# Week 3

MIS-5903

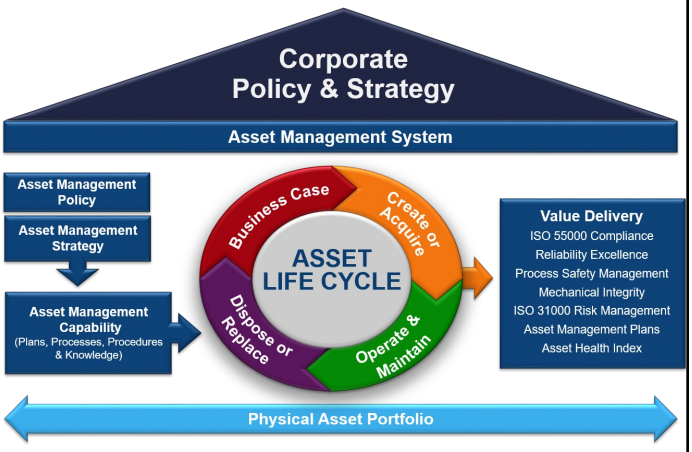
Asset Security

https://community.mis.temple.edu/mis5903sec711summer2022/

1

## Asset Lifecycle

- Identification of Need
- Change Management (introduction)
  - Doesn't break processes
  - No undue risks
  - Doesn't derail ongoing projects
- Operation & Maintenance
  - Do what was intended
  - Without interference of breakage
  - Must be secure
- Replace or Dispose (Retire)






2

# Inventory

- Hardware
  - Asset Monitoring
- Software
  - Application whitelisting
  - Gold Masters
  - Enforcing Least Privilege
  - Device Management Software
    - Unified Endpoint Management (UEM)
  - Automated scanning



3

# Secure Provisioning

- Securely shipping devices to users
- Securely sending credentials to user
- VPN requirements
- Remote monitoring – whether on VPN or not
- Remote Configuration Changes
- Multifactor Authentication
- Controlling Cloud Assets



4

# Asset Retention

- End of Life (EoL) – not sold
- End of Support (EOS) or End of Service Life (EoSL) – no patches for existing assets



5

# Information Life Cycle

- Create/Acquisition
- Store
- Use
- Share
- Archival
- Disposal




6

# Information Life Cycle – Acquisition

- Copied from elsewhere, or Created from scratch
- Information must be made useful
  - Data -> Information -> Knowledge -> Wisdom
- Additions:
  - Data/Time/Location
  - Permissions
    Metadata (data about the data)
  - Business process metadata
    - Classification, project, owner
  - Indexed



7

# Information Life Cycle – Store

- Authorized Media
- Output Restrictions
- Encryption
- Physical Security



8

# Information Life Cycle - Use

- Confidentiality:
  - Access Control
  - Encryption
- Integrity:
  - Hashing, Digital Signatures, CRC
  - Change Control
  - Access Control (physical and technical)
- Consistency
  - Internal Uses
  - Data Aggregation – Compliance Requirements (e.g. name + other details)





# Information Life Cycle – Share

- Authorized Distribution
- Acceptable Use Policy
- Non-Disclosure Agreements
- Data Minimization – Share Only Necessary
- Encryption
- Data Loss/Leak Prevention

# Information Life Cycle - Archival

- How long will it be regularly used?
- How long does it need to be readily available?
- How long is Information:
  - Useful, Relevant, Valuable?
  - Contractually or Legally Required?
- What is an acceptable SLA to deliver or recover?



