure

- Assume N-repairability

- only damages 1/nth -- can repair as long as another doc exists with that portion

- can repair based on smaller blocks

- smaller possibility of failure of simultaneous blocks

- shorter repair time

- roughly equivalent to using smaller doc-size, except for the case of

- random audits -- which will have larger blocks

- Compression

- Affects overall storage size/costs, doc size, repairability of format

- Assuming format is N-repairable, compress is M reduction, cost of copies is K \* cost of related storage. When is compression a win in terms of K,M,N ?

- Encryption

- Loss of keys -> loss of entire content

- Reduce loss from encryption to level based on other choices…

- non-intentional: how many copies of keys?

- insider/outsider attack: auditing of process, auditing of content with decryption

# Summary