UNIVERSITY OF CALIFORNIA MERCED

Information Security Policy, IS-3
Records Management Program, RMP-1
Unit Discussions

UNIVERSITY OF CALIFORNIA MERCED

Agenda

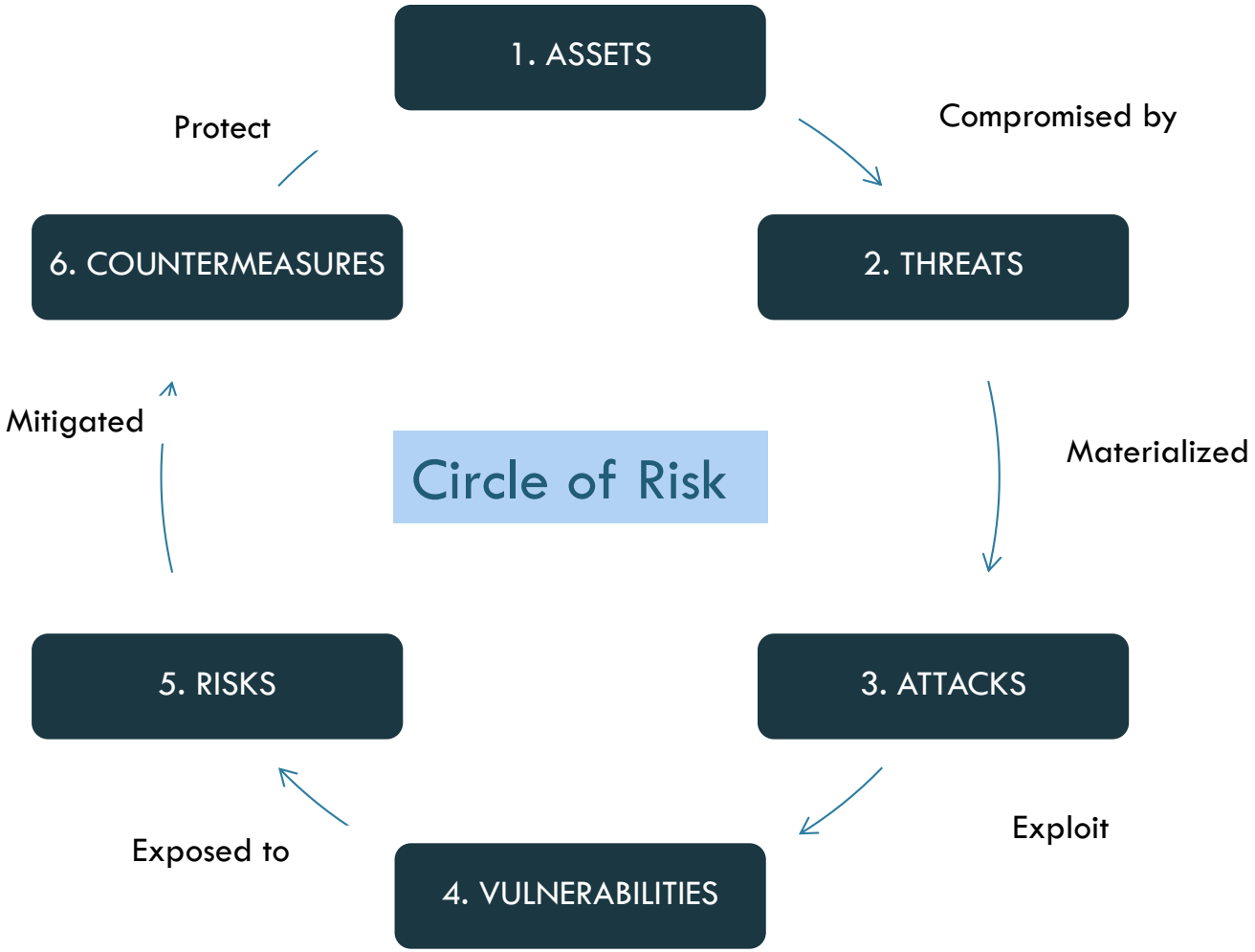
- Intros
- Risk Management Life Cycle
- UC Merced – Visibility Challenge
- Baseline Security Efforts – OIT Services
- IS-3 and Units
- Unit Heads – Unit Information Security Leads Roles
- Data Classification Standard
- Audits
- Summary

Project Contacts

Phil Herechski - pherechski@ucmerced.edu	Security Analyst
Eric Kalmin - ekalmin@ucmerced.edu	Director Records Mgmt.
Tolgay Kizilelma - tkizilelma@ucmerced.edu	CISO
Jose Magana jmagana@ucmerced.edu	Program Manager
Mercedes Zendejas mzendejas5@ucmerced.edu	IT Project Manager

Risk Management Life Cycle

Always start with Assets



Visibility for Protection

- What you don't see, you can't protect!

