Enforcing Information Security Policies in the Higher Education Community

David G Swartz, PhD

Co-chair Higher Education Information Security Council
Educause and Internet2

Chief Information Officer
American University, Washington DC

Overview

- The Challenge to Enforcement
- The Foundation to Information Security and the InfoSec Maturity Roadmap
- The Reasons for Lack of Compliance
- Addressing the Roadblocks to Compliance
- Focusing Security Efforts
- Importance of Collaboration
- Questions & Discussion

The Challenge

- Studies indicate that the majority of universities have an information security policy.
- But they stumble when they try to walk the walk and enforce the policy.
- Less than half of universities with policies go on to enforce them.
- **Why is that and what can we do about it?**

Enforcing Information Security at a University is like herding cats

Source: YouTube “Herding Cats” from EDS.com

Its not so much **WHAT** to do – but **HOW** to get it done!

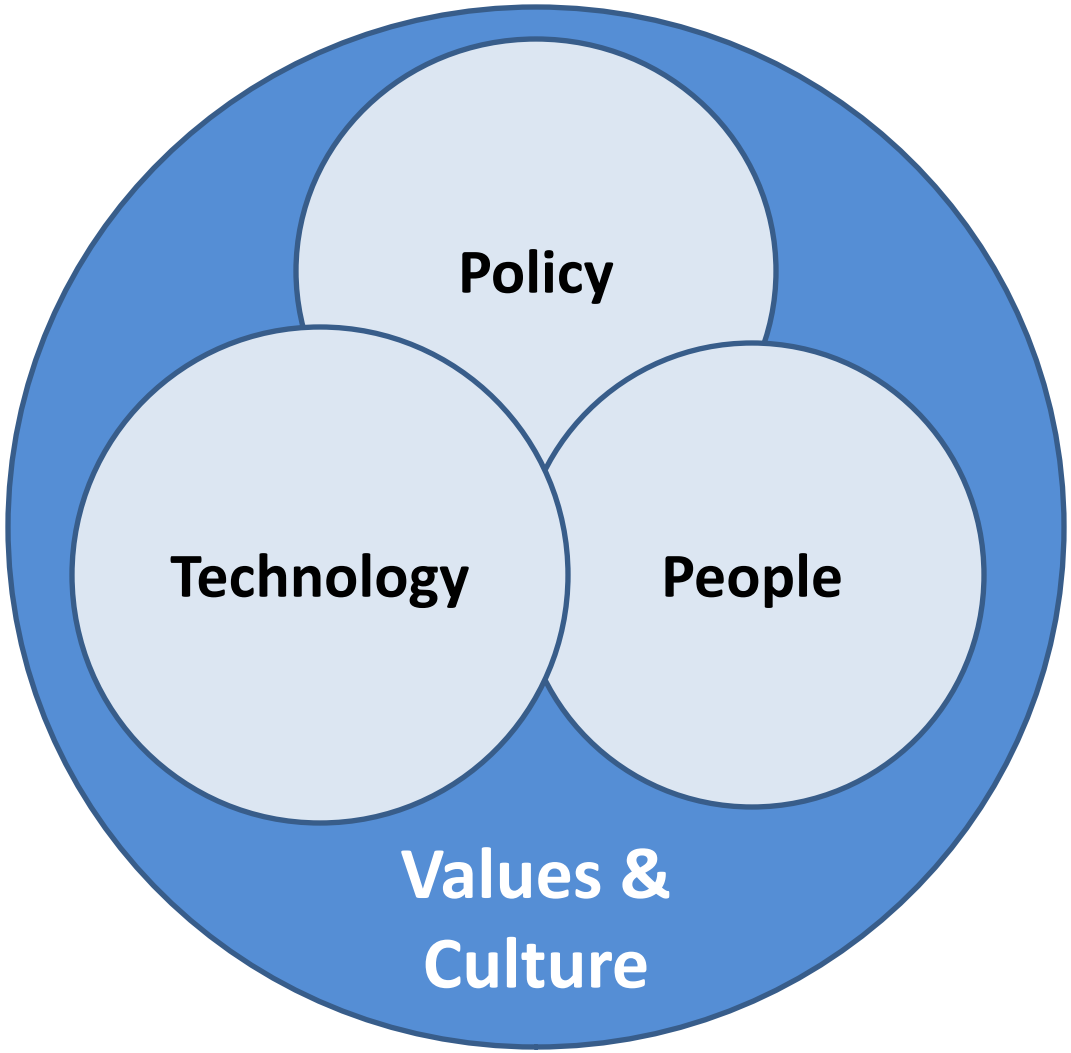
We need to focus more on the **HOW** to be more effective