11

# Information Life Cycle – Disposal

- Data Migration or Export?
- Legal Restrictions
- Secure Destruction
  - Degaussing
  - Overwriting
  - Physical Destruction



12

# Classification Levels – Military

- Unclassified – not sensitive or classified (e.g. recruiting information)
- Controlled Unclassified Information (CUI)
  - If Disclosed, would not cause serious damage
- Confidential
  - Adverse impact
  - Exempt from FOIA
- Secret
  - Serious adverse damage to national security (e.g. deployment plans)
- Top Secret
  - Grave damage to national security (e.g. blueprints, spy satellite, espionage)



13

# Classification Levels – Commercial

- Confidential
  - Disclosure serious adverse impact (e.g. trade secrets, healthcare information, competitive details)
  - Use within the company only
- Private
  - Unauthorized disclosure adverse impact to personnel or company (work history, human resources, medical information)
- Sensitive
  - Requires special precautions (e.g. financial information, profit forecasts)
- Public
  - Disclosure may not be welcome, but no adverse impact



14

# Private Data

- Personally Identifiable Information (PII) – SP800-122
- Children's Online Privacy Protection Act (COPPA) - 1998
- Family Educational Rights and Privacy Act (FERPA)
- Identity Theft and Assumption Deterrence Act – 1998
- Graham-Leach-Bliley Act (GLBA) – 1999
- States – California Consumer Privacy Act (CCPA) – 2018



15

# Protected Health Information (PHI)

- Health Insurance Portability and Accountability Act (HIPAA) – 1996
- Health Information Technology for Economic and Clinical Health (HITECH) – 2009
- HIPAA Omnibus Rule - 2013



16

# General Data Protection Regulation (GDPR)

- May 25, 2018
- Up to 4% global revenue
- Pseudonymization (alias)
- Anonymization
- Data Controller - determines the purposes for which, and the way in which, personal **data** is processed
- Data Processor - processes personal **data** on behalf of the **data controller**(excluding the **data controller's** own employees)



17

# Proprietary Data

- Copyright
- Patent
- Trade Secret
- Trademark



18

# Classification Criteria

- Usefulness of the data
- Value of the data
- Age of the data
- Level of damage is disclosed
- Level of damage if modified or corrupted
- Legal, regulatory, or contractual responsibility to protect
- Effects the data has on security
- Who should be able to access
- Who should maintain the data
- Who should reproduce the data
- Lost Opportunity if Not Available or Corrupted



19

# Classification Controls

- Access control for data or programs
- Encryption at rest, in motion
- Auditing and Monitoring
- Separation of Duties
- Periodic Review
- Backup and Recovery
- Change Cotnrol
- Physical Security
- Information Flow Channels
- Proper Disposal
- Marking, Labeling, Handling



20

# Classification Procedures

- Define Levels
- Specify Criteria
- Identify Data Owners (determine)
- Identify Data Custodian (maintain)
- Identify Security Controls
- Document any exceptions
- Indicate Data Transfer to new Data Owner
- Create Review Procedure
- Declassification Procedures
- Integrate into Security Awareness Programs



21

# Layers of Responsibility

- Executive Management (C-Suite)
- Chief Executive Officer (CEO) – chairperson of board of directors
  - Delegates tasks, but not responsibility
- Chief Financial Officer (CFO) – annual SEC and stakeholder reports
- Chief Information Officer (CIO)
- Chief Privacy Officer (CPO)
- Chief Security Officer (CSO) - includes business processes, legal issues, operational issues, revenue generation, reputation protection
- Chief Information Security Officer (CISO) – focused on IT.



22

# Other Roles

- Data Owner – member of management in charge of a business unit. (determines classification)
- Data Custodian – maintains and protects the data
- System Owner – ensures controls in place on systems
- Security Administrator – maintains security specific controls
- Supervisor (User Manager) – ensures staff understand their responsibilities
- Change Control Analyst – approving or rejecting requests
- Data Analyst – structures, definitions, organization
- User – routinely uses the data for work-related tasks (follows policies)
- Auditor – verifies compliance with policies, procedures.
- "Data Processor" – can be various roles; must understand "acceptable" actions.





