The Impact of Emerging Storage Security Standards on Solid State Storage

Walt Hubis

Hubis Technical Associates

ISO/IEC 27040

- **An international standard for Storage Security**
  - Currently in final approval stage (FDIS)
- **Objectives**
  - Draw attention to the risks
  - Provide guidance to better secure data
  - Auditing, designing and reviewing storage security controls
- **Broad Applicability**
  - Security of devices and media
  - Management activities related to those devices and media
  - Applications and services
  - Security relevant to end-users

ISO/IEC 27040

- **Target Audience**
  - Owners, operators or users of data storage devices, media and networks
  - Senior managers, acquirers of storage product and service, and other non-technical managers or users
  - Information/storage security focused managers and administrators
  - Planners, designers, and implementers of the architectural aspects of storage network security

Raising the Security Bar

- **ISO/IEC 27040 defines the best practices storage security**
- **Identifies other important standards and specifications**
  - e.g., FC-SP
- **Specific criteria for both vendors and customers**
  - e.g., Media sanitization methods
- **Creating a new focus on storage security**
  - Vendors, Users, and the security community.

A Guide for Storage Security

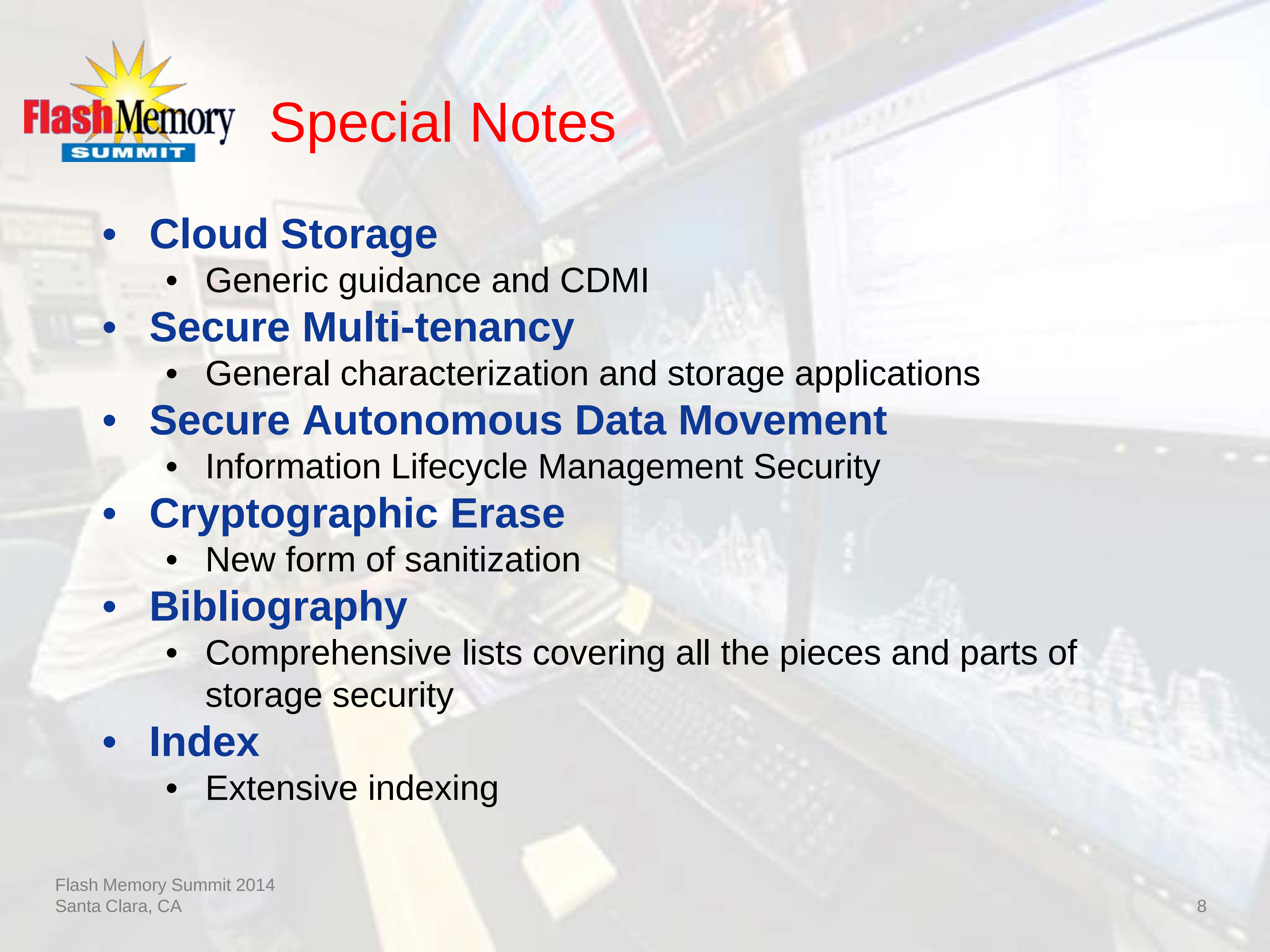
- **Securing Storage Management**
- **Securing Storage Networks**
  - Block
  - File
- **Data Retention Security**
  - Short term
  - Medium term
- **Virtualization Security**
  - Storage ecosystems
- **Encryption & Key Management**
  - In motion and at rest
- **Definitive Standard for Data/Media Sanitization**
- **Storage Security Checklists (Annex B)**

Overview of ISO/IEC 27040

- **Overview & Concepts**
    - Introduces the storage security topic
    - Overview of Storage Concepts
    - Introduction to Storage Security
    - Storage Security Risks
- **Supporting Controls**
    - Technology/control specific guidance.
    - Direct Attached Storage
    - Storage Networking
    - Storage Management
    - Block and File based Storage
    - Object-based Storage (cloud storage)
    - Storage Security Services (sanitization, etc)

Overview of ISO/IEC 27040

- **Design/Implementation Guidelines**
  - Storage Security Design Principles
  - Data Reliability, Availability, and Resilience
  - Data Retention
  - Data Confidentiality and Integrity
  - Virtualization
  - Design and Implementation Considerations
- **Annexes**
  - Media Sanitization
  - Selecting Appropriate Storage Security Controls
  - Important Security Concepts



Special Notes

- **Cloud Storage**
  - Generic guidance and CDMI
- **Secure Multi-tenancy**
  - General characterization and storage applications
- **Secure Autonomous Data Movement**
  - Information Lifecycle Management Security
- **Cryptographic Erase**
  - New form of sanitization
- **Bibliography**
  - Comprehensive lists covering all the pieces and parts of storage security
- **Index**
  - Extensive indexing

Applying ISO/IEC 27040

- **Customer Perspective**
  - Internationally recognized guidance
  - Can be an important reference for RFPs for storage products and service contracts
- **Vendor Perspective**
  - Major threats and risks identified
  - Insight into how technology-specific controls fit into an overall storage security approach
- **ISO/IEC 27040 could easily become a source of requirements**

Thank you!

Special thanks to

Eric Hibbard
Hitachi Data Systems

Walt Hubis
Hubis Technical Associates
walt@hubistech.com
http://www.hubistech.com
(+1) 303.641.8528