

Security Awareness Review

CSU
January 2006

CSU Security Awareness Training

Why Security Awareness Training?

- It's our responsibility.
- It's good business.
- It's the law.

Why Security Awareness Training?

It's our responsibility.

- We're custodians of non-public personal and financial data.
- We're responsible for ensuring the confidentiality, integrity and availability of that data.
- We all need to become educated regarding security best practices.

Why Security Awareness Training?

It's good business.

Security breaches can cause:

- Adverse media coverage
- Damage to CSU's reputation.
- Financial losses.

Why Security Awareness Training?

It's the law: FERPA and GLBA

- FERPA - The Family Educational Rights and Privacy Act of 1974 requires us to protect non-public student information.
- GLBA - The Gramm-Leach-Bliley Act requires financial institutions - including colleges and universities - to preserve the privacy, integrity and availability of nonpublic "personally identifiable" financial data.

What does FERPA have to do with CSU?

FERPA regulates a student's access to his/her educational records and prohibits unauthorized access.

- Many CSU employees have access to "covered data" under FERPA such as student:
 - Name and Address
 - Birth Date
 - Social Security Number and/or Student ID.
- Employees with access to student data must understand and comply with FERPA.

How does the GLBA apply to Higher Education?

We're NOT a financial institution... BUT...

- The Federal Trade Commission (FTC), which regulates GLBA compliance, has ruled that universities and colleges are financial institutions.
- Why? CSU processes student loans and engages in other activities that involve personal financial information.

If FERPA already mandates data privacy, why do we need the GLBA?

Federal Trade Commission regulations for implementing the Gramm-Leach-Bliley Act include:

- Privacy Rule
- Safeguarding Rule

What is the Privacy Rule?

The GLBA Privacy Rule:

- Focuses on how financial institutions share personal, non-public information.
- Mandates specific customer privacy measures.
- Requires customer notification of information-sharing practices (e.g. credit card privacy notices).

FTC states we're exempt from Privacy Rule as long as we remain in compliance with FERPA.

What is the Safeguarding Rule?

The GLBA Safeguarding Rule:

- Focuses on protecting “non-public, personally-identifiable” financial data from anyone WITHOUT a legitimate business or institutional need to know.

What is the Safeguarding Rule? (Cont.)

Requires financial institutions to take administrative, physical and technical measures to safeguard confidential customer data such as:

- Social Security Number

- Name, Address and Phone Number

- Credit Card and Bank Account Numbers

- Credit and Income Histories

- Income Tax Returns

What is Security Awareness?

May be defined as a basic understanding of:

- Potential threats to our information security.
- CSU policies and procedures for protecting our data.
- Employee behaviors and actions that can support or threaten information security.

WHAT are the major threats to our data?

- Cyber-threats ranging from malicious code (viruses, worms, Trojans) to denial of service attacks.
- Physical theft of data or equipment.
- Fire, electrical, water or other physical damage.
- Improper disposal of data.

WHO is a threat to our data?

- Over 300 million people now have access to the Internet- not all are well intentioned.
- Individuals who want to prove they can hack or disrupt a network for the fun of it.
- Sophisticated players who hack for profit (software pirates, identity thieves, phishers, etc.).
- Customers or employees with a grudge to settle.
- Authorized users.

World Wide Pirates

- Group arrested for selling pirated software, movies and music throughout the world.
- Took police forces from United States, United Kingdom, Australia, Poland and Slovakia to break up.
- Allegedly, group hacked into university and college computer networks world wide to “store, sell and serve” pirated materials.

http://www.theregister.co.uk/2004/08/24/anti-piracy_swoop/
CSU Security Awareness
Training

Identity Thieves

- Steal SSN, credit card number or other personal non-public information to commit fraud or other crimes.
- Use various methods to obtain data such as:
 - physical theft
 - “social engineering”
 - “phishing”

Physical Theft

Think the following headline could never make The Hartford Courant?

“Missing CSU hard drive contains student and employee data”

Physical Theft (Cont.)

That headline DID make the California papers:

- California State University (CSU) - Hard drive stolen from laptop.
- Hard drive - no bigger than business card - contained names and social security numbers of over 13,000 students and employees.

Source: [The Tribune SanLuisObispo.com](http://TheTribuneSanLuisObispo.com)

Social Engineers

- Also referred to as “pre-text callers.”
- Adept at obtaining unauthorized access to confidential data from unsuspecting victims.
- Pose as relative, potential landlord or mortgage processor to get student or employee information.

Phishers

- Use e-mail as primary mode of operation.
- Pose as legitimate businesses, e.g. Citibank or Ebay.
- Claim fictional security breach, system upgrade or other issue requires verification of personal information, password, etc.

Authorized Users

Users can pose a threat to our network and data by:

- Opening attachments which introduce viruses into the network.
- Downloading files from unknown or inappropriate sources.
- Not safeguarding confidential electronic and paper documents and files.
- Not safeguarding CSU property, such as laptops.

When a Security Breach Occurs...

- Negative publicity can cause intangible, long term damage.
- If individual can prove breach led to identity theft, university could incur financial damages.
- Identity theft not restricted to California or NYC.
- According to Federal Trade Commission 2003 figures, Connecticut ranked 23rd among states with the most ID theft complaints.

How is CSU Safeguarding our Data?

