



Securing Data in Storage

The Anatomy of an Attack
The Architecture of Defense

October 2003

DECURU

Agenda

- Introduction
- Networked Storage Overview
- NAS vulnerabilities
- SAN vulnerabilities
- Conclusions



Introduction

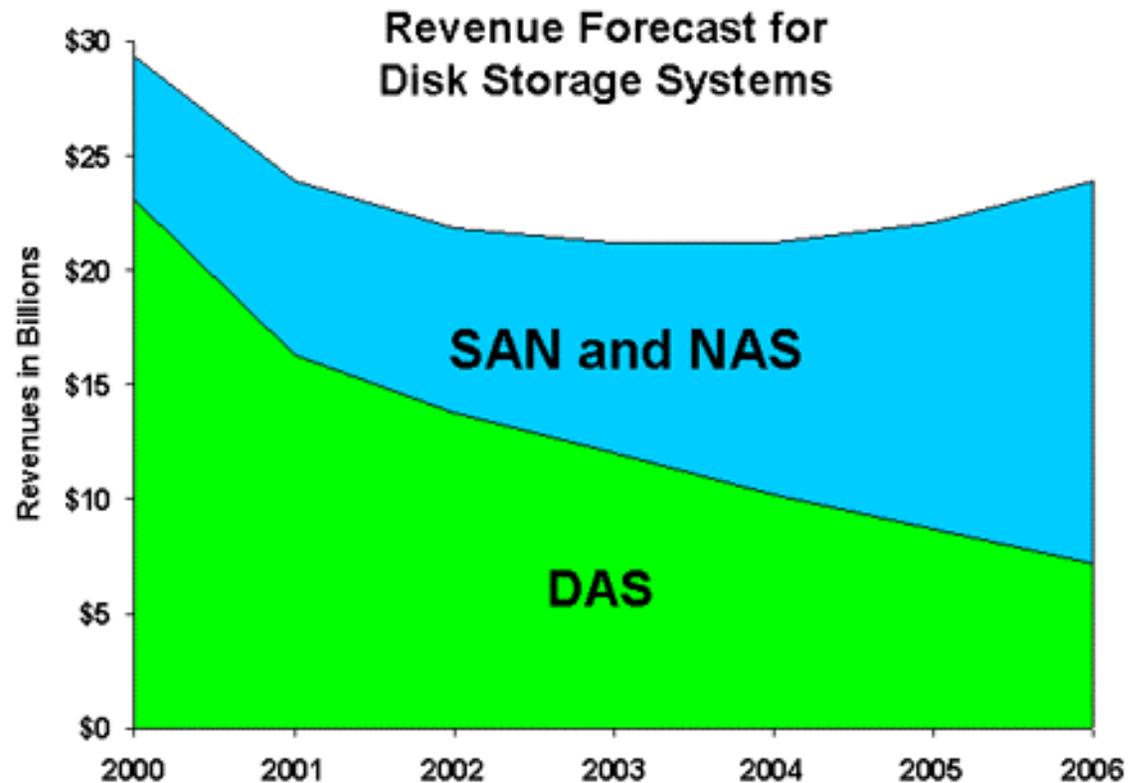
Data Security: A Harsh Environment

History Repeating

- Ethernet circa 1990
 - No perimeter defense
 - No practical encryption/VPNs
 - Limited access controls
 - No auditing
- Networked storage today
 - No defense in depth
 - No encryption
 - Limited access controls
 - Limited auditing

Networked Storage Adoption

Eliminates Traditional Compartmentalization of DAS



Source: Gartner Dataquest, 8/02

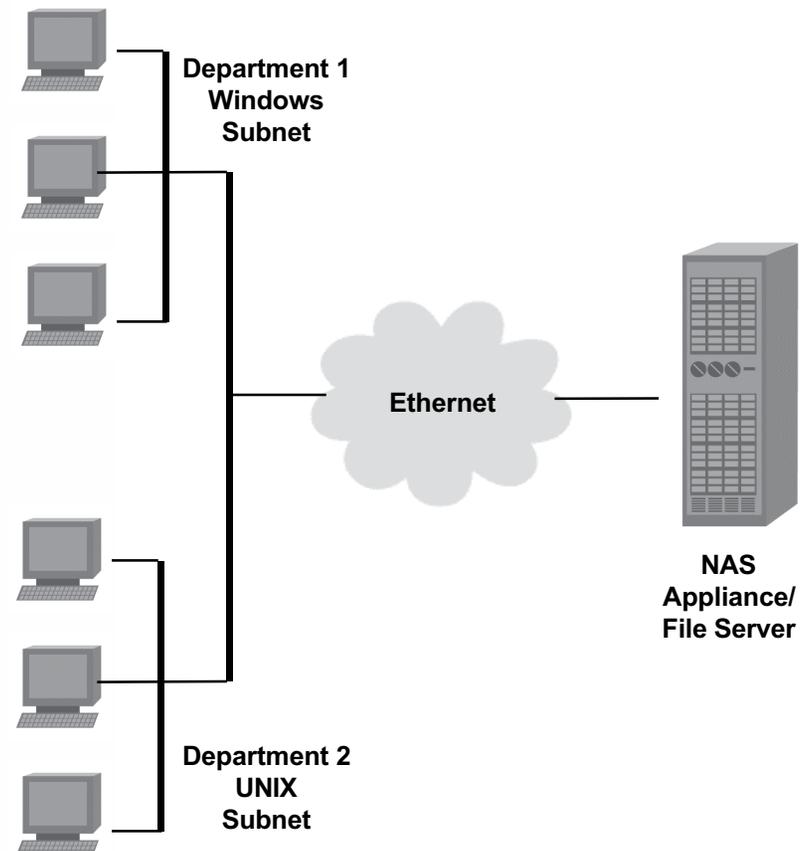
Networked Storage Advantages

- More efficient utilization of storage resources
- Centralized management and backup
- Improved performance and access to data
- Consolidated disaster recovery
- Improved scalability

Note: Improved security is not a driving factor!

