SNIA

STORAGE NETWORKING INDUSTRY ASSOCIATION

EDUCATION

Introduction to Storage Security

Gordon Arnold, IBM

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced without modification
  - The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.

Abstract

Introduction to Storage Security

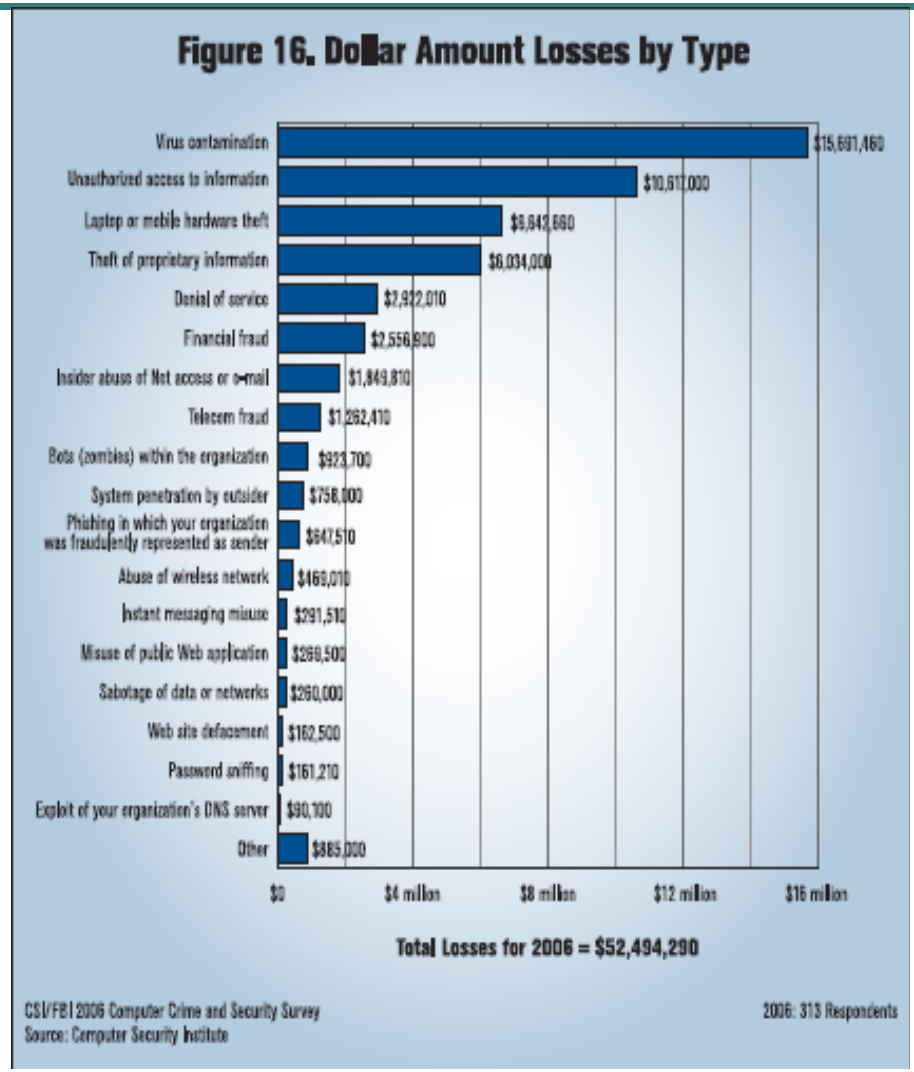
Many enterprises face the task of implementing data protection and data security measures to meet a wide range of legal, regulator, and/or due diligence requirements. Increasingly, these requirements are being applied to the storage layer, so it is important to understand the areas of most risk. In addition, understanding the differences between compliance and securing the data can be critical when information systems (IS) auditors are inspecting the storage ecosystem, looking for things like accountability, traceability, and proofs of encryption and destruction.

Objectives

- This session lays a foundation for you to better understand storage security risks, and their mitigation strategies. We will examine common security mistakes and challenges, including encryption and its impacts on disaster recovery and business continuity. Finally, we will provide specific recommendations and offer insights into emerging storage security measures.
- After completing this tutorial, you should be able to:
  - Know storage security measures in response to risk and threat
  - Understand storage security technologies including encryption, logging, and key management
  - Understand the upfront and continuing effort required to secure the storage layer

Introduction

- Security incidents are increasing
- Security is a business problem
- Storage is not immune
- Security and storage people have similar concerns and process
  - The capability of a system to fulfill its mission in a timely manner, despite attaches, failures or accidents

