

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 & regulations
- Security Awareness
 - Risk Assessment, Mitigation, & Monitoring
- 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)

Jargon: EIR = Electronic Information Resource(s)

Information Technology Basics

- Role of desktop systems
- 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:

- Is something close already available?
- Is the data already available electronically?
- How can this integrate with existing (and anticipated) systems or services? Should it?
- What about security?

Be *Proactive!*

November 2006

Managing Information Assets

franklin@uci.edu-5

Systems/Project Management, 1

IT projects can differ from other projects

- Changing technology, expectations, skills
- Vendor viability/stability
- Interactions with legacy systems
- Technical staff
- Increased security risks

November 2006

Managing Information Assets

franklin@uci.edu-6

Systems/Project Management, 2

IT projects must be:

- Well defined
(Avoid scope creep; consider scale)
- Cost effective
- Compatible
- Sustainable (change control)
- Secure and auditable

Systems/Project Management, 3

UC New Business Principles
(Our common goals)

- Enhance individual employee productivity
- Encourage collaboration and partnerships
- Manage technology as an investment
- Focus on outcomes
- Strive for simplification

UC Electronic Communications Policy

- Privacy, confidentiality, and security
- Allowable Use includes use “for incidental personal purposes”
- Key points updated in most recent version:
 - “Nonconsensual access”
 - “Unavoidable Inspection” → “System Monitoring”
 - Recently updated definitions of Public Records and University Administrative Records (RMP-1&8)
 - Encryption advisory and guidelines as in IS-3
 - Retention and disposition as in RMP-2

November 2006

Managing Information Assets

franklin@uci.edu-9

UC IS-3, Electronic Information Security

UC BFB IS-3 provides EIS guidelines

- Local campus implementation, coordination
- Key points in most recent version:
 - Scope now includes (all) “activities in support of the University’s mission”
 - Incident response and planning
 - “Logical” Security: Encryption, Access control (Authentication & Authorization)
 - “Physical” security including mobile devices

November 2006

Managing Information Assets

franklin@uci.edu-10

Policies, Laws & Regulations

- 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.
- Copyright & other Intellectual Property (IP)
 - Copyright issues include (*much*) more than DMCA
 - IP issues include (*much*) more than copyright

November 2006

Managing Information Assets

franklin@uci.edu-11

Policies, Laws & Regulations

- FERPA
Family Education Rights Privacy Act
 - Privacy of student education records.
 - Allows students to block access to their information or even existence.
- Gramm-Leach-Bliley Act (GLB)
“Financial Modernization Act of 1999”
- CAN-SPAM Act of 2003
“Controlling the Assault of Non-Solicited Pornography and Marketing”

November 2006

Managing Information Assets

franklin@uci.edu-12

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

Policies, Laws & Regulations

(California) SB 1386

Personal Information in Computerized Data

(California Civil Code 1798.29 & 1798.82-1798.84)

- “Personal Information”
Name and any of the following:
 - Social security number
 - Driver's license number or California ID Card number.
 - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

What is “IT Security”?

- “Information Technology” resources
 - Computer networks
 - Computers
 - “Servers,” Desktops, laptops
 - Portable computing and data storage devices
 - Data stored (“at rest”) or being transmitted
- UC jargon for these is “EIR” – “Electronic Information Resources”
- Security = Maintaining legitimate use & blocking unauthorized uses

What are the risks?

- Unauthorized access to restricted or “sensitive” information
- Compromised computer system (“compromised” = unauthorized access)
 - Attacks on network or other computer systems
 - 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 of attacks on campus networks every day

Data/Information where it does not Need to be

The Problem is Growing

- Increasing number of attacks
- Security exploits spread in minutes not days
- “Script Kiddies” use powerful tools
- Serious hackers have even better tools

Opportunistic exploitation increases with
increased publicity/awareness

Ad hoc & organized criminal networks

Personal Identity “Incidents”