- UCSF Ransomware Incident - $1.14M Paid
  - Research Data
- UC Merced Ransomware Incident
  - Research Data
  - $300 payment requested, most data recovered, Ransom NOT PAID
- Accellion Breach
  - PII – No Ransomware

- Visibility to Endpoints/Server
  - laptops, desktops, tablets, smartphones
  - UCM lacks visibility to endpoints and to some servers
  - Around 35% of Staff and Faculty endpoints are covered

- Visibility to Data
  - Sensitive Data protected
  - Backups to avoid ransomware
  - Backups to avoid data loss

Baseline Security Efforts

- OIT Services provided to Campus - No Unit Cost
- Bobcat Desktop – Managed laptops/desktops
  - Mobile Device Management - tablets/smartphones
  - FireEye HX - Endpoint Security
  - Encryption
  - CrashPlan – Backup Storage

IS-3 Deployment Roadmap

Timeline of IS-3 deployment	
Completion of Unit 1-1 discussions to go over Baseline Security projects	June 2021
Data Classification/Records Mgmt. Efforts	June 2022
Risk Assessments (RA) conducted	June 2022
Completion of Baseline Security Efforts for All Units	June 2023
Additional Controls implemented based on RA	June 2023

Information Security Policy #3 (IS-3)

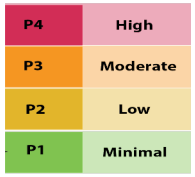
- UC Policy - https://policy.ucop.edu/doc/7000543/BFB-IS-3
- Sets a minimum-security baseline
- Based on a security standard adopted by many other universities (ISO 27001 & 27002)
- Supports a risk-based approach to managing security and new cybersecurity compliance requirements (NIST 800-171, PCI and HIPAA, etc.) governing data protection
- Approved by President Napolitano on September 7, 2018
- Some environments (e.g., critical infrastructure and credit card merchants) will require more controls

Information Security Policy #3 (IS-3)

- Security is a shared responsibility

- IS-3 focuses on risk management; risk assessment is key

- Units are responsible for managing their own risk



- Data classification affects security controls

IS-3 Policy Objectives

- Risk Management
- Human Resource Security
- Asset Management
- Access Control
- Compliance with External Requirements
- Encryption
- Physical and Environmental Security
- Operations Management
- Communications (Network) Security
- System Acquisition, Development, & Maintenance
- Supplier Relationships
- Incident Management
- Information Security Aspects of Business Continuity

IS-3 Policy Scope

- ***Locations***: All UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, UC-managed national laboratories and all other UC locations (Locations).
- ***People***: All Workforce Members*, Suppliers, Service Providers and other authorized users of Institutional Information and IT Resources.
- ***Data***: All use of Institutional Information, independent of the location (physical or cloud), ownership of any device or account that is used to store, access, process, transmit or control Institutional Information.
- ***Devices***: All devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information.
- ***Research***: Research projects performed at any Location and UC-sponsored work performed by any Location.

The UNIT is the Focal Point

- The Unit is a primary point of accountability and responsibility

- A *Unit* is an organization, such as a school, research project, administrative office, or may be a collection of departments

- In support of UC's decentralized organization structure, the policy provides *Units* with the flexibility to manage cyber risk

Key Roles within the Unit

Unit Head: A term used to describe a dean, vice chancellor or similarly senior role *who has the authority to allocate budget and is responsible for Unit performance*. Unit heads are responsible for *ensuring effective management of cyber risk* in a manner consistent with IS-3.

NOTE: Principal Investigators (PI) may also be Unit Heads. The policy formally places PIs in charge of managing security within the baseline set by their Location.

