Implementing a University Cyber Risk Mitigation Policy: Lessons from IT-28

Kim Milford
Director: REN-ISAC
Formerly IT Policy Officer

Brad Wheeler
VP for IT, CIO, and Dean
Professor of Information Systems
How to Balance Mission and Risks?

Essential, distributed culture of the Academy

The growing institutional cyber risks
“It’s just one server!”

Faculty Member → Tension → Chairs, Deans, Administrators → Tension → Senior Officers and Trustees

“Reduce Risk!”
Small Distributed Risks... Grow Organizational Risks

We think we only have about 4,000 servers. No one really knows.
June 2013
The Guardian exposes NSA surveillance programs as detailed by Edward Snowden

January 2013
NYT and WSJ both report being infiltrated by Chinese hackers

February 2013
Mandiant report on APT1

December 2013
Target customer data breached

February 2013
Posted for review

April 2013
Revised

January – May 2013
Draft policy creation and circulation

February 2014
IU potential sensitive data exposure

May 2013
Approved

May 2014 – Present
Conduct 107 peer reviews of planners

October 2014
CIO Approves first reviews

May 2014
Deadline to submit IT28 planners

May 2014
Present 53 reviews fully approved

February 2015
Anthem customer data breached

November 2014
Sony Pictures hacked by “Guardians of Peace”; presumed to be North Korea

September 2014
Home Depot customer data breached

October 2014
Deadline to submit IT28 planners

Key
Corporate
Government
IU

TIMING
IT-28: Cyber Risk Mitigation
The Policy
IT-28 The Policy

To the greatest extent *practicable*

- Move into secure facilities
- Utilize shared services
Spent most of a year working with all varieties of stakeholders to create policy and self-audit process.

Leveraged IT Managers Council, departmental IT, and frontline support staff.

Ran into the fire when anyone reported a problem or burden.
Development of Cyber Risk Mitigation Policy- FY 2013

1. Draft
2. Group Meetings
3. Revisions
4. Final
5. Additional Revisions
6. Presentations
Sub-Certification and Sign Off – FY 2015

Departmental IT Staff

Dean

CIO
Unit Submissions and Peer Review – FY 2014

Review Process Design

Inventory & Self Report

Peer Review
Central IT is **Not** Exempt

**Physician, heal thyself!**

Luke 4:23

Took 150 hours for EITS [central IT] to prepare the internal IT review submission -- just under 1 person-month.
Factors Contributing to Successful Implementation
Timing is Everything
Policy-Driven Culture @ IU

This website is your authoritative, easy-to-use guide to university-wide policies—the policies that apply to all Indiana University organizations. Please note, in addition to these university-wide policies, your campus or unit may have policies that apply to specific topics.

On this website, you can search for policies, see which policies are under review. Refer to our policy development resources and review/approval process. Ask questions and give us policy-related feedback.

FULFILLING the PROMISE
Support from All Levels of Administration

- Board of Trustees
- President & Provost
- Deans
- Department Chairs
Recognition of IT Job Redesign in Schools and Administrative Units
Lessons Learned
Misperception Battle and Real Policy

Server choices are the prerogative of schools and departments.

We are UITS. You will be assimilated.
Discovered More Servers than Previously Thought

1,578 Additional servers identified through IT-28 review process

33% Reduction in the number of servers outside of secure facilities

4,572 Servers (88.4%) will be in Secure Facilities
Many School Level Managers Saw IT-28 as an Opportunity

- We’ve been saying this for years!
- They finally have to take us seriously!

School Level Managers
Most Common Criticisms

- We understand our users’ needs best
- Central services are too expensive
- Common services aren’t secure enough
- Time-consuming!
- Risk management isn’t our responsibility
- We’re unique!
Cyber Risk Mitigation Policy: The Cookbook

Develop a culture of risk management

Get executive buy-in

Communicate, repeat

Seek feedback and assistance

Evolve services in response to need

Deploy resources to support
Implementing a University Cyber Risk Mitigation Policy: Lessons from IT-28

Kim Milford
Director: REN-ISAC
Formerly IT Policy Officer

Brad Wheeler
VP for IT, CIO, and Dean
Professor of Information Systems