People	Date	University
178,000	April 2004	San Diego State
380,000	May 2004	UC San Diego
207,000	May 2004	UCLA (2 thefts)
600,000	September 2004	UC Berkeley
430	November 2004	UC Irvine
7,000	February 2005	UC San Francisco
98,000	March 2005	UC Berkeley
120,000	March 2005	Boston College
107,000	April 2005	Tufts
34,000	August 2005	University of North Texas
106,000	April 2006	University of Texas at Austin
26,500,000	May 2006	US Government
367,000	May 2006	Ohio University
220,000	June 2006	Western Illinois University
170,000	July 2006	Nelnet (student loan company; missing tape)
64,000	September 2006	University of Texas San Antonio

November 2006

Managing Information Assets

franklin@uci.edu-19

“Sensitive” Data

Obvious examples

- Passwords
- Research data
- Human resources personnel files
- Student information
- Email messages

Less obvious examples

- Professor’s contact list
- Personal phone numbers
- Home address
- Birth date
- Ethnicity information
- Gender information

“Restricted” – Limited by law or policy

“Sensitive” – Would you want such information about *you* in unknown/public hands?

November 2006

Managing Information Assets

franklin@uci.edu-20

Why care about (EIR) Security

- Legal responsibilities
- Institutional & personal reputation & trust (e.g., identity theft)
- Lost time, lost work
- Denial of service
- Cost of remediation
- Real risks/threats and consequences

Even “small” incidents can be “Big Trouble”

Electronic Information Security

- IS-3 framework
 - Policy revision: Change of context/scope
 - Campus-level coordination
 - Identify and limit risk
- Technical measures
 - May need administrative backing. For example, Minimum standards (requirements) for network-connected devices; scanning & monitoring
- “Social” measures (“Social Engineering”) Security Awareness, Reaching Everyone

Security Awareness

(Fuller version at end of this presentation)

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

November 2006

Managing Information Assets

franklin@uci.edu-23

Mobile Devices and Communications

- *Assume the device will be lost or stolen*
- Limit the information stored
- Encrypt or de-identify the information
(“De-identify” = Require access to data stored elsewhere to make this information of value.)
- Keep a current and secure backup
Backups can amplify security risk
- Use secure communications
- Even greater care needed when using
equipment other than “your own”

November 2006

Managing Information Assets

franklin@uci.edu-24

IT Security Awareness Summary

- Technical measures/staff key, but “can only do so much”
- “End user” information security responsibility
- Balance technical and “social”
- Areas of continued & growing risk:
 - Information where it doesn’t have to be
 - Mobile devices, “backups,” “spare copies”
 - Insecure communication and passwords
 - End user inattention and lack of caution
- Balance costs, risks and convenience

November 2006

Managing Information Assets

franklin@uci.edu-25

UC Information Security Working Group

- April 2005: Initiated by UC President & Chancellors
- August 2005: Report focusing on “safeguards for restricted information in electronic form”
- Leadership Initiatives to
Ensure Information Security
“Information Security is an Exercise in Risk Management.”
- Management Initiatives to
Safeguard Restricted Data

November 2006

Managing Information Assets

franklin@uci.edu-26

UC ISWG Recommendations

- Leadership:
Chancellors (or their designates) develop
“guidelines to ensure compliance with standards of
accountability for data security breaches.”
- UC-wide communication campaign
- Information security training
- Handling of security incidents
- Policy updates
- Campus security programs
- Encryption
<http://www.ucop.edu/irc/itsec/uc/EncryptionGuidelinesFinal.html>

November 2006

Managing Information Assets

franklin@uci.edu-27

UC IT Leadership Council (ITLC)

- Chief Information Officers (CIO's) and other
senior IT leaders
- Quarterly Meetings with “Campus Reports”
- Initiatives (Federated Authentication Project)
- Specifications for “corporate systems
communications” (e.g., corporate budget
system, undergraduate admissions)
- Sponsor/Participate in Conferences, Awards

November 2006

Managing Information Assets

franklin@uci.edu-28

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

November 2006

Managing Information Assets

franklin@uci.edu-29

UC IT Guidance Committee

“... established to engage in a consultative, 18-month systemwide planning process to identify and recommend strategic directions to guide investments in information technology (IT) and the academic information environment.

