Information Technology
Managing Information Assets

Stephen D. Franklin
franklin@uci.edu
http://webfiles.uci.edu/franklin
What you need to know

- IT resources to be managed
- What’s available on your campus
- Systems/project management principles
- Policies, laws & other legal considerations
- Security Awareness: Risk Assessment, Mitigation & Monitoring
- Privacy & Information Security Considerations
- Resources to help you
IT Resource Management

Managing

• People (IT staff, user support, programmer analysts)
• Data/Information (e.g., electronic records, databases)
• IT Infrastructure
  – Systems (e.g., departmental billing system)
  – Software (e.g., “productivity” software)
  – Hardware (e.g., servers, desktops, laptops, PDAs)
• Contractual Relationships

UC Jargon: EIR = Electronic Information Resource(s)
ESI = Electronically Stored Information
Information Technology Basics

• Role of desktop systems and mobile devices
• Role of application systems in supporting business processes
• Role of network (web) & its available resources
• Security Risk Assessment
  – Network Security
  – Computer (Server, Desktop, Laptop) Security
  – Data Security ➔ Information Security

IT is only one part: Technical and “Social”
What’s Available?

Ask

1. Is something close already available?
2. Is the data already available electronically?
3. How can this integrate with existing (and anticipated) systems or services? Should it?
4. What about privacy and security?

Be Proactive!
IT Systems/Project Management, 0

“But I don’t manage IT systems/projects”

1. IT systems/projects may be “just” configuration/deployment

2. Systems/Projects that are “not IT” often (increasingly) have significant IT components.

3. IT (security) awareness
   – We all have to manage our own use.
   – “Social Engineering” weaknesses (e.g., “phishing,” “spear phishing,” …)
IT Systems/Project Management, 1

IT projects differ from other projects:
1. Changing technology, expectations, skills
2. Vendor viability/stability
3. Interactions with legacy systems
4. Technical staff
5. Increased Security Risks
IT Systems/Project Management, 2

IT projects must be:

1. Well Defined
   (Avoid scope creep. Consider scale.)

2. Cost Effective

3. Compatible

4. Sustainable (change control)

5. Secure and Auditable
UC Electronic Communications Policy

• Privacy, confidentiality, and security
  – Allowable Use includes use “for incidental personal purposes”

• Key points:
  – “Nonconsensual access”
  – ”System Monitoring” (was “Unavoidable Inspection”)
  – Definitions of Public Records and University Administrative Records as in BFB-RMP-1 & BFB-RMP-8
  – Encryption advisory and guidelines as in BFB-IS-3
  – Retention and disposition as in BFB-RMP-2
Electronic Information Security

UC BFB-IS-3 provides EIS guidelines

*(Revision/replacement underway)*

- Local campus implementation, coordination
- Key points
  - Covers (all) “activities in support of the University’s mission”
  - Incident response and planning
  - “Physical” security including mobile devices and archives/backups

*Information Security is Everyone’s Business*
Intellectual Property Laws & Policies

DMCA – Digital Millennium Copyright Act
- Provides for limits to the liability of online service providers who are unaware of violations
- Each campus has a designated agent to receive and handle notices of infringement
- Different rules for cases related to faculty or graduate students performing teaching or research than for students, faculty and staff in general

Intellectual Property (IP) is Central to Universities
- DMCA is very visible but only a (small) part of universities’ copyright picture
- Copyright is only part of IP picture
Policies, Laws & Regulations

• FERPA
  Family Education Rights Privacy Act
  – Privacy of student education records.
  – Allows students to block access to their information or even its existence.