# How We Retain

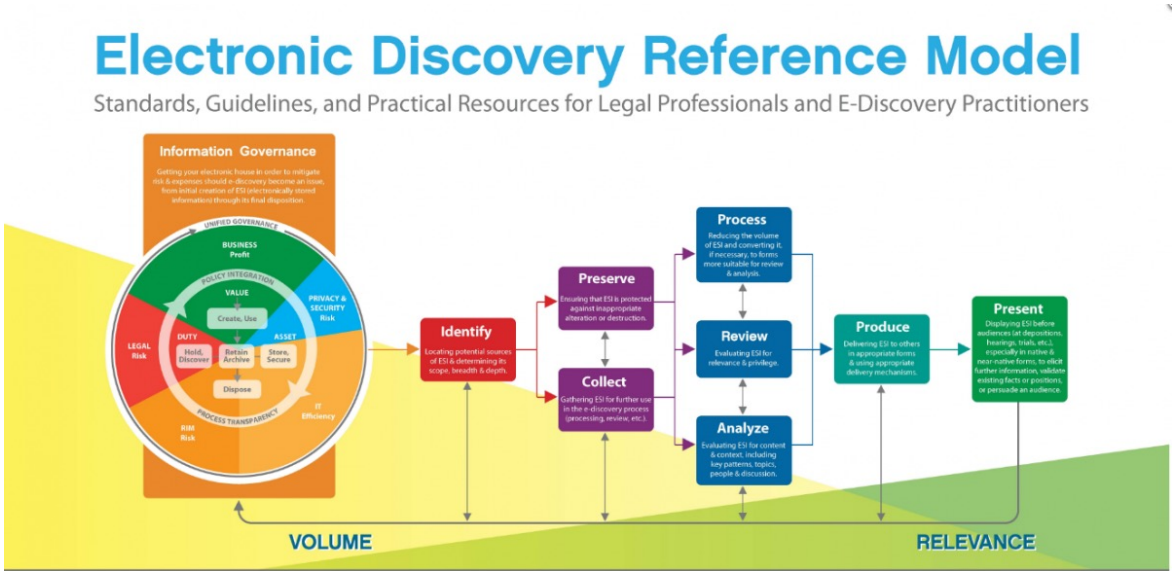
- Taxonomy – scheme for classifying the data (department, time, etc.)
- Classification – based on sensitivity level
- Normalization
  - Tagging data
  - Common formats
- Indexing – enable queries for later retrieval

# Retention

- What?
- How long?
  - Business Documents – 7 years
  - Accounts Receivable or Payable – 7 years
  - Invoices – 5 years
  - Human Resources – 7 years for employed, 3 if not hired.
  - Tax Records – 4 years after taxes paid
  - Legal correspondence - Permanently
- Where?
- Policy must be deliberate, specific, and enforceable







# Data Remanence

- NIST SP 800-88r1 “Guidelines for Media Sanitization”
- Erasing – perform ‘delete’ operation on file(s); data remains
- Clearing / Overwriting – writes fixed patterns of 1’s and/or 0’s
  - At least once
  - Spare/”Bad” sectors remain
- Purging – repeat clearing process multiple times
- Degaussing – magnetic force applied to media
- Encryption – deletion of key renders data unrecoverable “Cryptoshredding”
- Physical – shred or expose to caustic or corrosive chemicals, incineration



27

# Data Security Controls – Three States

## Data at Rest

Hard drive, Optical drive, Solid state drives

Encryption – PHI, PII

- Refer to NIST SP800-111 – Storage Encryption Technologies for End User Devices

## Data in Motion

Transport Layer Security (TLS), IP Security (IPSec)

Virtual Private Networks (VPNs)

