Optimal Data Protection - Security, Replication and Archiving in Storage Area Networks

Rob Peglar

Vice President, Technology

Xiotech Corporation

Less-than-Optimal Storage Security

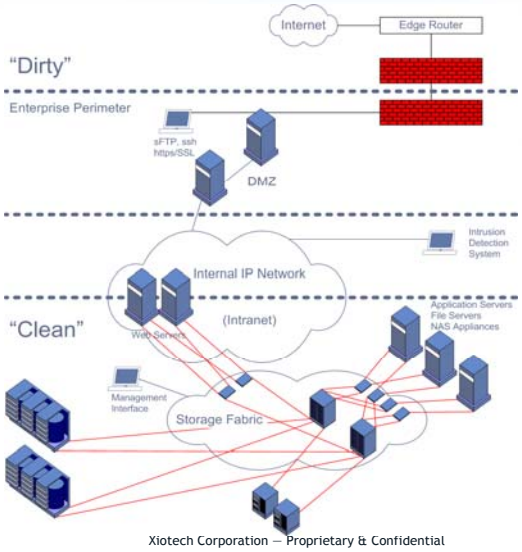
- Well known bank lost data tapes in Singapore, resulting in $500M fine from SEC
- A different well known bank lost data tapes containing credit card information on all U.S. Government employees
- Healthcare processor exposed records to unauthorized people, litigation pending.
- A financial institution exposes 2600 customer email addresses; each account credited £50 ($96.18 USD)
- A "Banking consultant's system stolen from a shopping mall in Southern CA, exposed thousands of customer accounts; all customers had to be notified within 48 hours"
- Japanese BB leaked subscriber data, accidentally; 500 yen ($4.79 USD) vouchers were sent to all of its 4.5 million subscribers"
- Lost disks at Los Alamos National Laboratory closes down operations; UC contract placed in jeopardy
- Replaced disk went on junk pile for scrap sale, still containing client credit card data; loss of reputation to storage vendor and costs to credit card company

From "A Practical Approach to Storage Security", SNIA 2007

Xiotech

What technically changed about storage?

- Glass house
- Distributed Technology
- Traditional Security
- Source Status
  - Dirty
  - Clean
- Storage on the Net
- Vulnerabilities
  - Access
  - Components

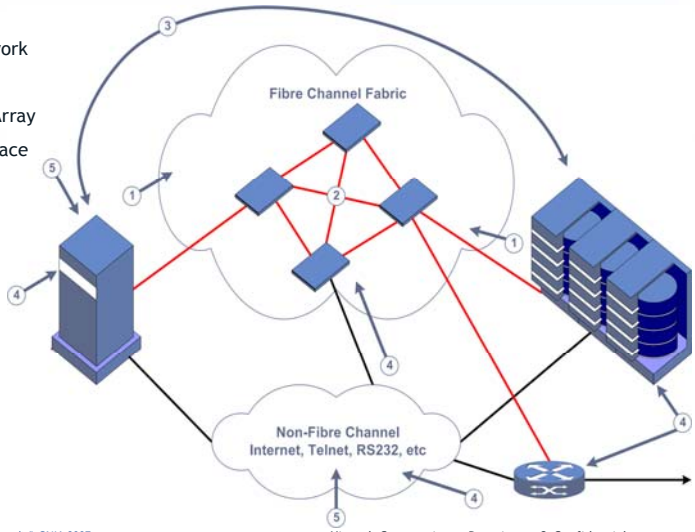


From "A Practical Approach to Storage Security", SNIA 2007

Xiotech

Storage Threats

1. End device to network
2. Switch to Switch
3. Server to Storage Array
4. Management Interface
5. Denial of Service
   Hijacking
   Man-in-middle
   Spoofing



From "A Practical Approach to Storage Security",,SNIA 2007

Security is a People-based Problem

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

…it is far more effective to think of security as an ongoing process of "risk management" that includes not just protection, but also detection and reaction mechanisms

