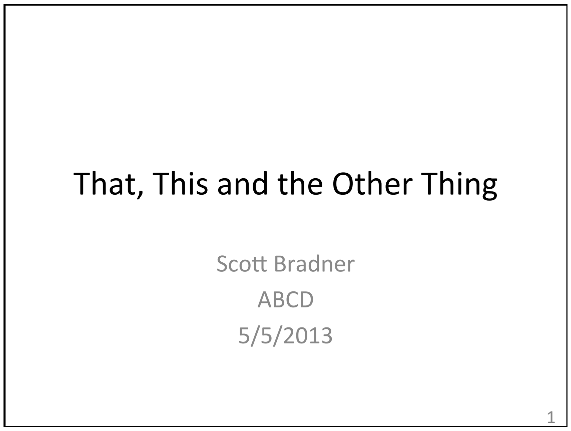
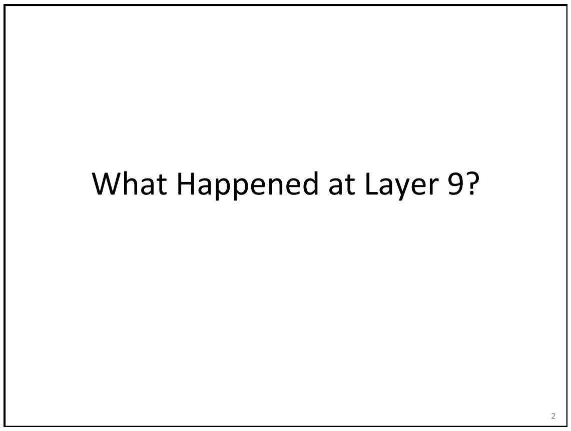
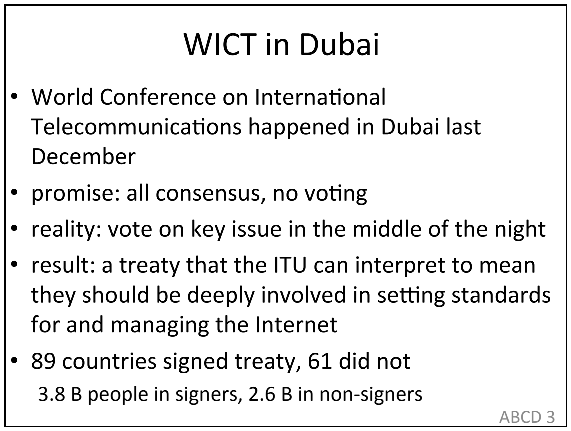


That, This and the Other Thing

Scott Bradner
ABCD
5/5/2013



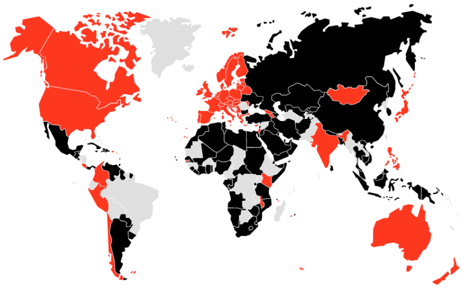
What Happened at Layer 9?



WICT in Dubai

- World Conference on International Telecommunications happened in Dubai last December
- promise: all consensus, no voting
- reality: vote on key issue in the middle of the night
- result: a treaty that the ITU can interpret to mean they should be deeply involved in setting standards for and managing the Internet
- 89 countries signed treaty, 61 did not
  3.8 B people in signers, 2.6 B in non-signers

Treaty Signers & Non-Signers

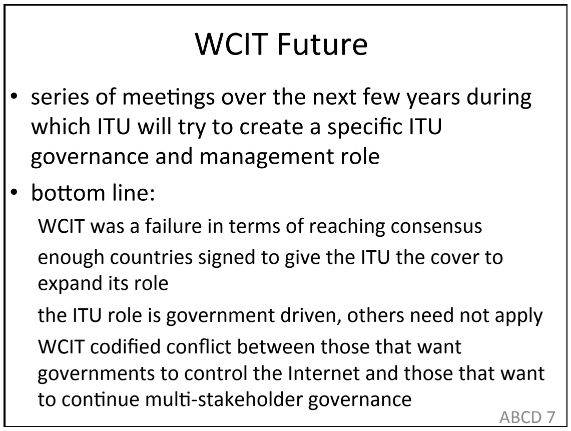


WCIT, Contd.

