



# *Information Technology*

## **Managing Information Assets**

Stephen D. Franklin

franklin@uci.edu

<http://webfiles.uci.edu/franklin>

October 2008

## **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
- 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)

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

## 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

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 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,” and “whaling”)

## IT Systems/Project Management,

### 1

IT projects can 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

## IT Systems/Project Management, 3

### UC New Business Principles (Our common goals)

1. Enhance individual employee productivity
2. Encourage collaboration and partnerships
3. Manage technology as an investment
4. Focus on outcomes
5. 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”
  - “System Monitoring” (was “Unavoidable Inspection”)
  - Definitions of Public Records and University Administrative Records as in RMP-1 & RMP-8
  - Encryption advisory and guidelines as in IS-3
  - Retention and disposition as in RMP-2

## Electronic Information Security

UC BFB IS-3 provides EIS guidelines

- Local campus implementation, coordination
- Key points
  - Scope 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 and archives/backups

## 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 existence.

## 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

## Policies, Laws & Regulations

Electronic Discovery (“e-discovery”)

(“discovery” = pretrial disclosure)

- Federal Rules of Civil Procedure mandate the Identification & Preservation of Electronically Stored Information (ESI) when one should “reasonably should know that the evidence may be relevant to anticipated litigation.”

1. [http://en.wikipedia.org/wiki/Electronic\\_discovery](http://en.wikipedia.org/wiki/Electronic_discovery)
2. <http://www.fjc.gov/public/home.nsf/pages/196>
3. [http://www.uscourts.gov/rules/EDiscovery\\_w\\_Notes.pdf](http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf)

## 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.
  - Senate bill S. 2168: Identity Theft Enforcement and Restitution Act of 2007 now (September 2008) in House which also has H.R. 6060: Identity Theft Enforcement and Restitution Act of 2008
  - FTC Business Guide (a guide, not regulation): “Protecting Personal Information”  
<http://www.ftc.gov/infosecurity>

## Other Legal Considerations

### 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

“Outsourcing” or “Sharing”

Confidential/Private/Restricted/Sensitive Information

## 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 = Maintaining legitimate use & blocking unauthorized uses

***Six Scarey Pages Coming Up!***

## 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/Millions/??! of attacks every day

***Data/Information Where  
It Does Not NEED To Be!***

## The Problem is Growing

1. Increasing number of attacks
2. Security exploits spread in minutes not days
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**

## Personal Identity “Incidents”

<u>People</u>	<u>Date</u>	<u>University</u>
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
98,000	March 2005	UC Berkeley
120,000	March 2005	Boston College
107,000	April 2005	Tufts
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)
45.7 to 94 million	July 2005(?) – Feb 2007	TJX (TJ Maxx, Marshalls, etc.=2,500 stores)
800,000	November 2006	UCLA
63,000	1996 – April 2007	US Census Bureau

Educational Security Incidents: <http://www.adamdodge.com/esi/>

## “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?**

## Why care about (EIR) Security

1. Legal responsibilities
2. Institutional & Personal Reputation & Trust (e.g., identity theft)
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 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

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

## “My Personal Password Practices”

- Different passwords for different uses
- If/When you need to write down passwords, use personal obfuscatory codings:  
“june+3” ↔ “3-neju”    “ff” ↔ “5” or “30”  
8 ↔ a, 3 ↔ e, 6 ↔ i, 4 ↔ o, 5 ↔ u  
Even when saved in an encrypted file
- Good free, open source encryption:  
<http://www.truecrypt.org/>
- Develop your own practices

## 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

## 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  
Backups can amplify security risk.
5. Use Secure Communications
6. Even Greater Care is needed when using equipment other than “your own”  
“Keystroke loggers” 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

## 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

## UC ISWG Recommendations

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

## 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

## 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://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>

## 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 & Privacy Act)  
<http://www.ed.gov/offices/OM/fpc/ferpa/students.html>
- HIPAA (Health Insurance Portability & Accountability Act) <http://www.hhs.gov/ocr/hipaa/>
- Ca Civil Code 1798.29 & 1798.82-.84 (SB 1386 & AB 1298) <http://www.privacy.ca.gov/lawenforcement/laws.htm>
- NACUBO (National Association of Colleges & University Business Officers) <http://www.nacubo.org/>
- EDUCAUSE <http://www.educause.edu/>

## Web Sites, 3

- UC ITLC (UC Information Technology Leadership Council) <http://www.ucop.edu/irc/itlc/>
- UC Information Technology Guidance Committee <http://www.universityofcalifornia.edu/itgc/>
- 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://technology.berkeley.edu/policy/UCITPSO/>

## Thanks To...

- Marina Arseniev, UC Irvine – Associate 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

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, 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. 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