• HEOA
  Higher Education Opportunity Act, 2008
  – Student authentication in distance learning
  – University responsibilities in copyright compliance
Policies, Laws & Regulations

HIPAA = Health Insurance Portability & Accountability Act

- Protected Health Information (PHI)
  - Past, present or future physical or mental health or condition
  - Provision of or payment for health care to the individual
- Privacy regulations apply to PHI in any form or media: electronic, paper, or oral
- Security regulations apply to electronic PHI
Personal Information Security Laws

California 2002 SB 1386 & 2007 AB 1298

Personal Information in Computerized Data
(California Civil Code 1798.29 & 1798.82-1798.84)

Must notify about security breach disclosing

“Personal Information” = Name & any of these:

– Social security number
– Driver's license or California ID Card number.
– Account number, credit or debit card number, in combination with any information that would permit access to an individual's financial account.
– Medical or Health Insurance Information
Electronic Discovery ("e-discovery")
("discovery" = pretrial disclosure)

- Federal Rules of Civil Procedure mandate the identification & preservation of Electronically Stored Information (ESI) when one “reasonably should know that the evidence may be relevant to anticipated litigation.”
- Increasingly an issue with use of services outside of University control:
  - Where such information is stored and what access the University has to it
Policies, Laws & Regulations

• More of all of these for research data.
• In general, more of all of these on the way.
  – Identity theft a driving concern.

• PCI Data Security Standards
  PCI = Payment Card Industry = credit/debit cards
  PCI Data Security Standards are contractual obligation for those accepting payment via credit/debit cards

Best Advice: Consult Local Experts
Other Considerations/Concerns

• Immature/Evolving Policies & Practices on
  – BYOD (Bring Your Own Device)
  – Individually bought “Apps”
    • Vendor models vs (?) Institutional expectations
• “Outsourcing” or “Sharing” Confidential/Private/Restricted/Sensitive Information
• Use of “Third Party” (“Off-Campus”) Services With or Without (!) University Contract
• New (types of) Resources vs (?) Existing Models/Expectations/Constraints
  – Personal/Individual vs (?) Institutional
What is “IT Security”?

• “Information Technology” resources
  – Computer networks
  – Computers: “Servers,” Desktops, Laptops
  – Portable computing & data storage devices
  – Data stored (“at rest”) or being transmitted

UC jargon for these is “EIR”
  = “Electronic Information Resources”

• Security =
  Blocking unauthorized uses while
  Maintaining legitimate use

Five Scarey Pages Coming Up!

Fall 2013          Managing Information Assets          franklin@uci.edu-18
What are the risks?

- Unauthorized Access to Restricted or “Sensitive” Information
- Compromised Computer System ("compromised" = unauthorized access)
  - Attacks on network or other computers
  - Normal work blocked/impeded
  - Data/Information destroyed or altered
  - Restricted/Sensitive Information Disclosed
The Risks are Real

- Lost laptops and portable storage devices
- Data/Information “left” on public computers
- Data/Information intercepted in transmission
- Spyware, “malware,” “keystroke logging”
- Unprotected computers infected within seconds of being connected to the network. Thousands/Millions/??! of attacks every day

Data/Information Where It Does Not NEED To Be!
The Problem is Growing

1. Increasing number of attacks
   (Educational Security Incidents: http://www.adamdodge.com/esi/)
2. Security exploits spread in
   minutes (seconds), not days (hours)
3. “Script Kiddies” use powerful tools
4. Serious hackers have even better tools

**Opportunistic Exploitation** Increases with
Increased Publicity/Awareness

Ad Hoc & Organized Criminal Networks
“Sensitive” Data

- Passwords
- Research data
- Human resources personnel files
- Student information
- Email messages
- Professor’s contact list
- Personal phone numbers
- Home address
- Birth date
- Ethnicity information
- Gender information
- ...

Would you want such information about you in unknown/everyone’s hands?

How would someone more sensitive feel/react?
Why care about (EIR) Security

1. Legal responsibilities
2. Institutional & Personal Reputation & Trust
3. Lost Time, Lost Work
4. Denial of Service
5. Cost of Remediation
6. Real risks/threats and Real consequences

Even “small” incidents can be “Big Trouble”
Electronic Information Security

- IS-3 (Revision/replacement underway) framework
  - Comprehensive
  - Campus-level coordination
  - Identify and Limit Risk \textbf{Limit} ≠ \textbf{Eliminate}

- Technical measures
  - May need administrative backing.
    For example, in meeting minimum standards (requirements) for network-connected devices; scanning & monitoring

- “Social” measures (“Social Engineering”)
  \textbf{Security Awareness, Reaching Everyone}
Why Lock Your Laptop/Tablet/Phone?