Examples:

the WHAT = deploy a firewall
the WHAT = deploy an IPS/IDS

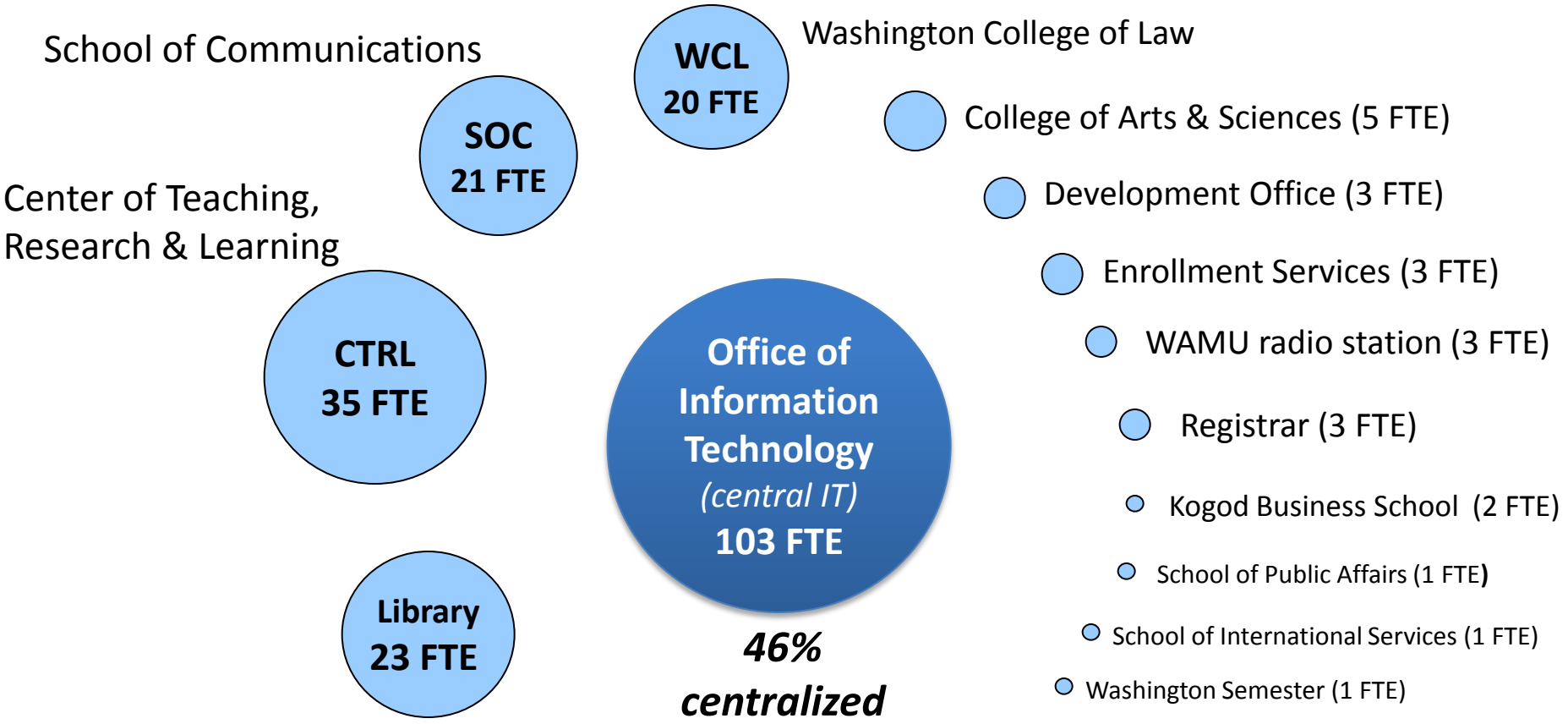
the HOW = get authority
the HOW = get resources
the HOW = build awareness
the HOW = develop partnerships

Dimensions to Information Security



AU Decentralized Technology Landscape

Herding the Cats!