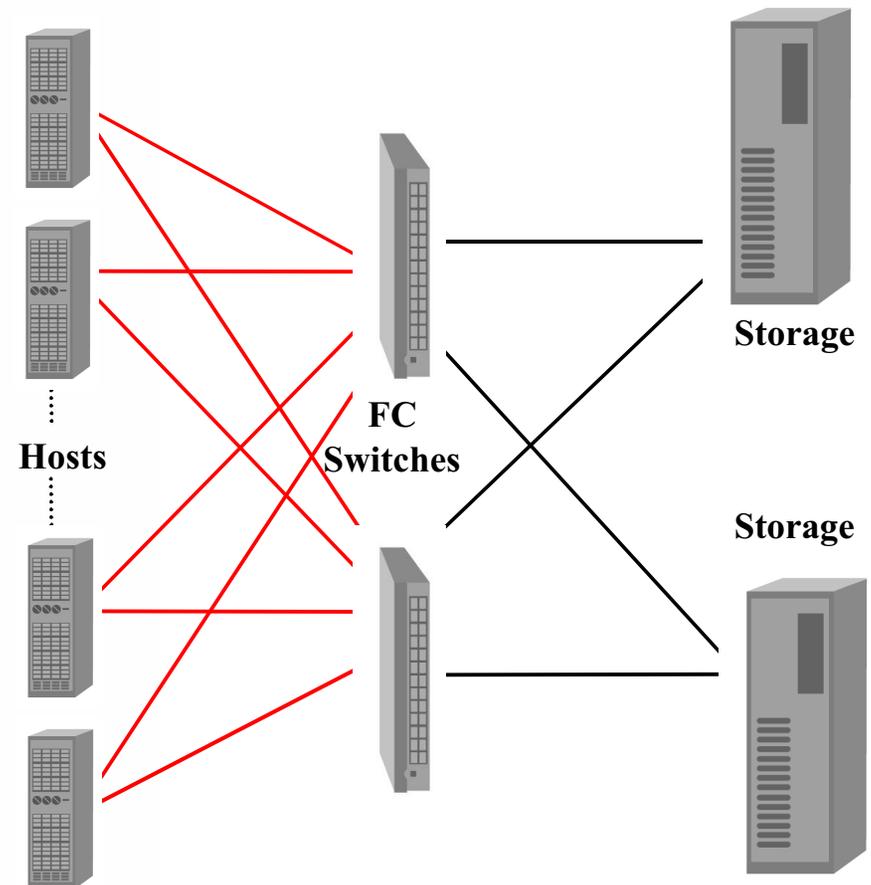
Network Attached Storage (NAS)

- High density NAS appliances enable centralized storage and file sharing
- Typically connected via gigabit Ethernet
- Frequently serve heterogeneous environments



Fibre Channel SANs

Storage Area Networks (SANs) are a network architecture designed for high availability, high performance data access and storage





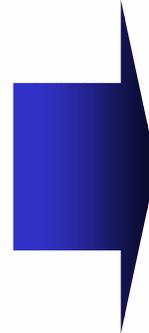
Networked Storage

A Rich Target

DECRO

Digital assets at risk

- Sensitive/regulated data
 - Customer data
 - Financial transactions
 - Patient data
 - Intellectual property
 - Corporate financial records
 - Legal files
 - Human Resources data



As storage becomes more aggregated, a single breach can expose terabytes

- Dec 2002 - TriWest Healthcare
 - Stolen disks contained medical records on 500,000 military personnel
- Jan 2003 – IBM Global Services
 - Notifies customer, Co-operators Life Insurance, that a disk containing personal and financial information on its customers is missing, presumed stolen.
- Feb 2003 – Visa, Amex, Mastercard
 - Hacker breaches 8 million credit card accounts through a third-party processor
- May 2003 – Coca-Cola Inc.
 - Unauthorized employee downloaded salary information and Social Security numbers of about 450 co-workers, leading the company to warn employees to check their bank accounts and credit cards.
- August 2003 – Acxiom Corp.
 - A computer hacker gained access to private files at Acxiom Corp., one of the world's largest consumer database companies, and was able to download sensitive information about some customers of the company's clients.



But I have Firewalls...

Spending Mismatch

- Organizations are rapidly building networked storage and aggregating data
- Security is an afterthought
- Spending mismatch:
 - Security spending today focused on network and perimeter
 - Highest exposure: terabytes of poorly secured storage

**Security
Investment**



**Actual
Exposure**



Insider Threat

- 50-80% of electronic attacks originate inside the firewall
- 67% of companies reported internal breaches in last 12 months
- Average loss from breach of proprietary data was \$2.7 million

Source: FBI/Computer Security Institute

Insider Threat

- Hostile insiders are far more dangerous than external hackers & script kiddies
 - They know what's valuable, and where it lives
 - Familiar with existing security systems
 - Months or years to watch and plan
 - Physical access to machines, networks, storage
 - Ample opportunities for social engineering
- Perimeter holes give insider access to outsiders
 - VPNs, partner networks, contractors

Accelerating need for storage security...