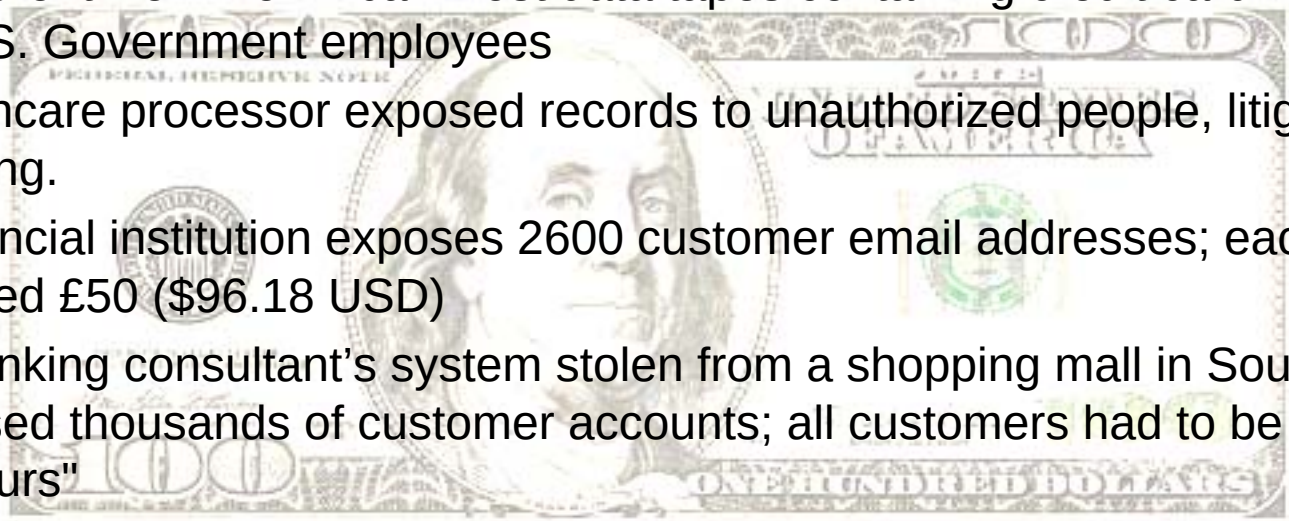


What are business drivers for storage and data security?

- Theft Prevention
- Prevention of Unauthorized Disclosure
- Prevention of Data Tampering
- Prevention of Accidental Corruption/Destruction
- Accountability
- Authenticity
- Verifiable Transactions
- Service Continuity
- Regulatory and Legal Compliance