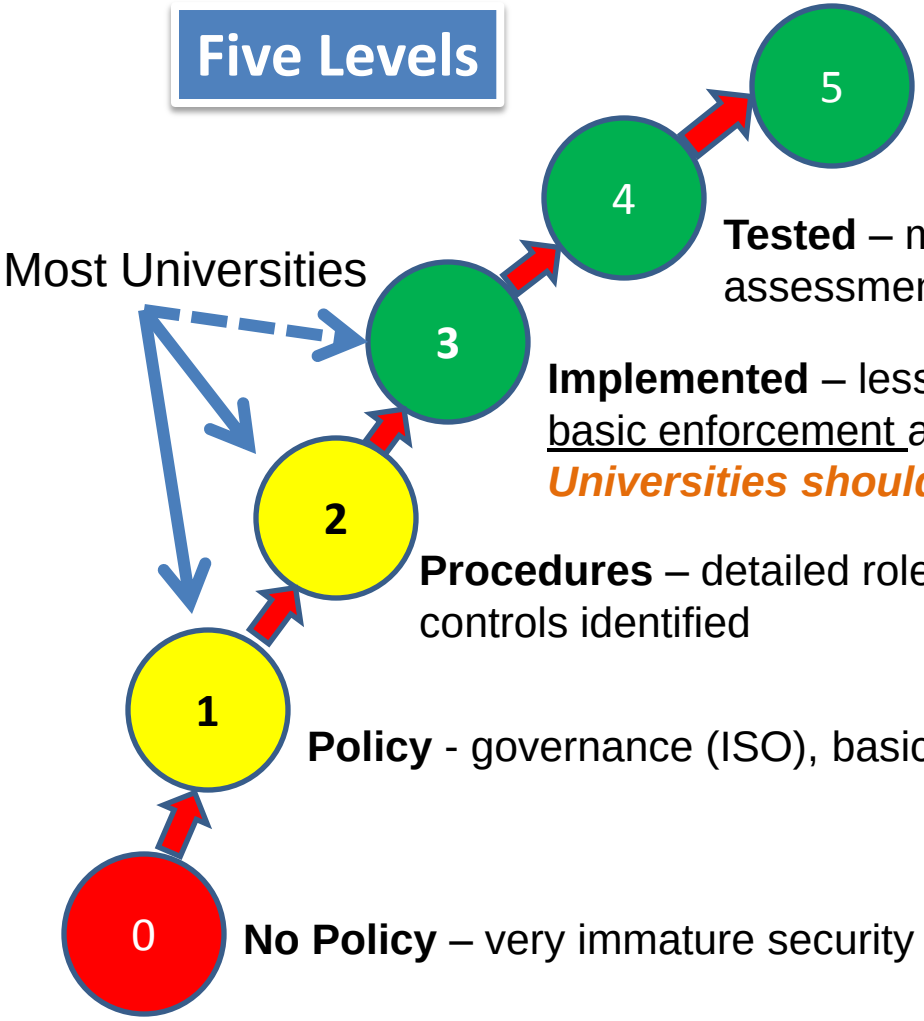
The Foundation to Information Security

- The **Information Security Officer (ISO)** is central to building a mature information security program
  - A majority of universities now have an ISO
  - Organizational reporting of the ISO:
    - A majority of ISOs report to the CIO. The level of the CIO therefore affects the ISO and their access to university management.
- An **Information Security Policy** is also needed
  - A majority of universities now have an information security policy

The Policy

- Policy should be clear, concise, assign authority, list roles and responsibilities, and also link to procedures that lay out detailed rules and standards.
- Often universities think once a policy has been approved they are done.
- Policy needs regular review, updates, and progress reports to management.
- Policy should link to procedures, but unless they are implemented the policy is basically useless.