- As storage becomes more aggregated and networked, a single breach can expose terabytes
- Perimeter security insufficient as threats evolve
- Growing vulnerability of storage systems:
 - Administrator and “root” privileges in the network
 - Human error, theft or misuse of ID/credentials
 - OS & application exploits, viruses
 - SAN vulnerabilities, arrival of iSCSI
 - Physical security of disks (repair, theft, disposal)
 - Replication and offsite backup multiply risks



Networked Storage Vulnerabilities

Data Stored in Cleartext

- Storage devices lack integrated security capabilities
- Without encryption, no effective method to compartmentalize data in shared storage
- Disk/tape: small, portable, contain GBs of data and are easy to steal
- Disk repair and disposal: even “wiped” drives can still yield information

Offsite Backup and Disaster Recovery Increases Risk

- Data duplication significantly increases exposure and risk
- Loss of physical control increases chance of media loss or theft
- Outsourcing = subcontractors with access to your sensitive data

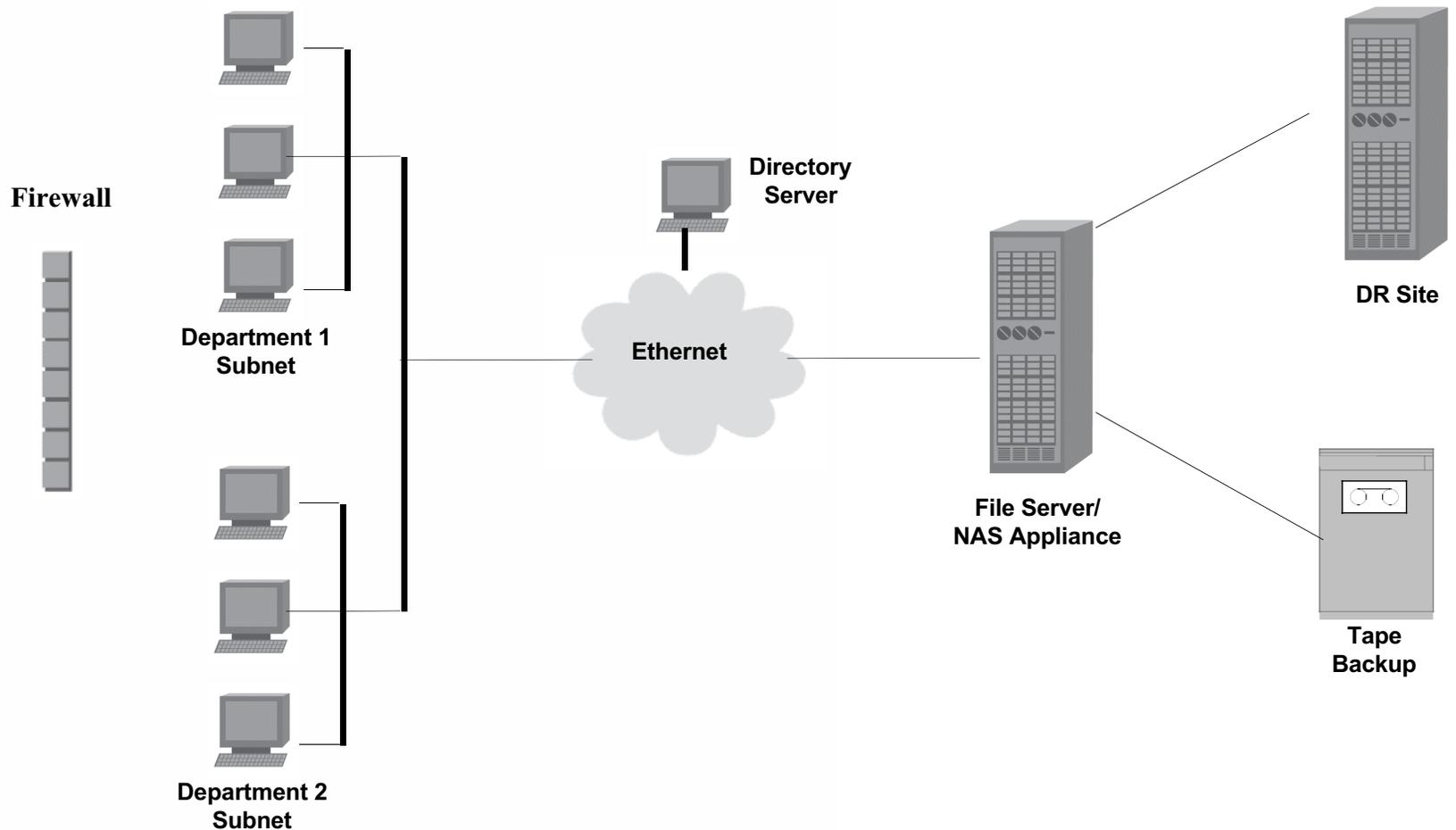
Limited Access Controls

- Unlimited access points
- No security barriers/firewalls
- Storage administrator has unlimited access to data
- System administrator can abuse privileges to access sensitive data and cover their tracks
- No defense in depth for storage: single breach gets you everything