Not an effective strategy…

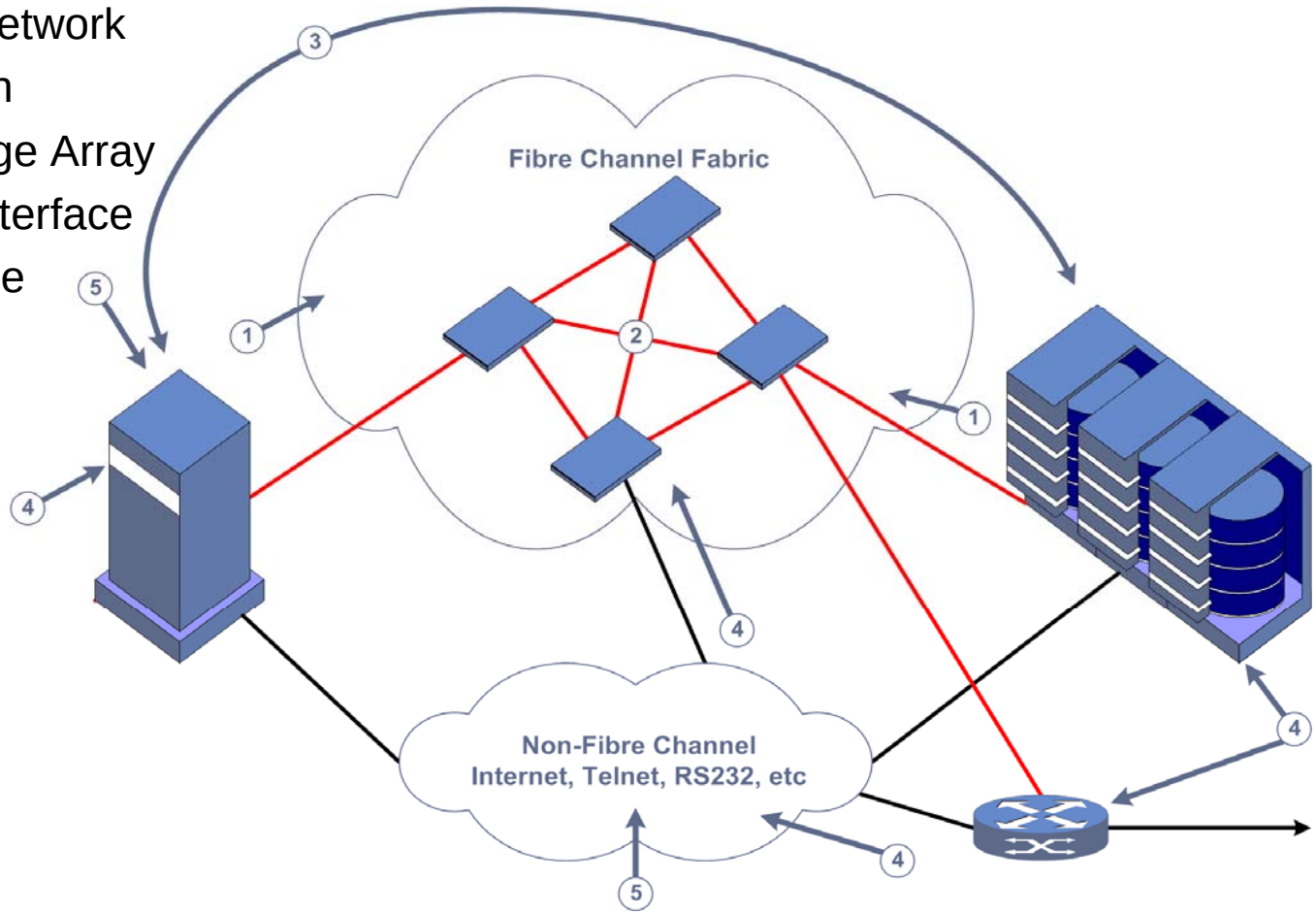
Penalties in the News



- 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

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



What has the industry been focused on?

- Confidentiality
  - Encryption at rest, starting with Removable media
  - Encryption in transit between sites
  - FCsec
- Integrity
  - Link level and object level checks
- Availability
  - Dual paths, highly available storage components
- Access Control
  - LUN masking, zoning, storage management security
  - FC-SP authentication
  - WORM

Threat scenarios

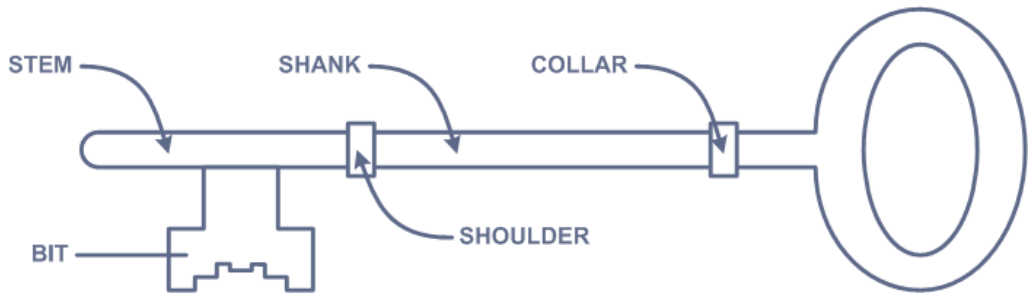
- Examples
  - Loss of removable media
  - Compromise of SAN attached server
  - Rogue administrator
  - Disaster recovery

Loss of removable media

- Security through obscurity is not sufficient
  - Even though data may be in a hard to decipher format personally identifiable information may still be decipherable
- Encryption can be one technique to help with disclosure burden and protects data from unintended disclosure
  - Privacy and identity protection legislation are evolving
  - Proof of encryption for auditors
  - Key management should be a focus

Why is key management important?

- One of the best methods for securely erasing data is to encrypt and loose the key…
- What meta-data is available to help recover the keys?
  - Volume labels?
  - Key labels in audit trails?



Encryption Key Management

- Protection of keys
  - Hardware assistance
    - Tamper aware memory for master keys
  - Long term retention
    - Meta-data or volume labels optionally in the clear
- Life cycle for keys
  - To support reducing the amount of data which uses a single key
  - To support secure erase function
- Revocation of keys
  - In the case of compromise
- Protection of data without access to keys
  - Media duplication

Key Management

- Methods for key management for encryption capable storage
  - Applications can supply keys
    - The backup program manages the keys and gives to storage
  - Library or array supplies the keys
    - Keys are associated with Library or array
  - Keys are management centrally
    - Software
    - Workstation
- Attend ABC's of Data Encryption for more on this topic