Information Security Maturity Roadmap



Integrated – very mature, continuous improvement, security part of culture

Tested – mature testing, independent audits, self assessments, and <u>good enforcement</u> and compliance

Implemented – less ad hoc and more consistent application, <u>basic enforcement</u> and controls, basic testing and training.
Universities should be at level 3 or above.

Procedures – detailed roles & responsibilities, and basic controls identified

Policy - governance (ISO), basic roles & responsibilities, and guidelines

No Policy – very immature security program

Lack of Compliance

- Compliance with policy and procedures is a major challenge for universities, problems are due to several reasons:
  1. Lack of authority to match responsibility
  2. Lack of resources to implement security programs and enforce policy
  3. Lack of awareness and enforcement across a decentralized campus

Getting the Authority

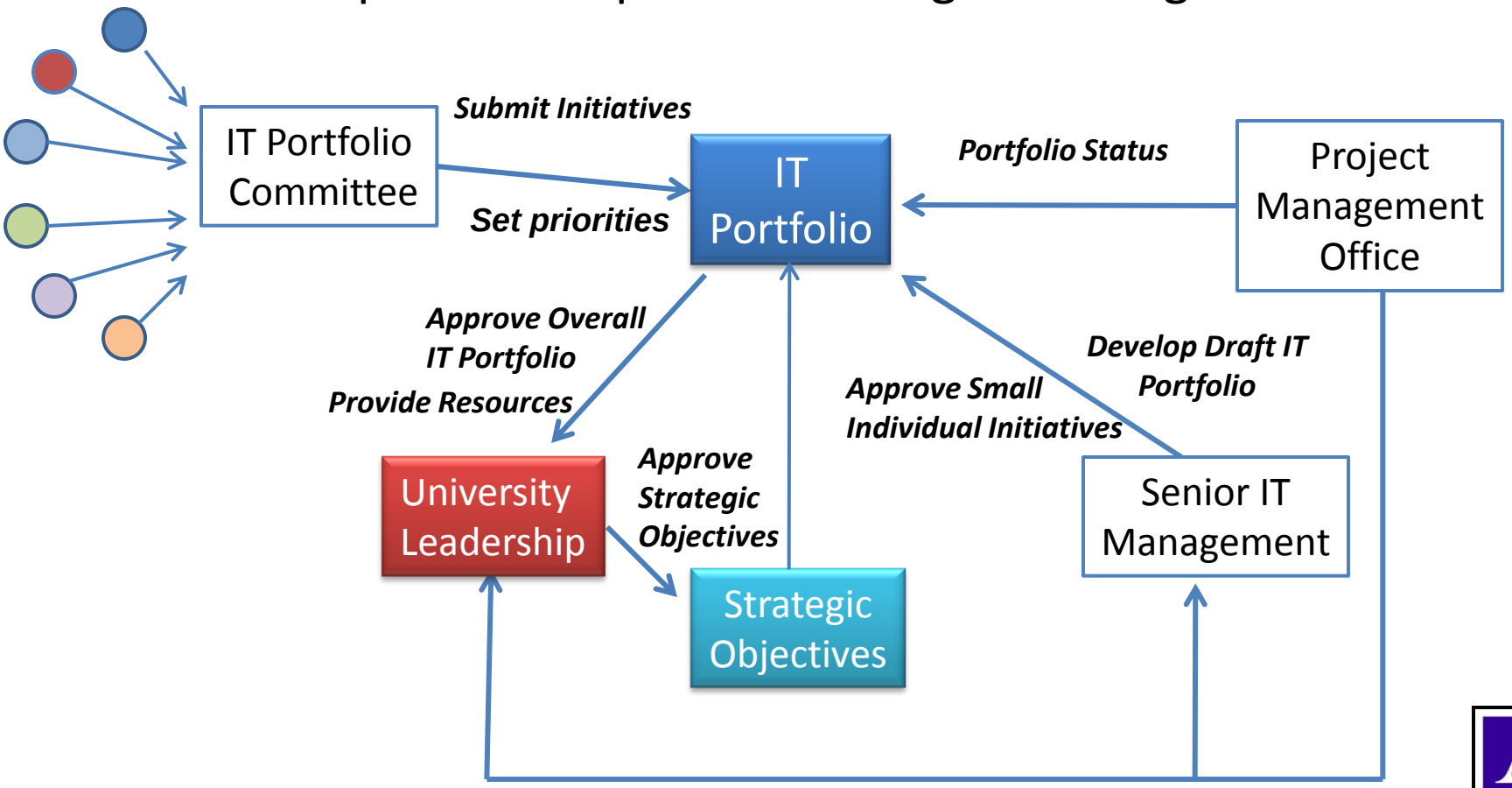
- Spelling out the appropriate level of authority in the security policy is key, not just the responsibility for security
- To enhance the level of authority it is important to partner with:
  - Auditors, Office of General Counsel, Risk Management Committee, and other campus stakeholders such as the Data Custodians in Human Resources, Comptrollers Office, and Registrar.