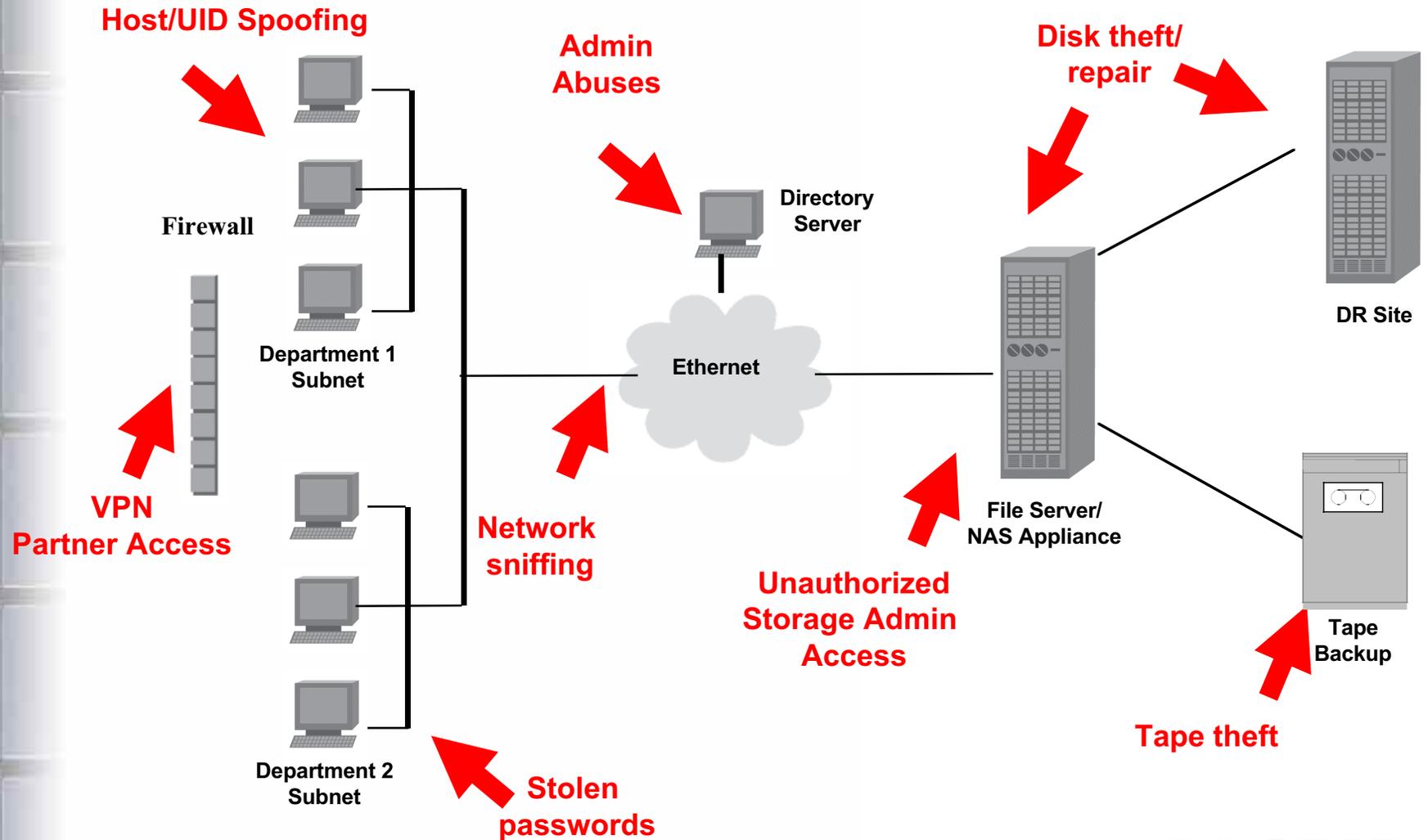
Limited Auditing

- No deterrent: Nobody is watching storage
- Administrator and “root” privileges in the network give insiders free rein
- Limited methods for capturing IT insider attacks on storage
 - Add name to secure group
 - Grant access
 - Read classified/sensitive docs
 - Erase footsteps
- Difficult to determine if logs have been manipulated or deleted