And Someone Stole My Identity.
Where are the risks?

Security Breach Notifications to the California Office of Privacy Protection

- 46% Lost or stolen laptops or other devices
- 21% Hacking (may include social engineering)
- 11% Web site exposures
- 5% Insiders
- 5% Improper disposal
- 5% Mis-sent mail/e-mail
Security Awareness

1. Use/store restricted/sensitive information very carefully/sparingly
2. Good password practices
3. Secure transmission: VPN, https, ssh, ...
4. Be very cautious with email and web
5. Encrypt (or de-identify) data on mobile devices and store definitive copy elsewhere
6. Archive information on professionally managed systems
7. Keep critical software up to date: patches and virus protection
Mobile Devices & Communications

1. **Assume the device will be lost or stolen**
2. Limit the information stored.
3. Encrypt or de-identify the information.
   (“De-identify” = Require access to data stored elsewhere to make this information of value.)
4. Keep a Current, Secure backup.
   (Warning: Backups can amplify security risk.)
5. **Use Secure Communications**
6. **Even Greater Care** is needed when using equipment other than “your own”
   (“Keystroke loggers” are always a possibility.)
IT Security Awareness Summary

1. Technical measures/staff are key, but they “can only do so much”
2. “End user” responsibility
3. Balance technical and “social”
4. Areas of continued & growing risk:
   1. Information where it doesn’t have to be
   2. Mobile devices, “backups,” “spare copies”
   3. Insecure communication and passwords
   4. End user inattention and lack of caution
5. Balance Costs, Risks and Convenience
Third Party (Off Campus) Services

• Many Excellent Ones
• Attractive
  – Functionally
  – Technically
  – Financially
  – Contractually (?)
• Personal Discovery/Use ➔ ?
  University Use (!?)
Third Party (Off Campus) Services

• Governed by contracts with University?
  – Such contracts involve effort and time
  – Service Delayed is(?) Service Denied
    (Classic Convenience/Confidence tradeoff)
  – Consequences of going without such contracts
  – “Consumer-grade” End User License Agreements
    (aka “EULAs”)

• Use of such services is just a fact of life
  – Many Benefits & Definite Risks
Where’s My Information?

The Cloud Ate My Homework.
Changes & Constants

- “Mainframe” to PC + Network
  ~1985 to ~1997
- PC + Network to Mobile + “Cloud”
  ~2009 to ~2016(?)
- Institutional + Individual
- “Right” ↔ “Reasonable”
- Convenience ↔ Security
UC President's Privacy and Information Security Initiative (P&ISI)

Privacy is Fundamental to the University
Long an essential part of its culture
- Underpins academic and intellectual freedoms key to its mission
- Basis for an ethical and respectful workplace
- Paired with Information Security, critical to stewardship of information entrusted to it
Why Now?

- Changing Technologies and Social Situations/Expectations
- Consequences of failure (e.g., breaches)
- Proliferating obligations (e.g., law, regulation, etc.)
- Proliferating partnerships with external vendors
- Tensions between privacy and information security
- Overlapping policy jurisdictions need adjudication
- How to balance P&IS with other values and obligations
Charge to P&ISI Steering Committee

Considering what’s appropriate for UC in today’s world, recommend:

• Overarching Privacy Framework
• Governance, implementation and accountability structures
• Formal ongoing process to address technical and societal changes impacting privacy and information security
• Specific actions to implement the framework

(Working Group developed concepts and recommendations under Steering Committee’s direction)
P&ISI Deliverables

• Definitions
• Recommendations providing overarching framework guiding UC decision-making and policy development when privacy is involved.
• Implementation schedule
Autonomy Privacy
Ability of individuals to conduct activities without concern of or actual observation.

Information Privacy
The appropriate protection, use and dissemination of information about individual, protecting information about individuals.