## Data in Use

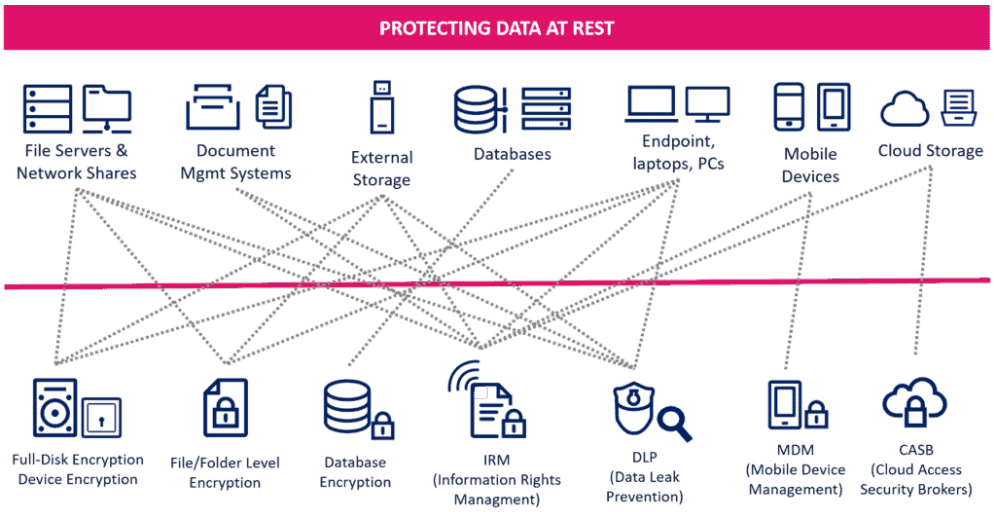
Data in RAM

Heartbleed vulnerability



28

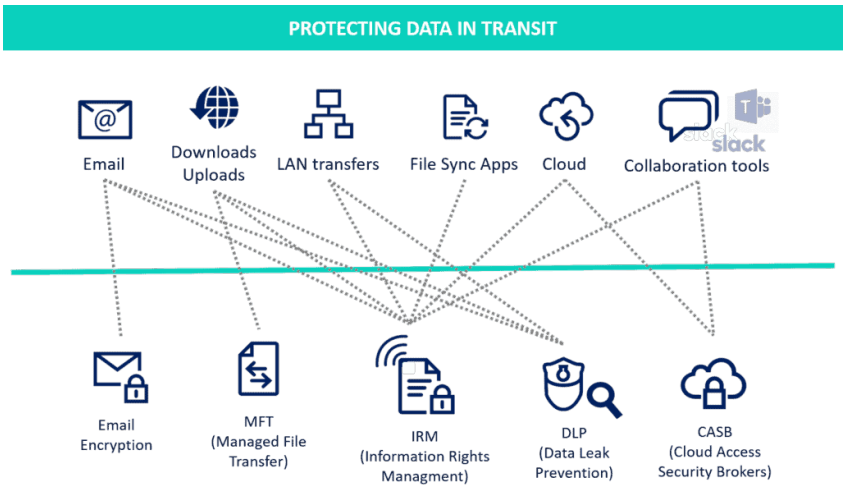
# Data at Rest






29

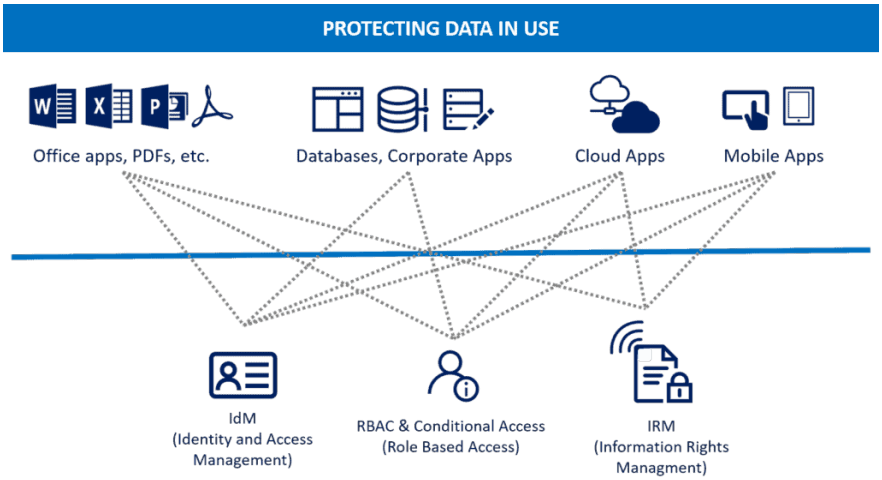
# Data in Motion






30

# Data in Use








# General Data Protection Approaches

- Data Inventories – What, Where
- Data Flows – Inputs, Outputs, Other Parties
- Data Protection Strategy
  - Backup and Recovery
  - Data Life Cycle
  - Physical Security
  - Security Culture
  - Privacy
  - Organizational Change