Typical NAS Infrastructure



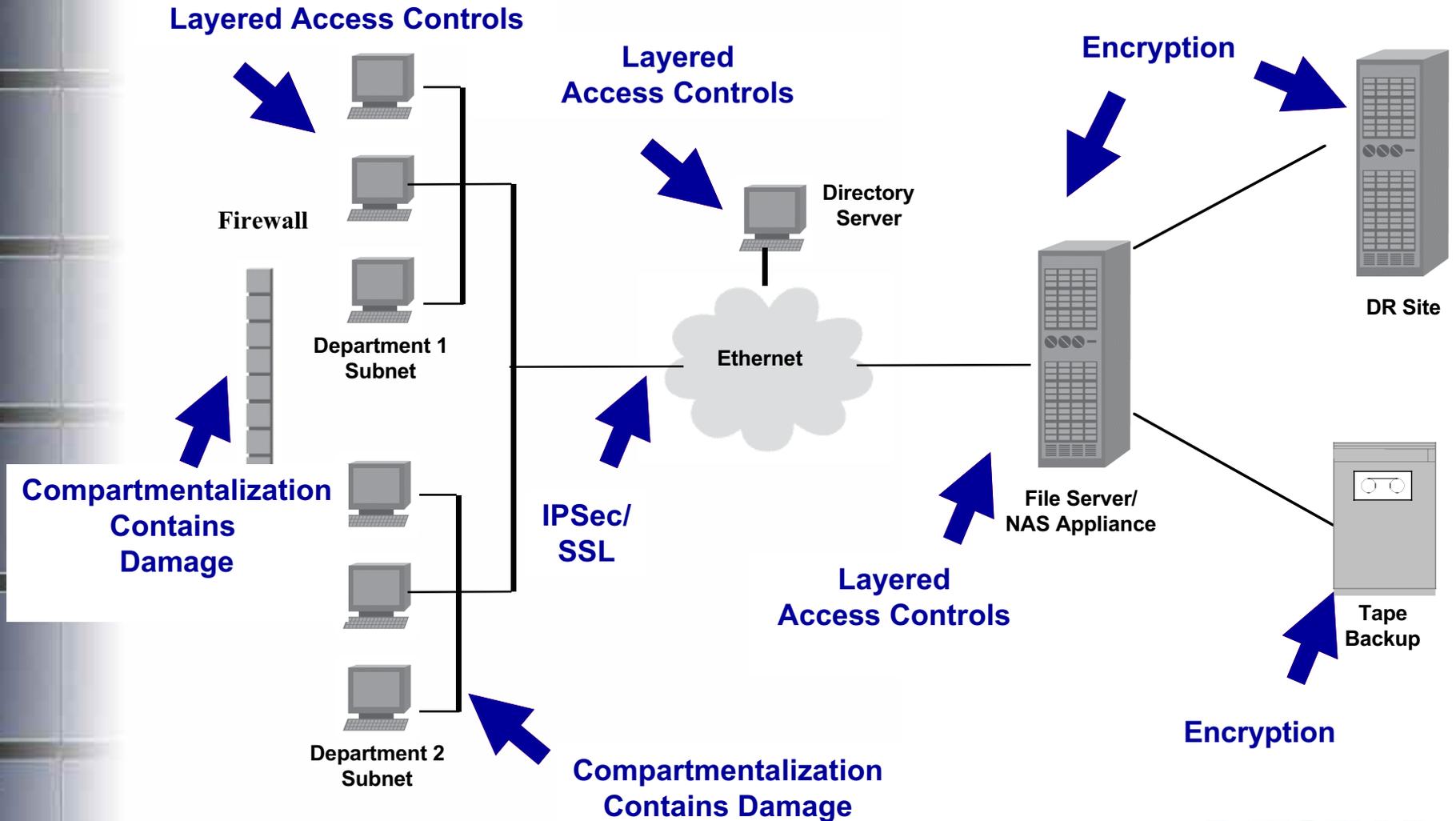
NAS Threats





SAN Vulnerabilities

Threat Mitigation



SANs are Changing

- **Historically:**
 - Originally intended to exist as a standalone, “trusted” network
 - Physical security thought to be “good enough”
 - Single administrator
 - Few individuals with SAN expertise
- **Today**
 - Connect hundreds (not dozens) of hosts and storage devices
 - FC increasingly serving IP networks
 - Co-mingling of sensitive and non-sensitive data
 - Multiple administrators

SAN Security Weaknesses

- FC SAN designed as a trusted network, so security was not built in
- Primary function of zoning/LUN masking was for ease of administration, not for security
- Complexity leads to administrative errors or misconfiguration, which can expose terabytes of data
- No authentication for hosts paves way for spoofing attacks
- Increasing number of people with SAN knowledge