- US felt that the treaty should not mention the Internet & that the ITU should have no role in the Internet –per see
- treaty tells ITU *"to continue to take the necessary steps for ITU to play an active and constructive role in the multi-stakeholder model of the Internet as expressed in § 35 of the Tunis Agenda"*
- i.e. ITU to keep inserting itself in Internet issues

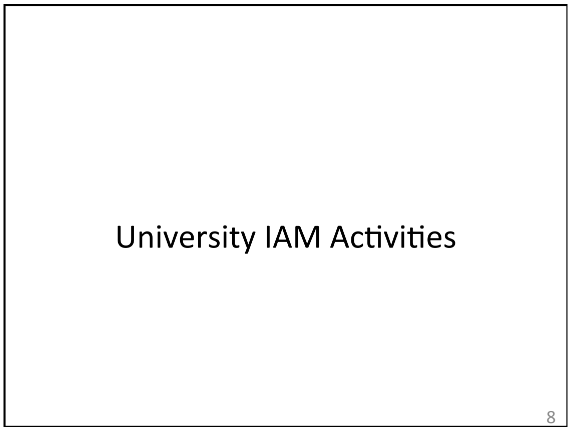
WCIT, Contd.

- treaty also says: *All governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized,;*
- i.e., governments rule -- 1 country one vote -- other stakeholders "consulted"

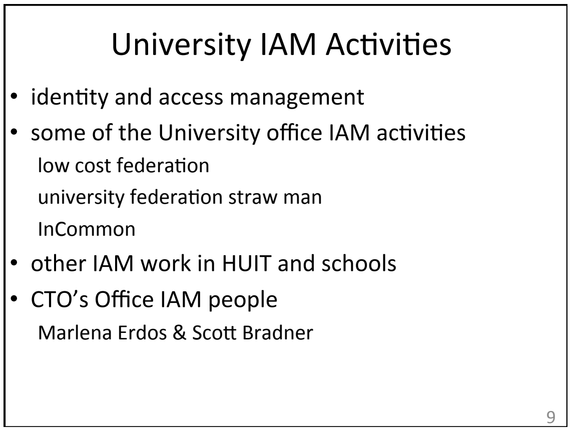


WCIT Future

- series of meetings over the next few years during which ITU will try to create a specific ITU governance and management role
- bottom line:
  - WCIT was a failure in terms of reaching consensus
  - enough countries signed to give the ITU the cover to expand its role
  - the ITU role is government driven, others need not apply
  - WCIT codified conflict between those that want governments to control the Internet and those that want to continue multi-stakeholder governance



University IAM Activities

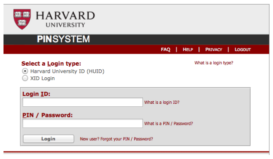


University IAM Activities

- identity and access management
- some of the University office IAM activities
  - low cost federation
  - university federation straw man
  - InCommon
- other IAM work in HUIT and schools
- CTO's Office IAM people
  - Marlena Erdos & Scott Bradner

Existing PIN Operation #1

- you attempt to access http://harvie.harvard.edu/
  a site that needs HUIDs
- you are sent to the PIN server


HARVARD
UNIVERSITY
PINSYSTEM
FAQ | HELP | PRIVACY | LOGOUT
What is a login type?
What is a login ID?
What is a PIN / Password?
Login
New user? Forgot your PIN / Password?

Select a Login type:
● Harvard University ID (HUID)
○ XID Login

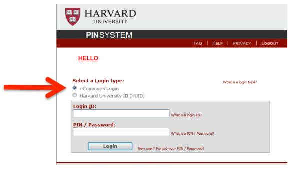
Login ID:

PIN / Password:

- enter HUID/PIN & click on “Login”
- PIN server checks its database
- if successful match, you are sent to Harvie & Harvie is given HUID

Existing PIN Operation #1

- some application support alternate logins


HARVARD
UNIVERSITY
PINSYSTEM
FAQ | HELP | PRIVACY | LOGOUT
HELLO
What is a login type?
What is a login ID?
What is a PIN / Password?
Login
New user? Forgot your PIN / Password?