Information Security
Protection of all information and infrastructure resources from unauthorized access, which could compromise their confidentiality, integrity, and availability of those resources.
P&ISI Recommendations

1. Adopt UC Statement of Privacy Values, Privacy Principles, and Privacy Balancing Process (Principles for both Autonomy and Information Privacy)

2. Campus Privacy and Information Security Boards (Joint AcademicSenate-Administrative board)

3. System-wide Privacy and Information Security Board (Awaiting campus experience, with Office of Ethics and Compliance serving in the interim)

4. Campus Privacy Officials (An operational/management point, need not be new person, at least a new responsibility)
P&ISI Implementation Schedule

2013-14
- Adopt committee recommendations
- Board formations
- Privacy Officials designated
- System work group – policies and communication
- Training and education

2014-15
- Training and education
- Build out campus privacy programs
- Collect metrics and evaluate overall approach

2015 and beyond
- Revise approach according to feedback received
- Establish privacy reviews
- Review and share balancing cases
P&ISI Key Outcomes

- Identifying and distinguishing *autonomy privacy* from *information privacy*, and relating them to *information security*
- Integrating autonomy privacy and information privacy into a holistic framework led by the University’s mission and values
- Allowing for institutional deliberation across values, obligations, policies, and jurisdictions through the Boards
- Increased awareness and communication
UC IT Leadership Council (ITLC)

- Chief Information Officers (CIO's) and other senior IT leaders
- Regular Meetings with Campus Reports
- Initiatives
- Specifications for “corporate systems”
- Sponsor/Participate in Conferences, Awards
UC ITLC’s Primary Purposes

• Provide IT Leadership
• Promote Inter-Campus IT Collaboration
• Guide Development of IT Applications & Services
• Promote IT Policy Strategy and Development
• Encourage Collaboration among UC Constituencies
• Ensure Requisite IT Infrastructure
• Seek Economies of Scale
• Develop and Promote Funding Strategies
• Facilitate Information Flow and Responsiveness
• Represent UC in External Forums
You Are Not Alone

Many Resources Available:
- Central IT organizations/experts on security, etc.
- Internal Audit
- Records Management contacts & online resources
- Campus/General Counsel
- Organizations like NACUBO and EDUCAUSE: meetings, training, email lists, web sites
- UC-wide groups and email lists
- Magazines, journals
- Peers
- The Web
Web Sites, 1

- UC Electronic Communications Policy (ECP)
  [http://policy.ucop.edu/doc/7000470](http://policy.ucop.edu/doc/7000470)
- UC Business and Finance Bulletins (BFB) within
  [http://policy.ucop.edu/policies-by-subject-area/](http://policy.ucop.edu/policies-by-subject-area/)
  - BFB-IS-3, Electronic Information Security
    [http://policy.ucop.edu/doc/7000543](http://policy.ucop.edu/doc/7000543)
  - BFB-RMP-1, University Records Management Program
    [http://policy.ucop.edu/doc/7020453](http://policy.ucop.edu/doc/7020453)
  - BFB-RMP-2, Records Retention and Disposition
    [http://policy.ucop.edu/doc/7020454](http://policy.ucop.edu/doc/7020454)
  - BFB-RMP-8, Legal Requirements on Privacy of and Access to Information
    [http://policy.ucop.edu/doc/7020454](http://policy.ucop.edu/doc/7020454)
Web Sites, 2

- Copyright and DMCA (Digital Millennium Copyright Act)
  [http://www.ucop.edu/irc/policy/copyright.html](http://www.ucop.edu/irc/policy/copyright.html)
  [http://www.universityofcalifornia.edu/copyright/](http://www.universityofcalifornia.edu/copyright/)
- FERPA (Family Educational Rights & Privacy Act)
- HIPAA (Health Insurance Portability & Accountability Act)
- California Privacy Laws and Legislation
  [http://www.privacy.ca.gov/privacy_laws.htm](http://www.privacy.ca.gov/privacy_laws.htm)
  [http://www.privacy.ca.gov/privacy_leg.htm](http://www.privacy.ca.gov/privacy_leg.htm)
- NACUBO (National Association of Colleges & University Business Officers)
- EDUCAUSE
  [http://www.educause.edu/](http://www.educause.edu/)
Web Sites, 3