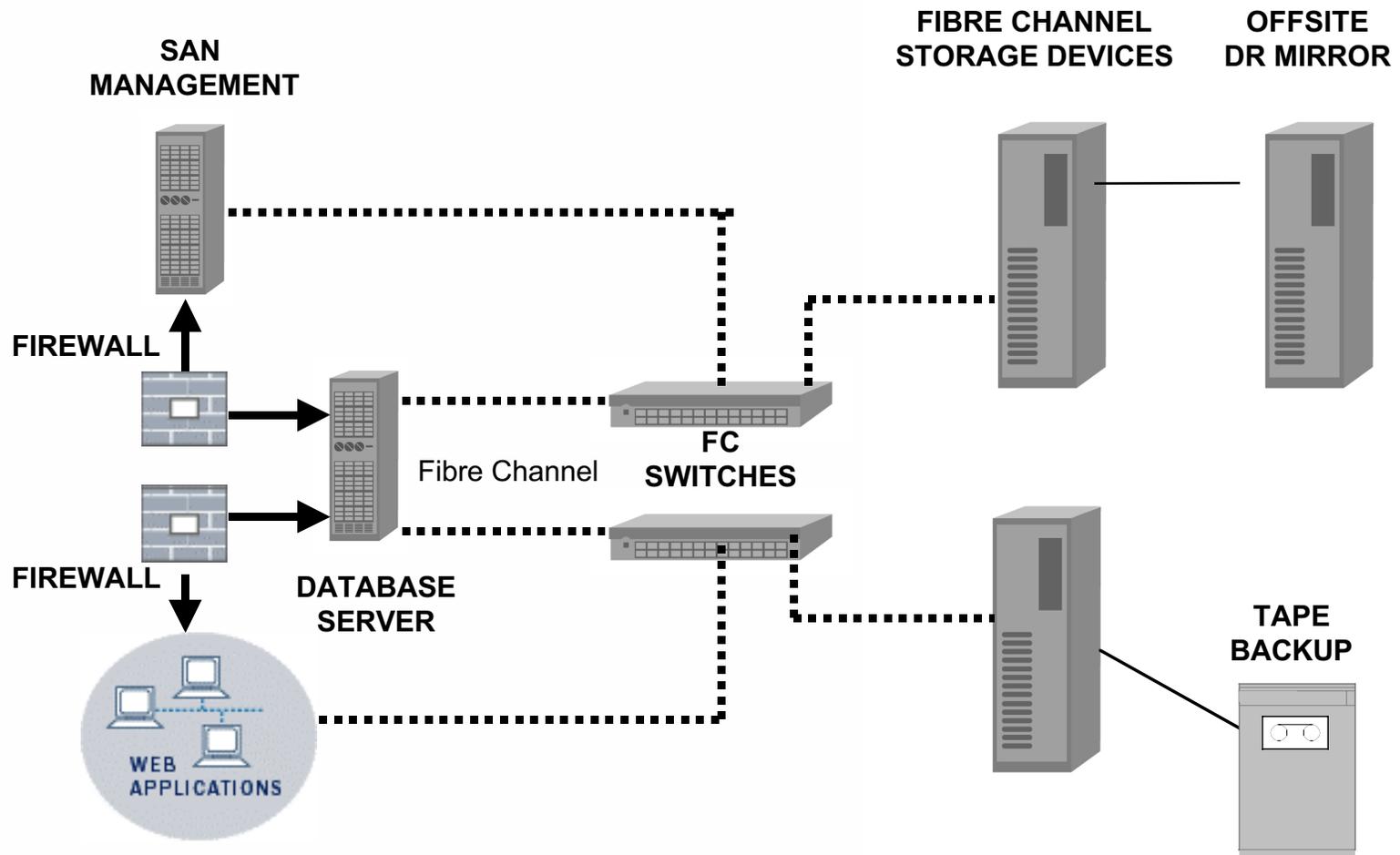
Management Interfaces are Vulnerable

- FC specs include in band management functionality:
 - Zone configuration
 - Unrestricted SNS access
 - Time service
 - Key distribution service
- Authentication is not required
- Illegitimate access to management services could render standard access controls ineffective

