Information Security in the Montana University System

Miki Cestnik
IS Audit Manager
April 26, 2022
Montana University System

- Two major units within the system (UM & MSU) that include a flagship campus and affiliate campuses
- Governed by the Board
- Administered by OCHE
Information Security within Higher Education

Federal Regulations to protect certain types of data
Information Security in Montana

Executive Branch

Governance & Administration
- State Law defines **WHAT** agencies are required to do
- **DOA & SITSD** determine **WHAT** needs to happen to follow law (Policy)

Management
- **Agency** determines **HOW** to follow law and policy

Montana University System

Governance & Administration
- State Law defines **WHAT** the MUS is required to do
- **Board and OCHE** determine **WHAT** needs to happen to follow law (Policy)

Management
- **University** determines **HOW** to follow law and board policy

Montana Information Technology Act (MITA) excludes University System.

However, law requires the Board to ensure state security laws are followed.
Scope and Objectives

Risk Management procedures at the two major university campuses

- How mature is risk management?
- How is risk management improving the security program?

Security Governance established by the Board and OCHE

- Does it provide guidance?
- Does it create accountability?
- Is there internal review?
Universities need direction & guidance to assess risks and improve security programs

- **Board of Regents**
  - 2 Recommendations
    - Stronger board policy and direction

- **University of Montana**
  - 1 Recommendation
    - Formalize security responsibilities
    - IT risk assessment

- **Montana State University**
  - 1 Recommendation
    - IT risk assessment
Risk Management is More than Assessing Risks

WHAT IS THE STRATEGY?
WHAT ARE THE CURRENT RISKS?
WHAT SHOULD WE DO?
IS THAT WORKING?
Audit Methodologies

Example:

Phishing Attack

User Awareness Training

User still provides credentials

Control assessed by LAD

Vulnerabilities identified and measured by Contractor

LAD Control Assessment

Vulnerabilities

Controls

RISK

Controls

Contractor Testing
Each Campus Faces Risks without Improvement

The effects of the current security programs are starting to happen and more have the potential of occurring without action.

What we see now...
- Increased costs for insurance
- Future funding challenges
- Federal Non-Compliance

What else could happen?
- Security Incidents
- Service disruptions
Law required the board ensure data security throughout the MUS. Board Policy doesn’t further define what, only suggests a NIST framework where appropriate.

Universities have to define WHAT and HOW.

Recommendation 1
Board Policy:
- Adopt a framework or set of frameworks
- Reviewed continuously
- Coordinated effort
Each University Has to Maintain Their Security Program

University of Montana
- Staffing challenges
- Role and responsibility definition
- IT risk management is informal

Recommendation 2
- Formalize security staff responsibilities
- Complete a comprehensive IT risk assessment to develop strategies and budgets to make progress

Montana State University
- No formal guidance
- Missing a structured approach
- IT risk assessments have been focused and not continuous

Recommendation 3
- Complete a comprehensive IT risk assessment to formalize the approach of the security program
Security Governance

- Strong organizational policy
- Roles are defined and coordinated
- Risk is managed
- Continuous monitoring and evaluation
- Policy does not include state law requirements
- Communication is informal
- Location of responsibilities needs reviewed

How are these ensured?
Who communicates the need for framework changes?
What’s the scope of the risk assessment?
No Clear “Right Way”

**Centralized**
- Security

**CONSIDERATIONS:**
- Independent Budgets & Resources
- Avoid one-size-fits all

**Decentralized**
- Security
- Security
- Security

**CONSIDERATIONS:**
- Prevent Silos
- Share Information
Security Programs Need Clear Roles & Boundaries

Recommendation 4
✓ Define OCHE’s role
✓ Security policy meets state requirements
✓ Roles, Responsibilities, and Authority
✓ Communication
Everyone Plays a Role in Information Security

- Board of Regents
  - Office of Commissioner of Higher Education
    - University of Montana (Missoula)
    - Montana State University (Bozeman)
  - Recommendation 1
  - Recommendation 2 & 3
  - Recommendation 4