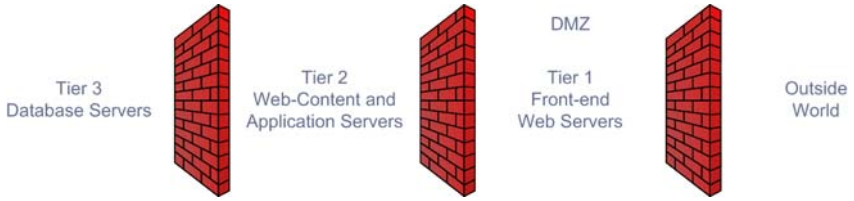
Bruce Schneier, *Secrets & Lies*

From "A Practical Approach to Storage Security", SNIA 2007

Xiotech

Typical Data Security Strategies

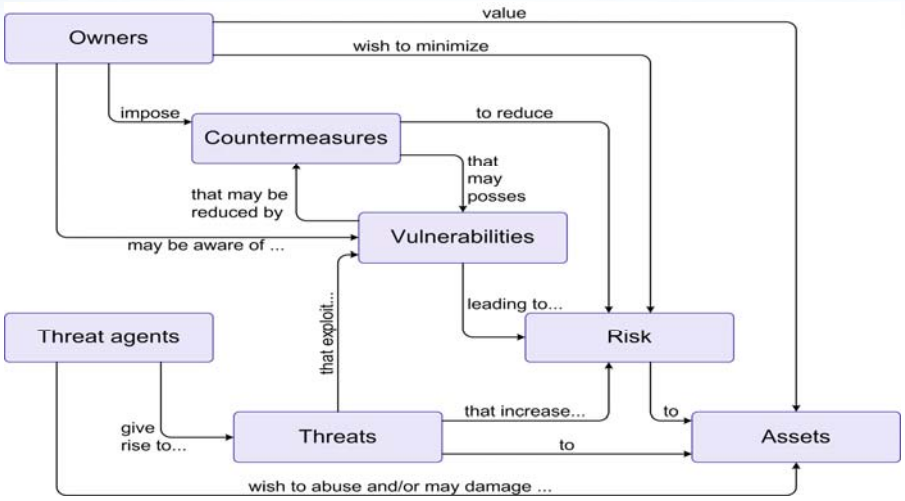
- Security by Obscurity Strategy
  - Basic premise is stealth / hiding
- The Perimeter Defense Strategy
  - More of a concentrated effort in defense
  - Defense between "insiders" and "outsiders"
- Defense in Depth Strategy (Recommended)
  - Employs a number of operationally interoperable and complementary technical and non-technical layers of defense
  - May use enclaves for stronger regions of defense



From "A Practical Approach to Storage Security", SNIA 2007

Xiotech

Defining value of a secure infrastructure



From "A Practical Approach to Storage Security", SNIA 2007

Xiotech

Data Security via Replication

Local Replication

- Local replication, mirroring
  - Within and across Storage Tiers
  - Within and across RAID types
  - Non-disruptive swap to new image
  - Replication pause / resume capability

Geographic Replication

- Remote replication, mirroring
  - Within and across Storage Tiers
  - Within and across RAID types
  - Non-disruptive virtual link to new image
  - Replication pause / resume capability

Continuous Data Protection

- Resilient, easy-to-use, scalable, out-of-band data protection for business continuity
  - Continuous Data Protection (CDP)
  - Synchronous
  - Asynchronous
  - Heterogeneous

Geographic RAID

- Automatic data protection and replication across geographically dispersed locations (up to 10 Km) from a single SAN system

Xiotech

Data Protection and Recovery Planning

- Planning Parameters
  - Physical Plant
  - Communications infrastructure
  - Bandwidth
  - Latency
  - Security
  - Expertise
- Protection and Recovery Alternatives
  - System-based replication
  - Cross-system replication across distance
  - Continuous data protection (CDP)
  - Replication service