Compromise of SAN attached server

- Risk of loss of data or unintended disclosure
- Scenario
  - Server is root level compromised
  - HBA device driver is replaced by malicious driver or memory could be monitored
  - Zoning and SAN fabric is not sufficient to protect against malicious storage access
  - Threat of WWN spoofing
- What is the industry doing about this
  - Signed drivers
  - Server monitoring

Privileged Access Abuse

- Disgruntled or rogue administrator
  - Erases data
  - Copies data
  - Creates openings for malicious access
  - The only owner of the key for encrypted data goes away
- What is being done about this?
  - Audit logging
  - Change management discipline

Disaster Recovery

- Threat
  - I'm a legitimate user and I can't read my data
  - My service provider can't read the data
- Data has to be transported to another site on a regular basis
  - Data has to be recoverable but not able to be stolen
- Key management
  - Can data be shared and recovered without having to distribute secret keys?
  - Can the data be migrated between media without access to the keys?
  - Is there a facility for long term retention of the keys as well as secure disposal of the keys?

Best Practices #1

- Secure the Storage management
  - Administrative accounts
  - Administrative interfaces
  - Administrative consoles
  - Management applications
  - Command line utilities

Best Practices #2

- Identify and assess all storage interfaces
  - What are the storage and data assets?
    - Management interfaces
    - Data interfaces
  - What is exposed?
    - Servers
    - Networks
    - Export to file serving

Best Practices #3

- Create Risk Domains
  - Logical and physical domains
    - Zoning for FC
    - IP/VLANs, firewalls
  - Isolate management traffic from normal server traffic
  - Manage storage infrastructure distinguishing class of service
    - Isolate and use separate ports, equipment, networks
  - Focus attention on interconnections like FC to iSCSI gateways

Best Practices #4

- Monitor and Control Physical Access
  - Restrict access
  - Lock components where possible
  - Disable unused components
  - Investigate errors to detect intrusions
  - Monitor removable media

Best Practices #5

- Avoid failures due to common mistakes
  - Change control for firmware and software
  - Remove default configurations and open access ports
- Maintenance
  - Schedules updates
  - Security around updates
  - Validate changes
- Need change control for changes to the SAN
  - Impact analysis prior to change

Best Practices #6

- Address data security compliance
  - Authentication, authorization, access control
    - Role based
  - Audit logging
  - Data retention, integrity, confidentiality
  - Shred data on deletion

Best Practices #7

- Protect Externalized Data
  - Removable media should be encrypted
  - Data in flight outside of the data center should be encrypted
  - Key management needs focus
    - Protection of keys
      - Hardware assistance
        - » Tamper aware memory for master keys
      - Long term retention
        - » Meta-data or volume labels optionally in the clear
    - Life cycle for keys
      - To support reducing the amount of data which uses a single key
      - To support secure erase function
    - Revocation of keys
      - In the case of compromise
    - Protection of data without access to keys
      - Media duplication
    - See ABC's of encryption tutorial

Best Practices #8

- Understand the exposures
  - Security scanning
  - Monitor vulnerability databases
  - Proactively install security patches
  - Leverage intrusion detection technologies

Best Practices #9

- Implement appropriate service continuity
  - Business continuity
  - Disaster recovery
  - Regular planning and testing
  - Integrate recovery activities into TI design
  - Automate to eliminate errors

Best Practices #10

- Utilize event logging
  - Centralize logging
  - Common accurate time source for correlation
  - Preserve log integrity
  - Analysis and correlation with security events

Summary

- Techniques exist for mitigating risks
- Best practices for security can be applied to storage discipline
  - SNIA's best practices for storage white paper www.snia.org/ssif/documents
- The storage industry is making progress but still has a long way to go

Continue Your SNIA Education Experience At SNW

SNIA
Storage Networking Industry Association
EDUCATION

- Attend Hands-On Labs in:
  - Data Classification
    Key to Service Level Management
  - Data Security and Protection
    Data Assurance Solutions to Meet Corporate Requirements
  - IP Storage
    iSCSI, Your IP SAN
  - Storage Management
    Manage Storage or Be Managed By It
  - Storage Virtualization
    Increasing Productivity
  - Zero to SAN
    - *Fibre Channel Connectivity in No Time*

Sessions begin Monday afternoon, April 16 and continue through Wednesday, April 18.

All sessions in Emma/Maggie/Annie, 3rd Floor of the Hyatt Manchester.

Registration at the SNW Registration area

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

SNIA Education Committee

LeRoy Budnik, CISA
Larry Krantz
Rob Pegler
Eric Hibbard, CISSP
Larry Hofer, CISSP
Phil Huml