Select a Login type:
● eCommons Login
○ Harvard University ID (HUID)

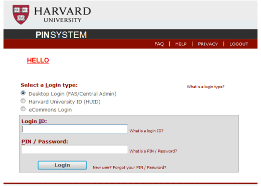
Login ID:

PIN / Password:

- select eCommons login
- enter eCommons/password + click on “Login”
- eCommons ID/password sent to eCommons server
- eCommons server responds with “OK” if match
- you are sent to application & application is given eCommons ID

“Low Cost Federation”

- for PIN2 enabled sites that want HUIDs


HARVARD
UNIVERSITY
PINSYSTEM
FAQ | HELP | PRIVACY | LOGOUT
HELLO
What is a login type?
What is a login ID?
What is a PIN / Password?
Login
New user? Forgot your PIN / Password?

Select a Login type:
● Desktop Login (FAS/Central Admin)
○ Harvard University ID (HUID)
○ eCommons Login

Login ID:

PIN / Password:

- select eCommons login
- enter eCommons/password + click on “Login”
- eCommons ID/password sent to eCommons server
- eCommons server responds with “OK” & HUID if match
- you are sent to application & application is given HUID

Low Cost Federation (LCF)

- enables the use of alternate (e.g. local) login credentials when accessing PIN2 applications that use HUIDs

  reduces the number of different credentials you need to remember and use

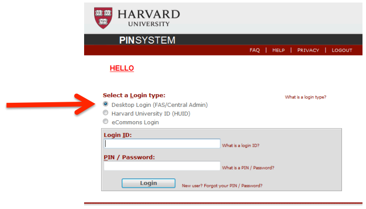
  may not reduce the number of times you need to enter credentials – that depends on each application' setup

- PIN server updated – ready to support LCF

  work underway at HMS to enable eCommons credentials

  other schools are invited to participate

LCF & Active Directory



HARVARD UNIVERSITY

PINSYSTEM

FAQ | HELP | PRIVACY | LOGOUT

HELLO

Select a Login type:

What is a login type?

● Desktop Login (FAS/Central Admin)

○ Harvard University ID (HUID)

○ eCommons Login

Login ID:

What is a login ID?

PIN / Password:

What is a PIN / Password?

Login

New user? Forgot your PIN / Password?

- LCF supports use of desktop login (Active Directory)

  use same credentials to access PeopleSoft as you use for ICEmail

  current support for both FAS and central admin AD

- to be enabled “soon” for all PIN2 HUID-based apps

LCF Features

- one-way

  can use school credentials to access PIN2-enabled apps

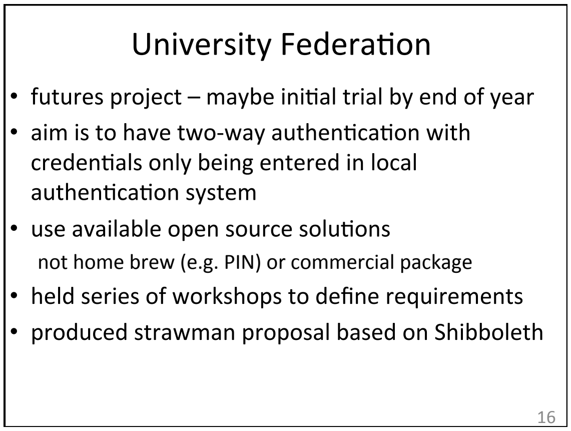
  error if non HUID holder tries to access app that requires HUID