Xiotech

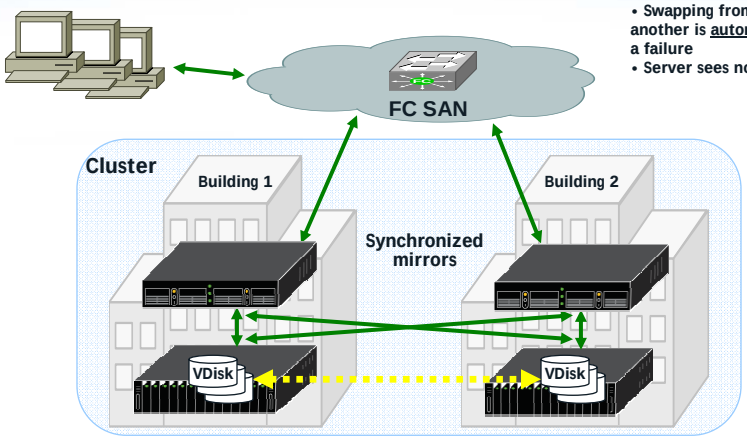
Disaster Recovery Alternatives

	Backup	Remote Backup	Information Recovery	Cold DR Site	Hot DR Site
Solutions	▪ Disk-to-Tape (D2T) ▪ Disk-to-Disk (D2D)	▪ Tape Vaulting (TV) ▪ Backup over Network (BSPN)	Replication Services to Managed Storage Ctr.	Replication to Remote Idle Site	Replication to Remote Site with servers active
Time / Labor Requirements					
For Recovery	▪ High to Moderate	▪ High to Moderate	▪ Moderate	▪ Moderate*	▪ Low*
Backup/ Replication	▪ High to Moderate	▪ High to Moderate	▪ Low	▪ Moderate*	▪ Moderate*
Recovery Attributes					
RTO - Recovery Time from Disaster Event	▪ D2T - Slow ▪ D2D - Fast	▪ TV - Very Slow ▪ BSPN - Moderate	▪ Moderate to Fast	▪ Moderate to Fast	▪ Fastest
RPO - Data Lost Between Backups	▪ High Risk	▪ Moderate Risk	▪ Low Risk	▪ Low Risk	▪ Low Risk
Risk of Data Loss	▪ High Risk	▪ Moderate Risk	▪ Low Risk	▪ Low Risk	▪ Low Risk
Costs					
Capital Costs	▪ $$/GB*	▪ $$/GB*	▪ $/GB*	▪ $$$/GB*	▪ $$$/GB*
Monthly Costs	▪ $$/GB*	▪ $$/GB*	▪ $$/GB*	▪ $$$/GB*	▪ $$$/GB*

Recovery Time ∞ ⟵ 0

Xiotech

Geographic RAID



- Swapping from one mirror to another is automatic in case of a failure
- Server sees no interruption

- Both controllers and drive bays are part of the same cluster

Xiotech

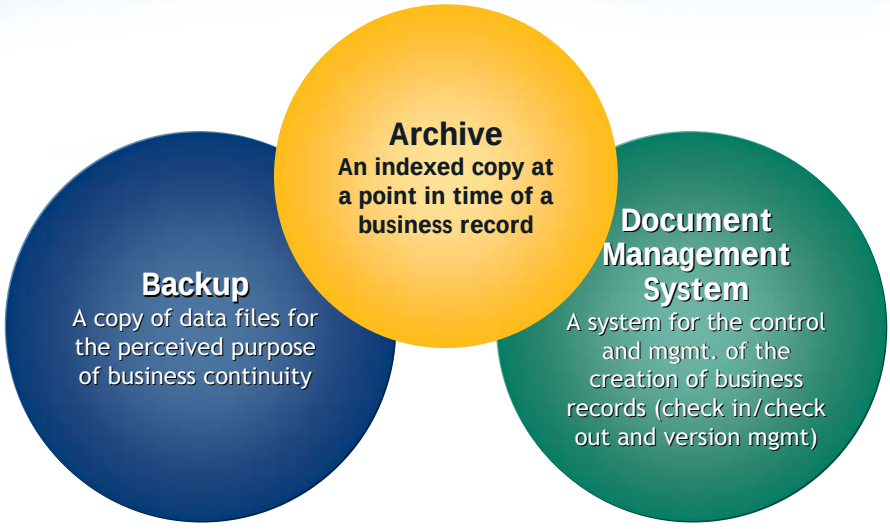
Data Replication Strategy

Why Replicate?

- Critical data requires more than just off-site tape backups
- Restoring from tape in the event of a disaster is not "good" enough
- Remote replication allows for a "piece of mind" knowing that your data is off-site, safe and recoverable
- Managing data replication requires time and companies are being asked to do more with less
- Data replication expertise is hard to find

Xiotech

What is Archive?



Xiotech

What about Backup Tapes?