Getting the Resources

- **Benchmark –** Compare your university to other peer universities – if your program is below the median of these groups it is a very effective technique to get leadership to provide additional resources.
- **Leverage the Crisis** – When an incident occurs do not hide, but go public for the need for resources, support will never be better than following such an event.
- **Portfolio Management** - Risk Managers and Auditors can help the ISO as advocates to a university IT portfolio group to help make proposals to senior management for resources to fund initiatives to mitigate risks.

IT Portfolio Management

- Getting university stakeholders to agree upon what is most important, including security initiatives.
- Helps to set IT priorities and get funding



Awareness & Education

- Lack of awareness of the information security policy and procedures leads to compliance issues. To address this use:
  - Training and certification programs to get access to systems
  - Regular Communications - Alerts, Hints, Posters, etc.
  - Cybersecurity Month (October)

Posters & Videos

Report Cards

Awareness of Performance

- For schools and departments across the university use a report card that has a clearly understood methodology for grading. This is a very effective approach to building awareness and getting units of the university on board.

Schools & Departments

Security Assessment	Business	Law	Medicine	Arts & Sciences	Education	Engineering	Public Affairs	Finance	Dev.	HR	Registrar
Physical Security	2	2	2	1	2	2	2	2	2	3	3
Confidentiality Agreements	2	2	2	1	2	2	2	2	2	3	3
Business Continuity Plan	1	2	2	1	1	2	1	2	1	2	3
Backups	2	2	3	2	2	3	1	2	1	3	3
Software Patching	2	3	3	2	2	3	2	2	2	2	2
Password Protection	2	2	3	2	2	3	2	3	2	3	3
Encryption	1	2	3	2	2	3	1	3	2	3	3
Vulnerability Assessments	2	2	2	1	2	2	1	3	1	2	2
Anti-virus	2	3	3	2	2	3	2	3	2	3	3
Firewalls	2	3	3	2	2	3	2	3	3	3	3
Logs	1	2	2	1	1	3	1	3	2	2	3
SDLC & Software Selection	1	2	2	1	1	2	1	2	2	2	2
VPN	2	2	3	2	2	3	2	3	2	3	3
Data Classification	2	3	3	2	2	2	2	3	2	3	3
Acess Management	2	3	3	2	2	2	2	3	2	3	3
Incident Response Plan	2	2	2	1	1	2	1	2	1	2	2
Media Purging & Disposal	2	2	3	2	2	3	2	3	2	2	2

Focusing Security Efforts

Privacy Levels (from Data Classification Policy)

Operations	Public	Official	Confidential
Enterprise System	**2**	**2**	**Highest Security Highest Operations** **1**
Department Server	**3**	**2**	**1**
Desktop/ Laptop	**Lowest Security Lowest Operations** **4**	**3**	**2**