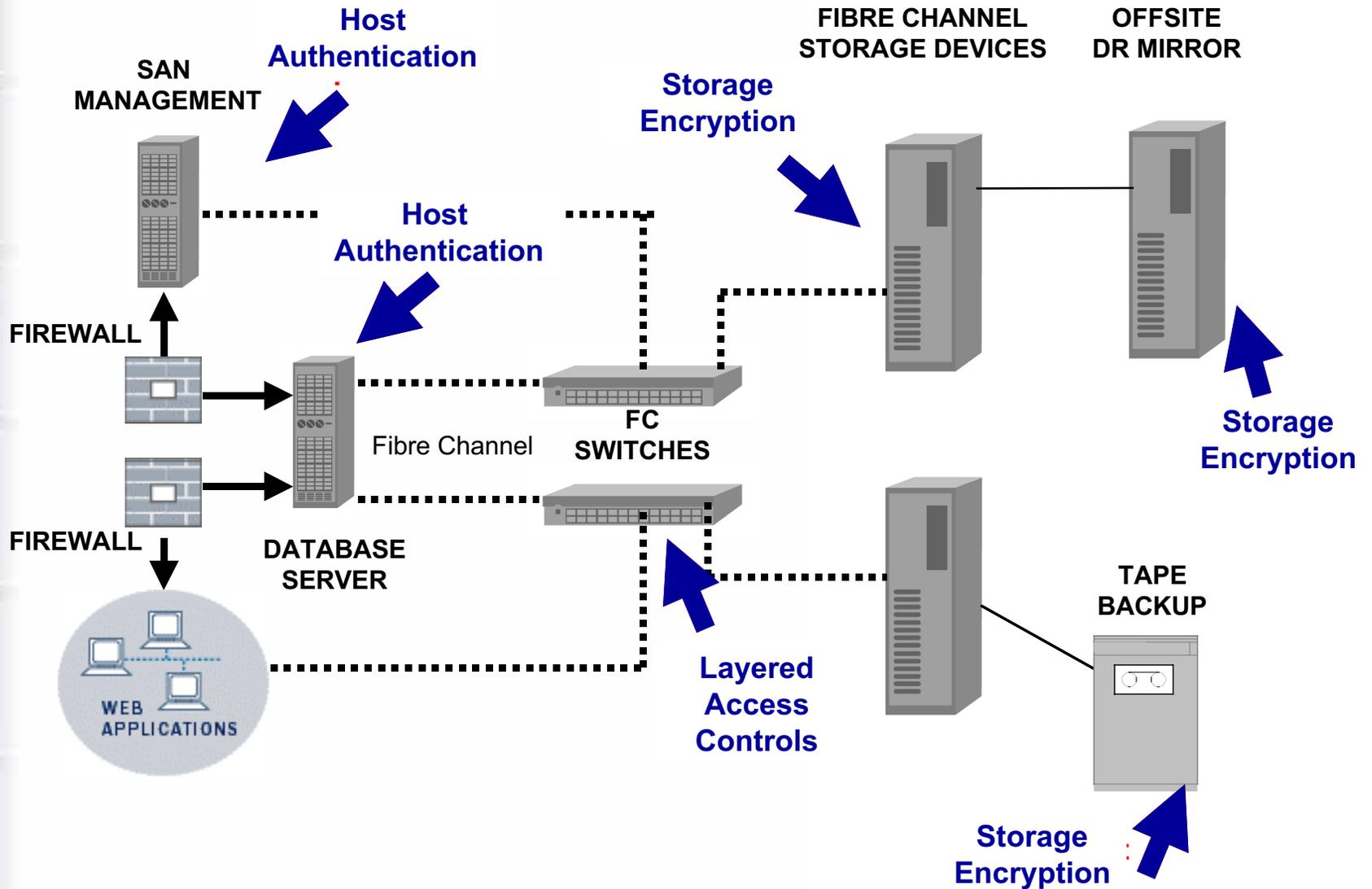
Risks of Physical Access

- Plug into a port and get access to everything
- Savvy attacker with the right tools on the host can breach everything
- Avoid zone restrictions by changing ports
- Drive/tape removal: all data is in cleartext

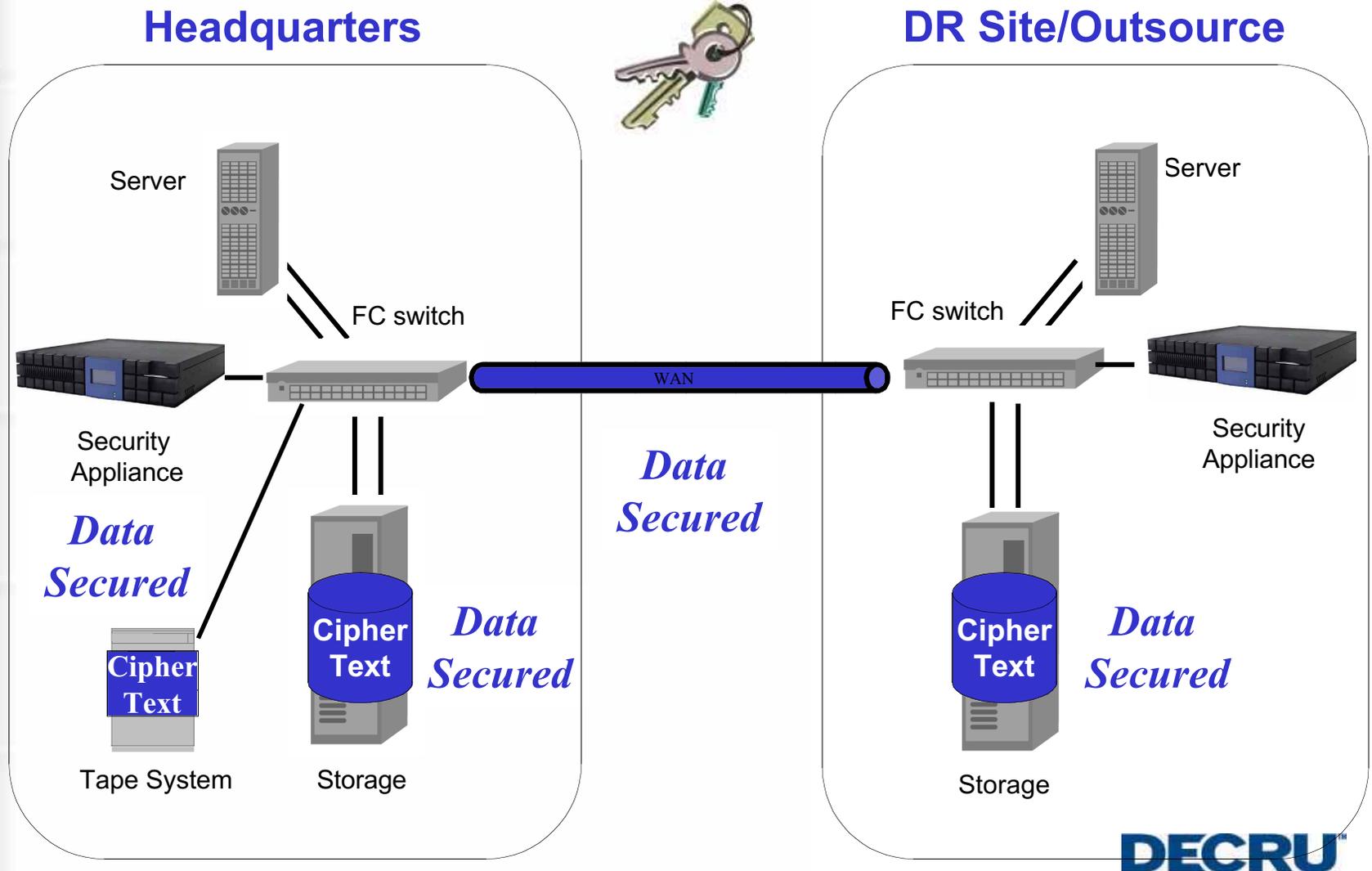
Typical SAN Infrastructure



SAN Threats



Securing DR: A Closer Look





Building Defense in Depth

Encrypting Data

- Creates a security model for lifecycle of data
- Enables effective compartmentalization
- With encryption, the default state of data is secure: all replicated copies are secure in flight and at rest.
- Facilitates role-based storage management
- Locks all “backdoor” access to stored data