Unit Information Security Lead: Responsible for *tactical execution of information security activities* including, but not limited to, implementing security controls and reviewing/updating Risk Assessment and Risk Treatment plans devising procedures for the proper handling, storing and disposing of electronic media within the Unit; and reviewing access rights.

Unit Head Responsibilities

- Protect Institutional Information and IT Resources according to policy
- Oversees the implementation of IS-3 in the Unit
- Assigns one or more UISL's
- Along with the CISO, approve exceptions appropriate to risk
- Ensures the identification and inventory of Institutional Information and Unit IT Resources
- Ensures that Unit Risk Assessments and Risk Treatment Plans are complete and implemented
- Reports security incidents involving P3+ to the CISO
- Reports legal and contract security non-compliance issues to the CISO
- Through the Risk Treatment Process, ensures that Service Providers and Suppliers meet the requirements of IS-3
- Specifies Protection and Availability Levels to Service Providers and Suppliers
- Reports to the CISO any policy or standard not implemented by the Unit, Service Providers or Suppliers
- Ensure that IS-3 requirements are included in Unit planning and budget processes

UISL Responsibilities

- Inventory of Institutional Information and IT Resources
  - Includes Protection Levels and Availability Levels
- Maintain Unit Risk Assessments and Risk Treatment Plans
- Review privileged accounts for P3+ and A4 assets
- Provide oversight and execution for security responsibilities within the Unit
- Maintain key management processes within the Unit
- Ensure implementation of appropriate and approved encryption methods in the Unit
- Ensure implementation of appropriate event logging requirements and a logging plan
- Implementation of a Unit Incident Response Plan and to inform the CISO of security incidents within the Unit
- Support Workforce Members and Proprietors in planning and executing data sanitation and disposal
- UISL's and IT Workforce Members are responsible for implementing the Secure Software Configuration Standard

New Incident Management Responsibilities

Units may bear some or all of UC's direct costs that result from a *significant failure* of the Unit to comply with IS-3.

These costs include, but are not limited to: Response, containment, remediation, forensics, notification, litigation, penalties, regulatory fines and any other costs directly attributable to the Information Security Incident.

Cyber Insurance Under IS-3

- IS-3 1.2.2
  - A significant failure to comply may affect the Unit's or Location's ability to seek cyber insurance reimbursement under Business and Finance Bulletin BUS-80 - Insurance Programs for Information Technology Systems

Protection Level Classification	**Deductible (Per incident)**
P4 - High	$100,000
P3 - Moderate	$75,000
P2 - Low	$40,000
P1 - Minimal	$20,000

New Data Classification Standard

Protection (P) Levels	
P4	***Statutory, regulatory and contract obligations are major drivers for this risk level.*** Other drivers include, but are not limited to, the risk of significant harm or impairment
P3	***Unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions.*** Could result in moderate damage to UC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate impact on the privacy of a group; could result in moderate financial loss
P2	May ***not be specifically protected*** by statute, regulations or other contractual obligations or mandates, but are generally ***not intended for public*** use or access
P1	Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources where the application of minimum security requirements is sufficient
Availability (A) Levels	
A4	***Loss of availability would result in major impairment to the overall operation*** of the Location and/or essential services, and/or cause significant financial losses
A3	Loss of availability would result in moderate financial losses and/or reduced customer service
A2	Loss of availability may cause minor losses or inefficiencies
A1	Loss of availability poses minimal impact or financial losses

UC Audits

- Threat Detection Identification Audit
  - Relevant to IS-3 implementation

- IS-3 Audit
  - Selected Units will be audited
  - Internal Audit will coordinate
  - Focus on IS-3 policy
    - Objectives
    - Baseline Security

Summary

- UISLs to complete
  - Inventory of records/data, endpoints, users, apps used
  - Classify data protection and availability levels (P1-P4/A1-A4)
  - High-level IS-3 Unit survey when made available
- Infosec team will coordinate the deployment of baseline security efforts
  - Endpoint Management: laptops, desktops, mobile devices
  - Endpoint Security via HX deployment
  - Data Backup/Storage via CrashPlan
  - Encryption
- Ongoing communication among PMO, UISLs, Infosec, Records Mgmt.
  - We are here to help!