March 4, 2011

Tina Darmohray, Assistant Vice President
and Chief Information Security Officer
Stanford Information Assets

- Stanford’s diversity results in many different types of information assets which the University wishes to protect:
  - Legal requirements
  - Contractual obligations
  - Strategic or proprietary worth
  - Business continuity
  - Data integrity
  - Prudent stewardship
Attack Targets

- Disclosure, destruction, or modification of non-public data (e.g., credit card, personal identity or health, donor, student); central Administrative Systems and copies

- Disclosure, destruction, or corruption of data & files of data at rest on the > 40K computers on open SUNet, including Restricted data, research results, etc.

- Data in transport such as files being copied across the net, sent via email, etc.

- Mobile computing devices, including laptops, smart phones, mobile storage devices, and home computers

- SPAM, Phishing, Fraud

- SCADA incident, e.g. taking over the phone system, commandeering machines and network resources

- Network Denial of Service affecting business continuity

- Nuisance factor
Data Breaches in Educational Industry

- Educational industry is a target
- Compromised machines
- Processing error / mis-handled data
- Stolen computers
- Insider threats, data disposal, physical loss of documents or media < 20% total
- Stanford’s network is attacked more than a million times a day; unprotected machines can be compromised within minutes of connecting to the network
The Cost of a Stanford Compromise

- August 2003 Campus-wide [non destructive] infection: $2M repair cost

- ‘05, ‘08 Credit Card data: consulting costs now; could be fined up to $500K

- June 2008 stolen laptop: > 60K individuals notified, > $1M
Stanford’s Information Security Solution

• Every computer user at Stanford is responsible for securing their computer and keeping Stanford data safe

• Stanford relies on its employees to adhere to and carry out its policies

• Managers make decisions which include:
  – Data classification
  – Data stewardship
  – Appropriate risk
Stanford Data Classification

• Non public data is classified into three categories: Prohibited, Restricted and Confidential data

• This data is subject to legal requirements of federal and state laws as well as contractual requirements, and Stanford’s desire to keep some information private

securecomputing.stanford.edu/data_class.html
Non-Public Data

• **Prohibited Data:**
  – Social Security Numbers
  – Credit Card Numbers
  – Financial Account Numbers
  – Driver’s License Numbers
  – Health Insurance Policy ID Numbers

• **Restricted Data:**
  – Student Records (one academic year)
  – Protected Health Information (PHI)
  – Passport and visa numbers
  – Research and other information covered by non-disclosure agreements
  – Export controlled information under U.S. laws
How Can You Protect Non-Public Data?

• Know when you are handling it

• Do not store non-public data on your computer unless you have a clear business need to do so

• If there is a business need to store non-public data on your computer, there are information security best practices and guidelines which should be followed
Be a Cautious Computer User

- Don’t open email attachments or clickable website addresses unless you are certain of their contents

- Be wary of potentially fake email messages; go directly to websites, rather than clicking through a link

- Never give personal or confidential information electronically unless you are certain of the website or service you are interfacing with and that it is secure

- Make sure you’re using a secure link; check for https:// or for the padlock icon in your browser window

- Take the online computer security awareness training: STARS course ISO-0001
Safe Computing

- Set passwords
- Stay up to date with patches; BigFix
- AntiVirus
- Encrypt data
- Secure connections when working remotely
- Use secure: email for non-public data
- Remove data before transferring or disposing of a computer
System Security Best Practices

- What is the policy?
  - Industry Best Practices

- Set passwords and change default settings
- Restrict access
- Limit services
- Encrypt data, and access
- Secure applications
- ...
  
  http://securecomputing.stanford.edu/iso-guidelines.html

- If you’re outsourcing services, the ASP must adhere to these requirements as well
Your Role as a Manager

• Your role at the university may include additional responsibilities

• Responsible for applying information security policies to systems, data, and other information resources under their care or control
  – Principle Investigators
  – Managers
  – Business & Data Owners

• Responsible for the application of information security policies to systems, data, and other information resources in their care at the direction of the business and data owners
  – System Administrators
  – Developers
BigFix Adoption

Active BigFix Subscriptions Over Time
with 8k boxes around summers (June 5 - September 20)
User Awareness Training

Completed Training
Whole Disk Encryption Adoption
Campus Network System Vulnerabilities

- Hosts with a High Risk Vulnerability
- Hosts with a Medium (but not High) Risk Vulnerability

Percent of Hosts

Year:
- 2004
- 2007
- 2010
Case Studies

• Credit card data
  – Decision to allow non-public data on unprotected machine

• Student health information
  – Under qualified personnel hired to handle non-public data

• White Hat role
  – Help Desk self-assigned forensics role

• Incident reporting
  – Employee directed to cover up incidents
Information Security Incident Response

• In the event data has been compromised, Administrative Guide Memo 67 – Information Security Incident Response outlines Stanford’s information security incident response

• Employees should report information security incidents involving non-public data to the Information Security Office

• The ISO performs an initial assessment and, if necessary, forms an incident response team

• Don’t touch the “crime scene” - the ISO will give you directions based on the initial assessment
Questions?

- Information Security Office:
  - 723-2911
  - security@stanford.edu

Directly:
- Tina Darmohray
  - 724-7661
  - tmd@stanford.edu