# Media Management

- Tracking – custody
- Access Controls – necessary level
- Backup versions – onsite and offsite
- Documenting History of Changes
- Ensuring Environmental Conditions
- Ensuring Media Integrity – media can become unreliable
  - Checksums or Signatures
- Regular Inventory
- Secure Disposal



33

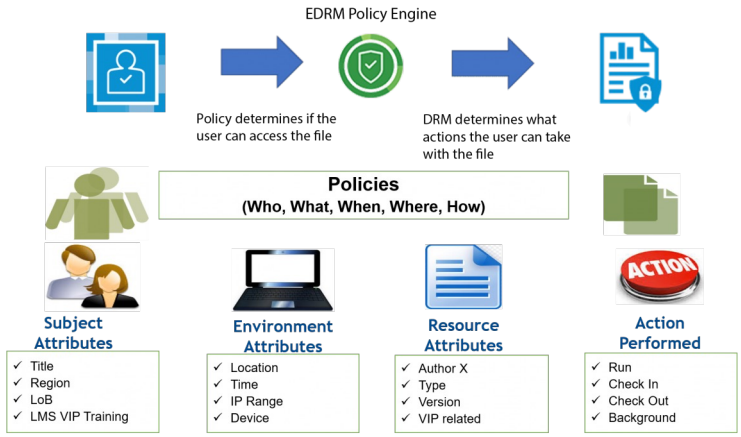
# Labeling of Media

- Data Created
- Retention period
- Classification
- Who created
- Destruction Date
- Name and version



34

# Digital Rights Management (DRM)




- Monetize Digital Content
- Maintain Ownership
- Helps enforce copyright laws
- Simplifies Third Party Relationships
- Aids in compliance with regional laws



35

# Steganography – Hiding in Plain Sight

- Carrier - Stream, Data Stream or File, with hidden information inside
- Stegomedium – Medium in which information is hidden
- Payload – information that is concealed

- Least Significant Bit (LSB) – undiscernible to human eye



36

## Data Leakage/Loss

- Investigation of Incident and Remediation of Problem
- Contacting affected individuals
- Penalties and fines to regulatory agencies
- Contractual liabilities
- Mitigating expenses (credit monitoring)
- Direct damages to affected individuals



37

## DLP Implementation, Testing, Tuning

- Sensitive Data Awareness
  - Keywords, regular expressions, tags, statistical methods
- Policy Engine
- Interoperability
- Accuracy
- Deployment Types:
  - Endpoint
  - Network
  - Hybrid (both)



38

# Mobile Device Protection

- Inventory including serial numbers
- Hardened operating system
- Password protected BIOS
- Registered Devices; Report if stolen
- Do not check devices; always carry-on.
- Don’t leave unattended; carry in non-descript case
- Engrave device with symbol(s)
- Use locks/cables
- Back up all data
- Encrypt data
- Enable Remote Wiping



39

# Paper Records

- Educate staff on proper handling
- Minimize use of paper records
- Ensure workplaces are kept tidy
- Clean Desk – Locked Cabinets
- Prohibit work taken home (prohibit remote printing)
- Label with classification level
- Conduct random bag searches
- Cross-Cut shred. (or burn)



40

# Safes

- Wall safe
- Floor safe
- Chests
- Depositories
- Vaults (walk-in)



41

# Next Steps

- Complete Discussion Questions / Participation
- Complete online quiz – Domain #2 (graded)
- Read Domain #3



42