  but not use PIN (or AD) credentials to access school apps

- credentials entered into PIN server & sent to local authentication system

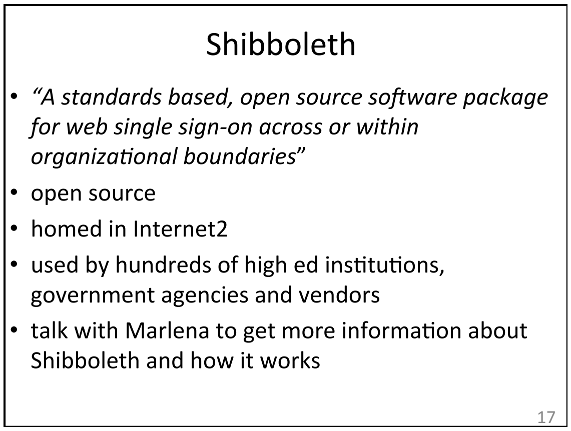
  so PIN server sees non-PIN credentials

  an issue for some security people



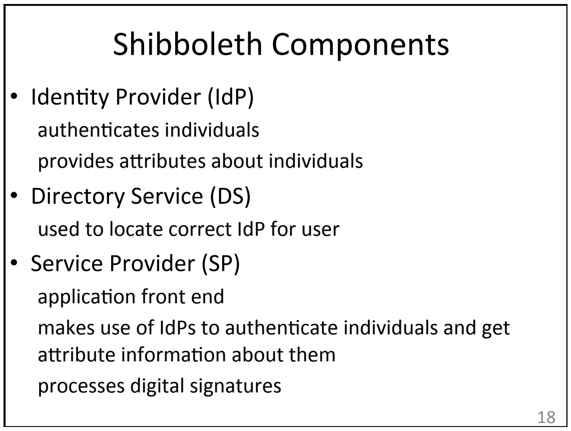
University Federation

- futures project – maybe initial trial by end of year
- aim is to have two-way authentication with credentials only being entered in local authentication system
- use available open source solutions
  - not home brew (e.g. PIN) or commercial package
- held series of workshops to define requirements
- produced strawman proposal based on Shibboleth



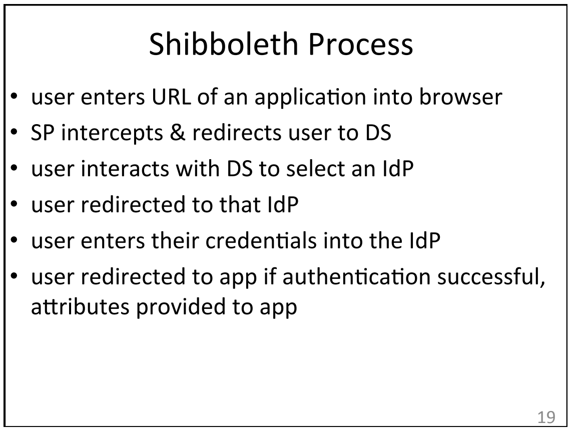
Shibboleth

- *"A standards based, open source software package for web single sign-on across or within organizational boundaries"*
- open source
- homed in Internet2
- used by hundreds of high ed institutions, government agencies and vendors
- talk with Marlena to get more information about Shibboleth and how it works



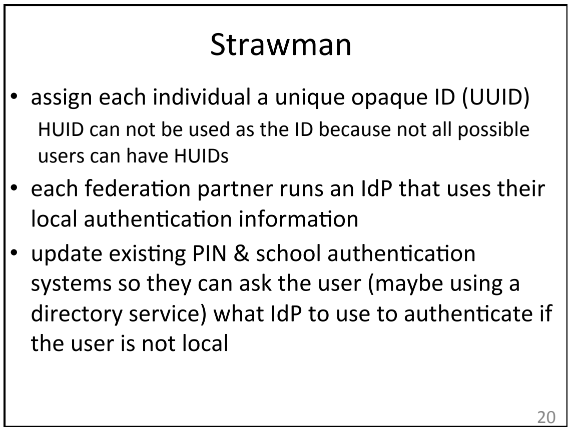
Shibboleth Components

- Identity Provider (IdP)
  - authenticates individuals
  - provides attributes about individuals
- Directory Service (DS)
  - used to locate correct IdP for user
- Service Provider (SP)
  - application front end
  - makes use of IdPs to authenticate individuals and get attribute information about them
  - processes digital signatures