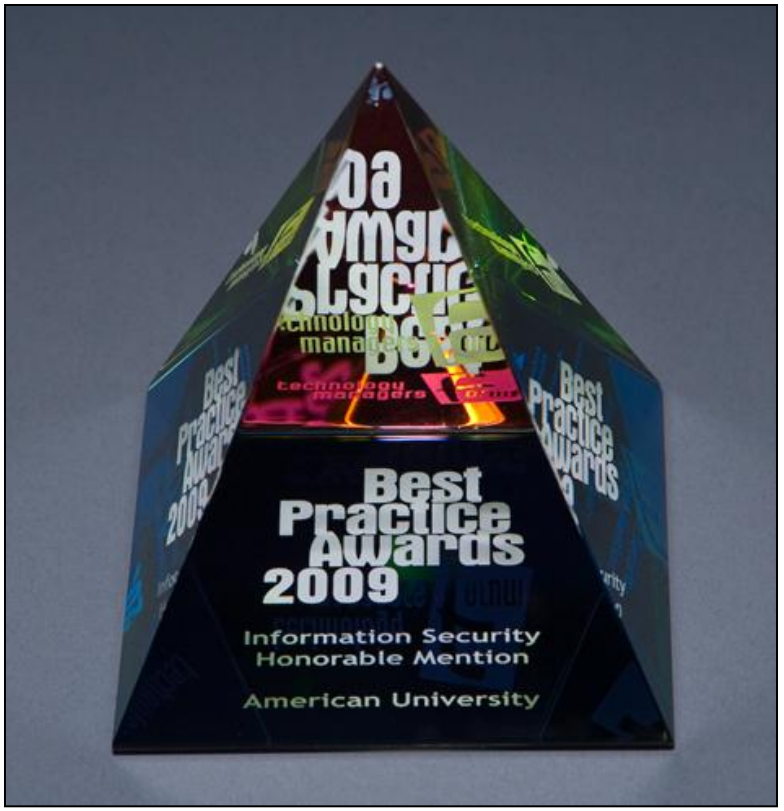
Operations → Systems Availability & Integrity

Automate

- Without automation, full compliance is nearly impossible to achieve.
- For some universities they are lucky to have one or two people to support information security. On a typical day:
  - That person can probably check a couple dozen systems per day to enforce security policies.
  - It could take many months to get through the entire organization.
  - At the end of the cycle, you start over again. That is a long time for something to happen and it often does. This is why there is no way to maintain a solid security posture manually.

Collaborate

- Collaborate with other universities to gain more depth and support, and to learn of best practices
- Regional: our award winning partnership with George Washington University and Georgetown University
  - In case of a major incident they can be called in to help back us up
- National: In the U.S. we have HEISC and also REN-ISAC



Award to American University

Higher Education Information Security Council (HEISC)

- **Created:** By Educause and Internet2 in 2000.
- **Membership:** > 2000 universities
- **Mission:** To improve information security and privacy across the higher education sector by actively developing and promoting effective practices and solutions for the protection of critical IT assets and infrastructures.

HEISC Activities

- Security Discussion Group
- Working Groups
  - People: awareness and training
  - Process: compliance, policies, risk, governance
  - Technology: effective practices and solutions
- Professional Development
  - Annual Security Professionals Conference (April)
- Collaborations and Partnerships
  - Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) – alerts & monitoring
  - and more -> **Joint Universities Computer Centre (JUCC) ?**

HEISC Special Projects

- Confidential Data Handling Blueprint
- Guidelines for Data and Media Sanitization
- Security Wiki including toolkits for Electronic Records Management, Data Retention, and e-Discovery
- Information Security Governance Guide
- Risk Management Framework
- Security Awareness Poster/Video Contest & Library
- National Cybersecurity Awareness Month
- Security Metrics

Effective Security Practices Guide from HEISC

- Risk Management
- Compliance
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Controls
- Information Systems Acquisition, Development, and Maintenance
- Incident Management
- Business Continuity Management

For More Information on HEISC

- **Visit:**
  - Higher Education Information Security Council http://www.educause.edu/security
- **Contact:**
  - David Swartz, American University, HEISC Co-Chair dswartz@american.edu
  - Rodney Petersen, EDUCAUSE, HEISC Staff rpetersen@educause.edu

Dave

QUESTIONS & DISCUSSION