Encryption Considerations

- **Strong encryption**
 - Standard algorithms
 - Large key space
- **Key management**
 - Ease of administration
 - Archival and recovery
- **Performance**
 - Low latency
 - Hardware acceleration
- **Data availability**
 - Clustering and failover
 - Methods of decryption

Layered Access Controls

- SAN host authentication
- Two factor authentication for sensitive operations
- Group review of administrative actions
 - Unauthorized access requires collusion
- Role separation
 - Storage admin provisions storage, but has no data access

Logging and Auditing

- Maintain several sources for logging data access and administrative events
- Auditing provides a level of deterrence
- Provides evidence of unauthorized access

Building Defense in Depth

Attack	Countermeasures
Unauthorized admin access	Encryption, ACLs, secure logging
Hostile admin adds user, changes passwords	Secondary authentication, secure logging, 2-step authorization
Stolen passwords	Compartmentalization limits damage
Network sniffing	Implement IPSec between clients/hosts and storage
UserID spoofing	IP range ACLs, IPSec authentication
WWN Spoofing	SAN Host Authentication
Disk theft/repair	Encryption of all data "at rest"
DR/Mirror attacks	Original copy of data is encrypted, providing transmission security



Conclusions

Data is Increasingly Persistent

- Regulations requiring data storage timeframes
 - HIPAA: worldwide capacity of compliant healthcare records will increase from 68PB in 2003 to 238PB in 2006 (Source: ESG)
 - Sec17a-4: Trading account records -- end of account plus 6 years
- Continued growth of reference data
 - (92% CAGR, 2001-2005)
 - Larger file sizes
 - Kept for decades, not months

Regulatory Pressure: GLBA

Financial Institutions, Insurance, Banking



Gramm-Leach-Bliley Act (July 2001)

“... each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the **security** and **confidentiality** of those customers' nonpublic personal information.” [15 U.S.C. § 6801(a)]

Institutions must develop safeguards:

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against **any anticipated threats or hazards** to the security or integrity of such records; and
- (3) to **protect against unauthorized access** to or use of such records or information which could result in substantial harm or inconvenience to any customer. [15 U.S.C. § 6801(b)]

Regulatory Pressure: HIPAA Healthcare & Pharma



Sec. 164.306 Security Standards

- “Covered entities must:
 - ensure the confidentiality, integrity and availability of all electronic protected health information they create, receive, maintain, or transmit
 - protect against **any reasonably anticipated threats** to the security or integrity of such information
 - protect against **any reasonably anticipated uses** or disclosures of such information that are not permitted
 - ensure compliance with these rules by their workforce (officers and employees)”

Regulatory Pressure: SB1386

All Businesses Operating in California



*California's Database Security Breach Notification Act
(Effective July 1, 2003)*

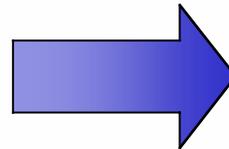
SEC. 2. Section 1798.29 is added to the Civil Code:

“(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person. “

Secure by Default

Considering the myriad threats to data, why not make the default state of data *secure*?

CUSTOMER	SSN	AMT
John Magnus	544-89-3021	\$304.31
Susan Wong	522-35-1105	\$91.05
Ken Hernandez	670-32-1145	\$21.88
Alicia Sparr	435-98-0498	\$209.95
M.J. Satyr	594-22-9038	\$76.55
Dan Spencer	543-09-3451	\$413.03
Mary Jones	495-38-8971	\$90.74
Jerome White	613-98-8932	\$247.11
Martin Ng	339-77-9201	\$20.89
Fay Dunlap	784-29-6290	\$401.92
Takeshi Doi	544-09-3193	\$29.01
Sarah Fisher	432-92-7105	\$142.28
Ingrid Parker	595-29-7406	\$102.48



```
DYHY^C^@^@^@~] <F2> ^?  
z<B2>0 ^N<E4>q<91><CD>x1<CB>^A^@^@^@  
^\<84>1 <92><F6>^Cq<89><90><CF><9C>  
<D9>1#<F6><8E><C1><CF><86><DA>B<EB>  
<F7>A.\<AD><CF><F0><D2>-<CA><C3><DA>  
<8E><F1><B7>^C^L<EE><E5><9E><A4><9E>  
_ ^W<CE><AD><BB>2<95>`<D3>E^T1<8D>  
<A7>^<CD><93><A6>/<F5><AC><DF>s<88>  
<87>,<F3>"=<F2>:P;<F3><B1><9F><82>  
<97>^Q<BA><ED>o<AF><C5><DF>u"6,Q^D  
<A7><B9>o1<87>\ 8<D3><B6><8D>k<9D><A8>  
)9^^A^Q)<F0><FE>-<C0><FB>^LI<82><DB>  
<E0><C8><D9>a<8E>W<BB><88>q<CC><C0>+  
^B^L<FA><DA><DD><E3><A5>O^O<D7>T7<9
```