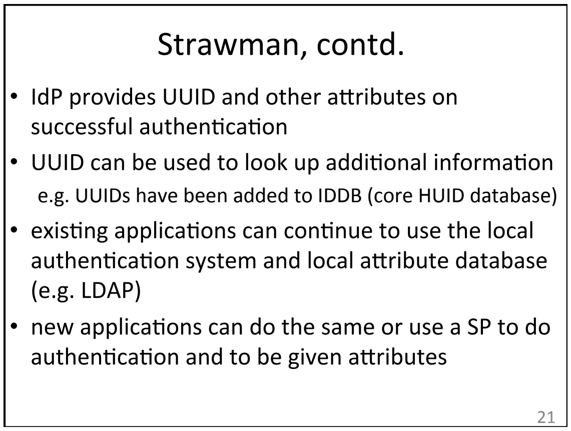
Shibboleth Process

- user enters URL of an application into browser
- SP intercepts & redirects user to DS
- user interacts with DS to select an IdP
- user redirected to that IdP
- user enters their credentials into the IdP
- user redirected to app if authentication successful, attributes provided to app



Strawman

- assign each individual a unique opaque ID (UUID)
  HUID can not be used as the ID because not all possible users can have HUIDs
- each federation partner runs an IdP that uses their local authentication information
- update existing PIN & school authentication systems so they can ask the user (maybe using a directory service) what IdP to use to authenticate if the user is not local



Strawman, contd.

- IdP provides UUID and other attributes on successful authentication
- UUID can be used to look up additional information
  e.g. UUIDs have been added to IDDB (core HUID database)
- existing applications can continue to use the local authentication system and local attribute database (e.g. LDAP)
- new applications can do the same or use a SP to do authentication and to be given attributes

Strawman, contd.

- provides two-way authentication and provides attributes
- assumes local authentication system can use provided attributes, or attributes looked up based on provided attributes (e.g. UUID) to deal with user

  e.g. a user that does not have a HUID will not be able to use an app that uses HUIDs as its internal key

  even though the user might be able to be authenticated

InCommon

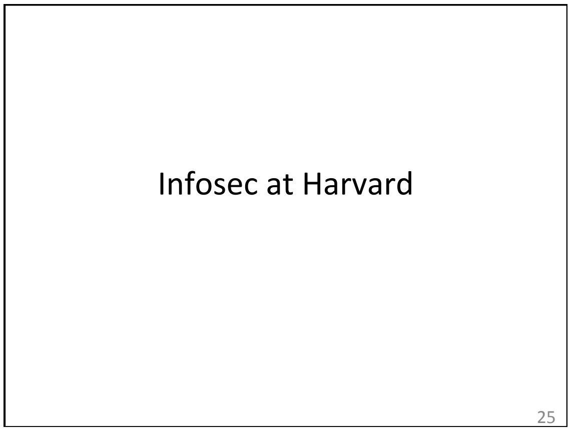
- Shibboleth-based higher-ed identity management federation based in Internet2
- permits university users to access InCommon resources using their university credentials without exposing those credentials
- university runs an IdP to authenticate university users to SPs run by InCommon partners and to provide attributes to those SPs
- currently: 354 High Ed, 28 government and 143 vendor participants

InCommon Contd.

- working on meeting InCommon requirements for participation
- test IdP up and running (Marlena)

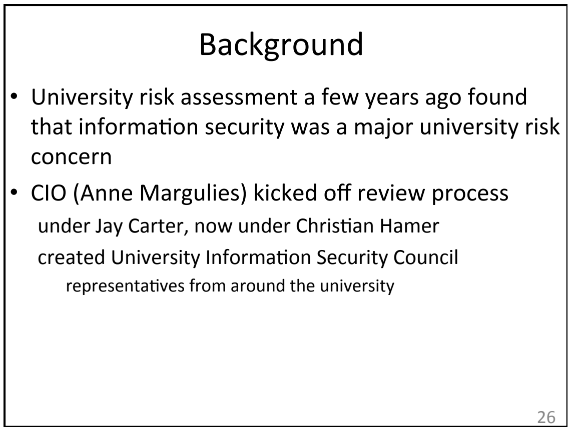
  uses PIN2 to authenticate, LDAP & IDDB for attributes
- production IdP planned for summer
- many policy decisions required before going live