- UC Privacy and Information Security Initiative (P&ISI)
  http://www.ucop.edu/information-technology-services/initiatives/privacy-and-information-security.html
- UC P&ISI Steering Committee Report to the President
- UC IT Security http://www.ucop.edu/information-technology-services/initiatives/uc-it-security/
- UC Information Technology Policy & Security
  http://www.ucop.edu/information-technology-services/initiatives/it-policy-and-security/
- UC ITLC (UC Information Technology Leadership Council)
  http://www.ucop.edu/information-technology-services/initiatives/information-technology-leadership-council.html
Security Awareness

1. Use/store restricted/sensitive information very carefully/sparingly
2. Good password practices
3. Secure transmission: VPN, https, ssh, …
4. Be very cautious with email and web
5. Encrypt (or de-identify) data on mobile devices and store definitive copy elsewhere
6. Archive information on professionally managed systems
7. Keep critical software up to date: patches and virus protection
1. Restricted/Sensitive Data

- Do you **need** to have restricted/sensitive information on your computer or portable storage device?
  - “Portable storage device” = Laptop, tablet, “smart phone,” USB memory key, SD card, external disk, DVD, CD, ...

- If not, get rid of your copy. Access the information securely from a secure site.

- If you need your own copy, protect it.

- If you don't have support, you must learn to protect it yourself.

- If you have support, follow its guidance.
2. Guidelines for “Good” Passwords

• Hard to guess, but memorable (for you)
  – Six to 12 characters in length.
  – At least 1 of each of the following:
    Upper case letters; Lower case letters;
    Digits; Special characters: ,._+-=!&%$#@()
  – Use digits for letters and syllables:
    1=L,l; 2=to,Z; 3=E; 4=for(e); 5=S; 8=ate
  – Possibly a short phrase (e.g., “2L8&2L1ttl3”)
  – Combine root with prefix, suffix, or infix

• Different passwords for different uses
• Change regularly.
“My Personal Password Practices”

• Different passwords for different uses
• If/When you need to write down passwords, use personal obfuscatory codings
  (e.g., “june+3” ↔ “3-neju”, 8↔a, 6↔i, 4↔o, 5↔u)

Maybe even when saved in an encrypted file

• Good free, open source encryption: http://www.truecrypt.org/

• Develop your own practices
  (They will be easier for you & safer. Why?)
3. Secure transmission

- “Secure connection” = no third-party eavesdropping
- https = A secure web connection
  - Look for the “s” in the URL of a web site.
    Typically, also the icon of a closed padlock
  - Doesn’t mean the site can be trusted, only that the connection to it is secure (encrypted)
- VPN = Virtual Private Network
  - A secure (encrypted) connection to a trusted network, using special software on your computer
4. Email & Web Security Awareness

• Do not open unexpected attachments
  – Cannot trust apparent source to be real source
  – Trusted source may send “dangerous” email
  – Unknown sources are to be trusted even less

• Do not send sensitive information via email

• HTML email = web page from unknown source

• Know source of current page and link target

• https for Security: “Look for the Lock”

All these “rules” are better viewed as cautions than as absolutes.
5. Protect Data on Mobile Devices

• Assume the device may be lost or stolen
• Store a definitive copy elsewhere on a secured system
• Encrypt or de-identify data on mobile devices
  – “De-identify” = Remove personal identifying information. This information can be replaced by other values which can be used to retrieve the original information from a secure system
6. Data Archiving & System Backup

- When a system has been compromised, the best or only way to restore it to service may require “rebuilding from scratch,” sacrificing any information not stored elsewhere.
- Archiving information creates another copy which also must be secured.
- Data on CDs or other mobile storage devices is vulnerable to loss or theft.
- Archive/backup on a professionally managed system.
7. Keep critical software up to date

- Unless advised otherwise by IT support staff, enable the automatic update feature on the software you have installed.
- Set your virus protection software for automatic updates and to scan e-mail before it is opened (especially e-mail attachments) and files whenever you open them.