- Tape is Expensive
  - Not the media itself – but everything around it
  - Drives, Libraries, and the killer expense ---
  - SOFTWARE and its care and feeding (i.e. people)
    - Backup/restore software
    - Tape drive OS drivers
    - Tape drive firmware
    - Tape library management software
    - Patches and maintenance to all the above
- Tape is Not an Archive
  - Tape holds a transformed copy of the data
    - To restore it, you must un-transform it
  - Tape cannot be directly content-searched
    - To search content on tape, you must first restore it to disk
- A backed-up file is equivalent to a photocopy in another language
- A tape cartridge is equivalent to a banker's box
- **Neither are an archive**

Accessing Data over the Long Term

- 74% said the #1 information management challenge is *improving employee or trusted user access to information*
  - Information Security, 2007 Priorities Survey, n=453 IT security professionals
  - That response was #1 – above strengthening endpoint security, better leveraging AD or other directory services, deploying stronger authentication, or deploying VPNs to remote users
- >50% of on-premise stored content is fixed from day one
  - ESG, December 2005
- 40% said the #1 information security challenge is *improving the detection of internal information attacks*
- 34% said the #1 regulatory compliance challenge is *auditing user access and user reviewing privileges*
  - Higher than encrypting information transmission
- *Change the nature of the stored information*
  - Because you may not be able to change the nature of the people

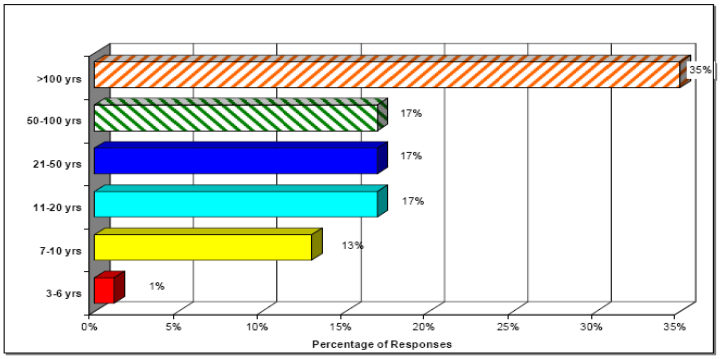
Power and Cooling – the Hidden Security Risk

- 50% said their own datacenter *will not have sufficient power and cooling capacity/capability by 2008*
  - Gartner DataCenter Conference, November 2006, n=575, CIO/IT directors
- Datacenters are designing today for 30KW/rack
  - That is 150 A @ 208 V *per rack*
  - *Average today is 6,800 W/rack – six years ago, it was 1,000W/rack*
- Power/cooling will be 33% of the average total IT budget in 2008
  - Robert Francis Group, December 2006
- 4 years of power to a $3K server *costs more than the server itself*
  - Luis Andre Barroso, chief server architect, Google
- By 2010, every $1 spent on hardware requires 70 cents of power/cooling
  - IDC, December 2006 – compare to 50 cents in 2005 and 21 cents in 2000
- *Change the location of the stored information*
  - Because you may not be able to store it on-premise

Xiotech

What is Long-Term?

What does Long-Term Mean?



SNIA Data Management Forum

Source: SNIA - 100Yr Archive Reqmts Survey, Nov, 2006

Xiotech

Preservation is Complex

- Technology Challenges
  - Maintaining Physical readability
  - Maintaining Logical readability
  - Migration of large repositories
  - Emulation of formats
  - Maintenance of historical readers and applications
  - Protection from change
  - Protection from loss or damage
  - Physical & logical Security
  - Automation
  - Deletion & Purging
  - Search – Discovery
  - Testing/Auditing
- Operations Challenges
  - Collaboration on requirements
  - Setting requirements
  - Classification
  - Establishing adequate Metadata
  - Standardizing practices
  - Finding value in the archives