HATHI TRUST Digital Library



Infosec at Harvard

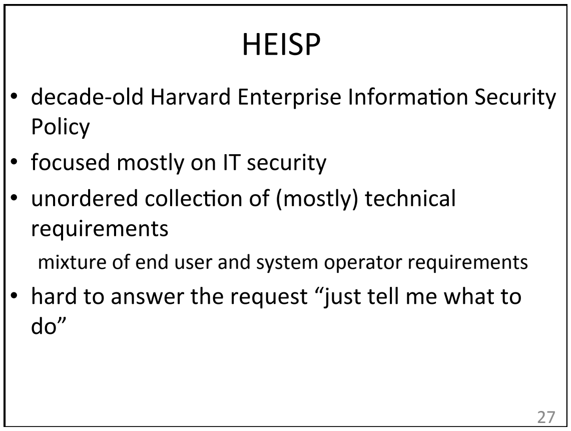
25



Background

- University risk assessment a few years ago found that information security was a major university risk concern
- CIO (Anne Margulies) kicked off review process
  - under Jay Carter, now under Christian Hamer
  - created University Information Security Council
    - representatives from around the university

26



HEISP

- decade-old Harvard Enterprise Information Security Policy
- focused mostly on IT security
- unordered collection of (mostly) technical requirements
  - mixture of end user and system operator requirements
- hard to answer the request “just tell me what to do”

27

HRDSP

- newer Harvard Research Data Security Policy
- technical requirements & processes for protecting (mostly) human subject information
  - general information security policies
  - assignment of responsibilities
  - checklists listing requirements
    - if you can say "yes" to all checklist items you are meeting the requirements

28

Information Categories

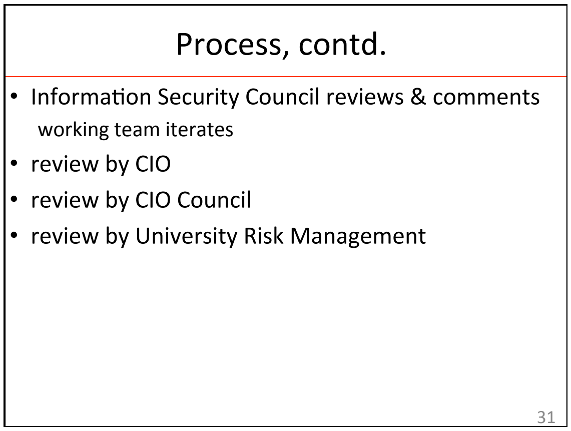
- HEISP: 3 categories
  - High Risk Confidential Information (HRCI)
  - other confidential information
  - non-confidential information
- HRDSP: 5 categories
  - very high risk (no network connections) information
  - HRCI
  - other confidential information
  - information university has decided to keep confidential
  - non-confidential information

29

Process being Followed

- "working team" proposing to information security council
  - Christian Hamer – University Security
  - Benoit Gaucherin – HLS
  - Jim Schwartz – HBS
  - Ken Carson – Provost/Research
  - Peter Katz – OGC
  - Scott Bradner – CTO's office
  - + Liz Eagan (keeping process running)

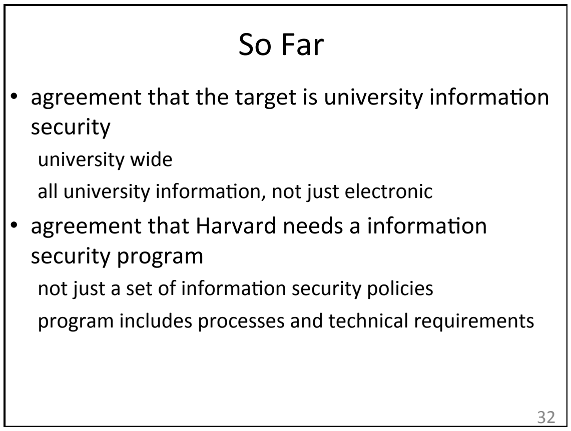
30



Process, contd.