The formation of this committee recognizes the increasingly important role that information technology will play in sustaining and enhancing the University's academic quality and competitiveness and in ensuring essential business effectiveness and efficiencies.”

— <http://www.universityofcalifornia.edu/itgc/charge/>

November 2006

Managing Information Assets

franklin@uci.edu-30

ITGC Work Group Focus Areas

- Advanced networking services
- Stewardship of digital assets
- Common information technology infrastructure
- High performance research computing
- Instructional technology
- Information technology in student life
- Scholarly collaboration

ITGC Outcome

“Issue a report that attempts to:

- “Identify **strategic directions for IT investments** that enable campuses to meet their distinctive needs more effectively while supporting the University’s broader mission, academic programs and strategic goals.
- “Promote the deployment of information technology services to **support innovation** and the enhancement of academic quality and institutional competitiveness.
- “**Leverage IT investment and expertise** to fully exploit collective and campus-specific IT capabilities.”

— <http://www.universityofcalifornia.edu/itgc/charge/>

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

November 2006

Managing Information Assets

franklin@uci.edu-33

Web Sites, 1

- UC Electronic Communications Policy (ECP)
<http://www.ucop.edu/ucophome/policies/ec/>
- UC Business and Finance Bulletins (BFB)
<http://www.ucop.edu/ucophome/policies/bfb/>
 - IS – Information Systems
<http://www.ucop.edu/ucophome/policies/bfb/bfbis.html>
 - IS-3, Electronic Information Security
<http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>
 - RMP – Records Management Practices
<http://www.ucop.edu/ucophome/policies/bfb/bfbrmp.html>
 - RMP-2, Records Retention and Disposition
<http://www.ucop.edu/ucophome/policies/bfb/rmp2.pdf>

November 2006

Managing Information Assets

franklin@uci.edu-34

Web Sites, 2

- Copyright and DMCA (Digital Millennium Copyright Act)
<http://www.ucop.edu/irc/policy/copyright.html>
<http://www.universityofcalifornia.edu/copyright/>
- FERPA (Family Educational Rights and Privacy Act)
<http://www.ed.gov/offices/OM/fpco/ferpa/students.html>
- HIPPA (Health Insurance Portability and Accountability Act) <http://www.hhs.gov/ocr/hipaa/>
- GLB (Gramm-Leach-Bliley) Act
<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>
- CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) <http://www.spamlaws.com/federal/can-spam.shtml>
- SB 1386 (now Ca Civil Code 1798.29 & 1798.82-.84)
<http://www.privacy.ca.gov/lawenforcement/laws.htm>

November 2006

Managing Information Assets

franklin@uci.edu-35

Web Sites, 3

- UC Information Technology Guidance Committee
<http://www.universityofcalifornia.edu/itgc/>
- UC ITLC (UC Information Technology Leadership Council)
<http://www.ucop.edu/irc/itlc/>
- UC Information Security Working Group Report
<http://www.ucop.edu/irc/initiatives/ucinfosecwg.html>
- IT Security at the University of California
<http://www.ucop.edu/irc/itsec/uc/>
- UC ITPSO (UC Information Technology Policy and Security Officers)
<http://itpolicy.berkeley.edu/UCITPSO>
- NACUBO (National Association of Colleges and University Business Officers) <http://www.nacubo.org/>
- EDUCAUSE <http://www.educause.edu/>

November 2006

Managing Information Assets

franklin@uci.edu-36

Thanks To...

- Marina Arseniev, UC Irvine – Assistant Director, Administrative Computing Services
- Mark Askren, UC Irvine – Assistant Vice Chancellor, Administrative Computing Services
- Marie Perezcastaneda, UC Irvine – Director, Business Services, Network & Academic Computing Services
- Dana Roode, UC Irvine – Assistant Vice Chancellor, Network & Academic Computing Services
- Dave Tomcheck, UC Irvine – Former Associate Vice Chancellor, Administrative & Business Services

Security Awareness

(Outline version)

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 a professionally managed system
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, PDA, “USB memory key,” 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,I; 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.

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. Protecting 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