Safeguarding involves three key areas:

- Administrative
- Technical
- Physical

Administrative Safeguards

Establishing CSU Policies:

- Information Security
- Responsible Use
- Remote Access
- Administrative Access to Electronic Data
- Security Breach (i.e. incident reporting/handling)
- Cell Phone, Pager and Laptop Usage

Administrative Safeguards (Cont.)

Developing Procedures and Best Practices:

- Train all employees on basics of information security.
- Perform reference/background checks for new hires.
- Require all new employees to sign agreement to conform to CSU's policy for handling non-public customer information.
- Require all service providers (e.g. vendors, consultants) to sign agreement complying with GLBA.

Administrative Safeguards (Cont.)

- Limit access to CSU data to legitimate business need.
- Distribute policy and list of non-public information considered protected under GLBA and FERPA (e.g. name, account number, social security number, etc.)
- Post reminders regarding employee responsibilities in areas where non-public information is stored.

Administrative Safeguards (Cont.)

- Impose corrective measures for employee policy breaches.
- Perform internal/external audits to detect improper disclosures or theft of customer information; report and respond to findings.
- Establish policy to ensure prompt notification to customers should a security breach occur.

Administrative Safeguards (Cont.)

- Establish and enforce guidelines for disposing of outdated information.
- Develop record retention policy based upon state and federal guidelines.
- Designate department representatives to work with Finance regarding record disposal.

Technical Safeguards

- Store student and employee data on secure servers.
- Maintain up-to-date firewall hardware and software.
- Install and maintain virus protection software.
- Obtain and install security patches promptly.
- Encryption

Technical Safeguards (Cont.)

- Establish electronic audit trails/transaction monitoring.
- Develop and maintain procedures for securing back-ups and archived data.
- Develop contingency/disaster recovery procedures.
- Implement user identification and authentication mechanisms.
- Enforce mandatory password changes.

Physical Safeguards

- Restrict physical and electronic access to records storage areas, file cabinets, servers, etc. Lock file cabinets and storage areas containing non-public customer information.
- Protect computers, servers and records storage from fire, water, moisture, heat, electrical hazards.

Physical Safeguards (Cont.)

- Utilize Entry Card/Sonitrol intrusion detection mechanisms for building and sensitive area access.
- Erase confidential data from computers, CD's, disks, tapes and other electronic media.
- Supervise destruction of hardware.
- Implement password-protected screen savers.

Test Your Security Awareness IQ

- Is CSU more likely to have a security breach by internal staff or external activity?
- Is CSU more likely to have a security breach by malicious activity or negligence?

Your Role in Safeguarding CSU Data

Our actions can affect confidentiality, safety and availability of our data.

- We have access to paper files and documents with sensitive or confidential information.
- We have access to electronic files, documents and systems through the CSU network.
- Our computers could be vehicles for a cyber-crime.

Choose Passwords Carefully

A strong password should:

- Consist of at least 8 characters.
- Contain a combination of numbers and letters.
- Contain upper case AND lower case letters.
- Contain punctuation marks or symbols such as !, #, %, *, etc.
- Be easy to remember but difficult to guess.

Choose Passwords Carefully (Cont.)

Your password should NEVER be:

- A word found in the dictionary (any language).
- A combination of words, e.g. "deskdrawer."
- An alphabetical or keyboard sequences, e.g. asdfg or qwert.
- Personal information, e.g. names of spouse, child or pet, birthdays, or license plate.

Safeguard Your Passwords

- Sharing a password is the same as sharing your computer account.
- Don't give your passwords to anyone - even technical staff.
- Don't store passwords online, don't e-mail them, and don't write them down.
- Don't use the same password for multiple accounts.

Secure Your CSU PC or Laptop

- Lock your PC when you leave your desk unattended.
- Log out when you leave for the day.
- Be discreet when viewing confidential information on your screen.
- Log out of enterprise systems (e.g. Banner, CoreCT) when not in use.

Secure Your CSU PC or Laptop (Cont.)

- Be cautious when using floppies, zip disks and CD's. Viruses can hide inside programs, documents or other files.
- If assigned a CSU laptop, periodically check with authorized IT staff to determine virus software is current.
- Don't leave your laptop in your car or other open or public location where it can be stolen.

Safeguard your E-mail

- Don't open unexpected attachments even from people you know - check with the sender first.
- Be very wary of attachments with extensions such as .exe or scr or those with double extensions, e.g. gif.exe.
- Report suspicious e-mails
- Don't send or forward e-mail chain letters. They could contain malicious code.

Protect Confidential Information

- Label and secure paper files, CD's, disks that contain confidential/sensitive information.
- When printing confidential documents retrieve them immediately.
- Don't fax confidential information unless essential; if receiving such information retrieve immediately.
- Do not send personal financial information such as social security numbers by e-mail.

Protect Confidential Information (Cont.)

- Don't discuss confidential data, e.g. grades, etc.
- Refer requests for confidential information to your department manager or other designated party.
- Don't use discarded confidential data for scrap paper.
- Shred confidential documents before disposing.
- Lock file cabinets and rooms where confidential information is stored.

Surf Wisely

- Web sites can contain code that could launch virus-laden programs, documents or graphics.
- Be very careful about downloading files from the Internet.
- Never download freeware, shareware or screensavers to your CSU computer unless approved by authorized IT staff.

Questions/Closing Comments