- Information Security Council reviews & comments
  - working team iterates
- review by CIO
- review by CIO Council
- review by University Risk Management

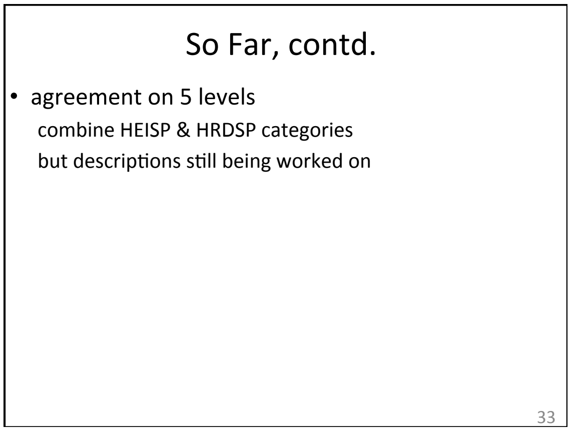
31



So Far

- agreement that the target is university information security
  - university wide
  - all university information, not just electronic
- agreement that Harvard needs a information security program
  - not just a set of information security policies
  - program includes processes and technical requirements

32

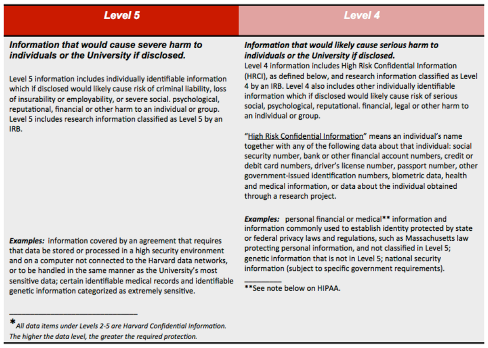


So Far, contd.

- agreement on 5 levels
  - combine HEISP & HRDSP categories
  - but descriptions still being worked on

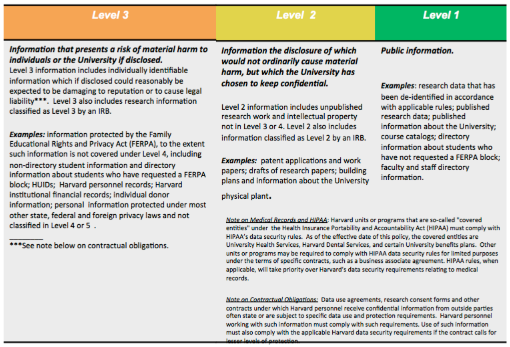
33

Information Classification



Level 5	Level 4
Information that would cause severe harm to individuals or the University if disclosed. Level 5 information includes individually identifiable information which if disclosed would likely cause risk of criminal liability, loss of insurability or employability, or severe social. psychological, reputational, financial or other harm to an individual or group. Level 5 includes research information classified as Level 5 by an IRB. ***Examples:*** information covered by an agreement that requires that data be stored or processed in a high security environment and on a computer not connected to the Harvard data networks, or to be handled in the same manner as the University's most sensitive data; certain identifiable medical records and identifiable genetic information categorized as extremely sensitive. ______________________________ * *All data items under Levels 2-5 are Harvard Confidential Information. The higher the data level, the greater the required protection.*	***Information that would likely cause serious harm to individuals or the University if disclosed.*** Level 4 information includes High Risk Confidential Information (HRCI), as defined below, and research information classified as Level 4 by an IRB. Level 4 also includes other individually identifiable information which if disclosed would likely cause risk of serious social, psychological, reputational. financial, legal or other harm to an individual or group. "High Risk Confidential Information" means an individual's name together with any of the following data about that individual: social security number, bank or other financial account numbers, credit or debit card numbers, driver's license number, passport number, other government-issued identification numbers, biometric data, health and medical information, or data about the individual obtained through a research project. ***Examples:*** personal financial or medical** information and information commonly used to establish identity protected by state or federal privacy laws and regulations, such as Massachusetts law protecting personal information, and not classified in Level 5; genetic information that is not in Level 5; national security information (subject to specific government requirements). ________ **See note below on HIPAA.

Information Classification, Contd.