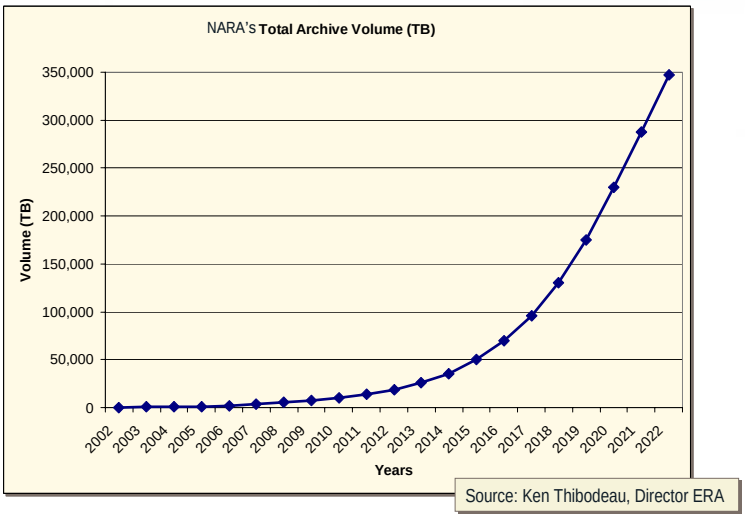
Digital Preservation requires not only the maintenance and disaster recovery procedures needed for securing the media and its contents but also strategies and procedures to maintain its accessibility and authenticity over time.

-- JISC, 2002

Xiotech

Projected Storage Volumes: Permanent Electronic Records

NARA's Archive Problem



Source: Ken Thibodeau, Director ERA

Xiotech

Peer Recommendations

ORGANIZATIONAL

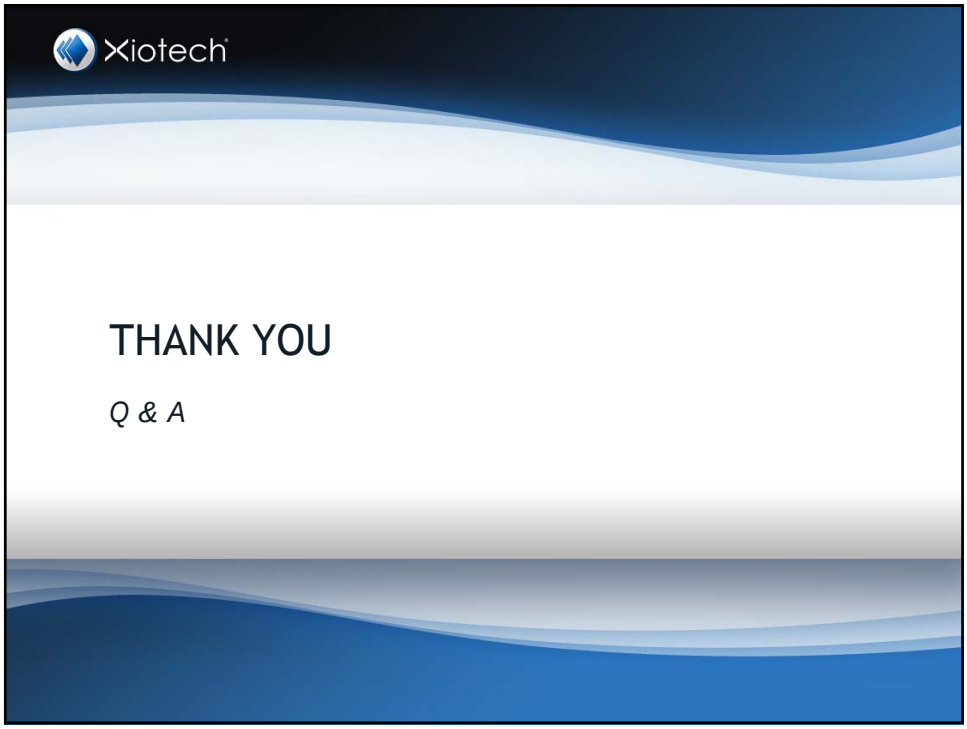
- "Get RIM and IT at the same table. Create a relationship. Both need to be included up front to develop solutions that will work on both sides."
- "Remember that IT doesn't own the information. RIM, Legal, Business units and IT all have a part to play in the decisions applied to business records and should be sitting down at the table together."

TECHNICAL

- "Metadata is important, and it's better to implement the metadata at the front end rather than populating the metadata after the record has been saved into the repository."
- "Stay with industry standards"
- "…use mass storage devices, not optical media "

OTHER GUIDANCE

- "Prayer "
- "Stay with paper? (just kidding)"


Xiotech
THANK YOU
Q & A