

IS-3 Electronic Security Coordination Group

July 29, 2005

Agenda

- A. Brief Update
- B. EIR Inventory Status
- C. Security Situation in Your Area
- D. Broad End-User Security Training
- E. UCInet Security Guidelines

Brief Update

- Many, many security breaches in the news
- UCB Incident of March 11
 - Laptop stolen that had sensitive data for 98,000 current and former graduate students
 - UCB reaction
 - Public reaction to this and other incidents
- UC Information Security Work Group
 - Formed to assess UC's efforts to safeguard restricted data and recommend further initiatives

Update: UCI Security Strategy

- Risk Assessment:
 - Sensitive Data EIR Inventory
 - Sharing results with UCI leadership
- Coordination/Outreach:
 - IS-3 Area Coordinators covering entire campus
 - “Administrative” and “Academic” IS-3 coordination groups
 - Planned new NACS Security Team position
 - End-user online interactive data/network security course
- Central end-user security web resource
 - security.uci.edu? Cybersecurity.uci.edu?

Update: UCI Security Strategy

- Policy:
 - IS-3 (Is local UCI policy needed?)
 - UCInet connected-device security guidelines
- Central services:
 - Network quarantine, network registration
 - Firewall, IDS for VPN, possibly for wireless network as well
 - NACS departmental firewall services
 - Continue to investigate commercial solutions to enhance network security

EIR Inventory Status

- EIRs entered as of yesterday:
 - A&BS: 15; Libraries: 2; NACS: 6
 - RGS: 6; Student Affairs: 24
 - Advancement: 1; Extension: 21
- Questions about tool?
- How are we doing for an October 1 deadline?
- How can we help?

Security Situation in Your Area?

- What aspect of data security is the greatest concern for your unit?
- How aware is your unit's upper management of the sensitive data maintained in the unit and the status of its security?

Security Situation in Your Area?

- Have you been able to eliminate any sensitive data fields from EIRs in your unit in response to growing privacy and security concerns?
- What is your unit's approach to patch management and virus protection?

Security Situation in Your Area?

- What can we do as a group to enhance security? What would you like central coordinators (AdCom, NACS) to do to enhance security?
- If a “security review team” comprised of UCI IT staff in several units was created, would your unit be interested in asking them to review the security of your higher risk EIRs? How important or valuable is this to do?

Broad End-User Security Training

- Goal: gain everyone's participation in enhancing security
- Online interactive tutorial
- If we expect all faculty and staff to run it, how long should it be?
- How do we get people to run it?
 - Gain support to make it "mandatory"?
 - Offer incentives of some sort?
- What sort of Incentives?

UCInet Security Guidelines

- Goal:
 - ensure people maintaining systems on UCInet know what they must to do make them secure
- Guidelines:
 - Musts, Shoulds
 - Desktop systems, network services/applications
- Policy? Consequences of not following guidelines?
- How do we get the word out?