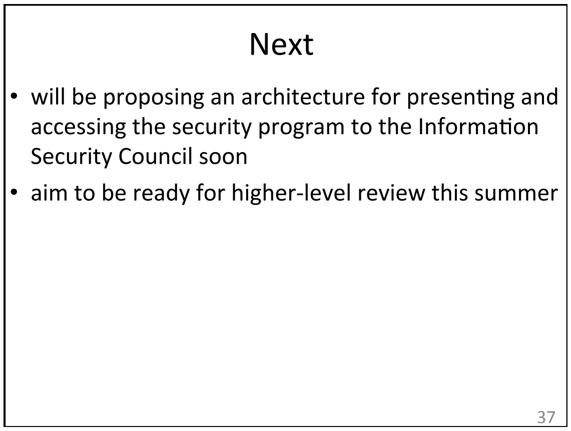
Level 3	Level 2	Level 1
Information that presents a risk of material harm to individuals or the University if disclosed. Level 3 information includes individually identifiable information which if disclosed could reasonably be expected to be damaging to reputation or to cause legal liability***. Level 3 also includes research information classified as Level 3 by an IRB. ***Examples:*** information protected by the Family Educational Rights and Privacy Act (FERPA), to the extent such information is not covered under Level 4, including non-directory student information and directory information about students who have requested a FERPA block; HUIDs; Harvard personnel records; Harvard institutional financial records; individual donor information; personal information protected under most other state, federal and foreign privacy laws and not classified in Level 4 or 5 . ________ ***See note below on contractual obligations.	***Information the disclosure of which would not ordinarily cause material harm, but which the University has chosen to keep confidential.*** Level 2 information includes unpublished research work and intellectual property not in Level 3 or 4. Level 2 also includes information classified as Level 2 by an IRB. ***Examples:*** patent applications and work papers; drafts of research papers; building plans and information about the University physical plant.	***Public information.*** ***Examples***: research data that has been de-identified in accordance with applicable rules; published research data; published information about the University; course catalogs; directory information about students who have not requested a FERPA block; faculty and staff directory information.

Note on Medical Records and HIPAA: Harvard units or programs that are so-called "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA) must comply with HIPAA's data security rules. As of the effective date of this policy, the covered entities are University Health Services, Harvard Dental Services, and certain University benefits plans. Other units or programs may be required to comply with HIPAA data security rules for limited purposes under the terms of specific contracts, such as a business associate agreement. HIPAA rules, when applicable, will take priority over Harvard's data security requirements relating to medical records.

Note on Contractual Obligations: Data use agreements, research consent forms and other contracts under which Harvard personnel receive confidential information from outside parties often state or are subject to specific data use and protection requirements. Harvard personnel working with such information must comply with such requirements. Use of such information must also comply with the applicable Harvard data security requirements if the contract calls for lesser levels of protection.

So Far, contd.

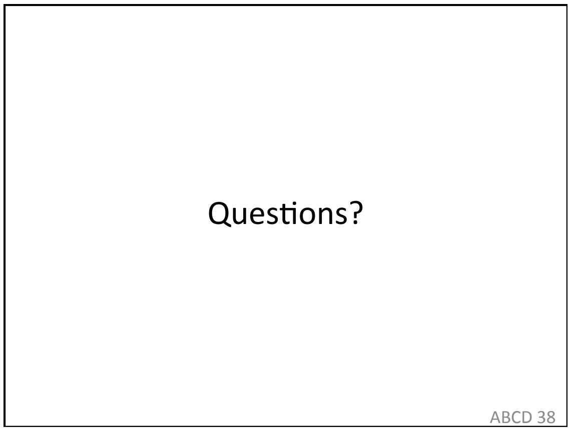
- agreement that things should be organized so that a person can see what they need to know
  - not everything (but can get to everything if they want)
  - "tell **me** what **I** need to do"
- presented a information security program to Information Security Council for discussion
- presented a set of draft policy statements to Information Security Council for discussion



Next

- will be proposing an architecture for presenting and accessing the security program to the Information Security Council soon
- aim to be ready for higher-level review this summer

37



Questions?

ABCD 38