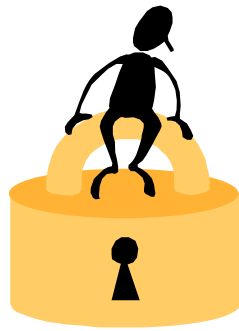


Information Security Annual Report



October 2006

Table of Contents

- I. Introduction..... 1
- II. Activities for the Fiscal Year 2005/06..... 1
 - A. Security Breach Notifications – FY 2005/06..... 1
 - B. Continue Migration of CMS PeopleSoft Student System 1
 - C. Engagement/Participation at System Level
in Ways that Benefit the Campus..... 2
 - D. Strengthen Awareness of Campus Constituencies..... 2
 - E. FERPA 3
 - F. Credit Card Regulations 3
 - G. Handling of Unsolicited Commercial E-mail (SPAM) 3
 - H. User Authentication..... 4
 - I. Data Center Firewall Implementation..... 4
 - J. Health Center Data Protection 5
 - K. CSU Network Security Design Standards 5
 - L. Server Patch Schedules..... 5
 - M. Secure Transmission to the Mainframe..... 6
 - N. Information Security Committee..... 6
- III. Goals for FY 2006/07 7
 - A. Increase Security of the Campus Wireless Network 7
 - B. Update Campus Password Standards and Processes 7
 - C. Develop Long Term Campus Plan for Comprehensive
Campus Security Services 7
 - D. Create Inventory and Document Existing "Shadow" Data Systems 7
 - E. Development of Standards for Technical Staff 7
 - F. Strengthen Awareness of Campus Constituencies..... 8
 - G. Record Retention 8
 - H. CSU Information Security Officers..... 8
 - I. CSU Policy Development..... 8
 - J. Complete Implementation of the CMS PeopleSoft
Student Administration System..... 9
 - K. Participate in the System-Wide Security Plan Project..... 9

I. Introduction

Cal Poly has information in many forms – electronic, paper, and verbal. The University takes the responsibility of information security seriously and continues to take steps to strengthen the security of information in all forms.

Section II summarizes activities during the past fiscal year (FY 2005/06) to improve the security of University information. Section III briefly describes projects that have been identified to be undertaken in FY 2006/07 that will support continuation of our efforts to secure and protect university data, including personal and confidential information.

II. Activities for the Fiscal Year 2005/06

A. Security Breach Notifications – FY 2005/06

For further information contact: Vicki Stover

Reference: http://security.calpoly.edu/what_employees/security_breach_notifications.html

During the FY 2005/06, there were two security breach notifications (California Civil Code 1798.29, commonly referred to as SB 1386). The University's practice is to disclose any breach of system security to all affected individuals (not only California residents as required by law) whose unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorized person.

Computer Science (December 8, 2005)

The campus was notified by e-mail that a file containing confidential information could be found if conducting a search of the campus website on Google. A professor had utilized student data from the year 2001 to populate a file for a class project. The file contained the names and social security numbers of 196 students who were on the Computer Science 101 class lists during Winter quarter 2001. It was the professor's intention to replace the real IDs with random numbers. Unfortunately, a mistake was made and the file was accidentally posted without the replacement. The file was removed immediately. Google and Microsoft (MSN) were also contacted to ensure that the data would be erased from their system.

Animal Science (February 10, 2006)

A professor's car had been broken into off campus. Grade books were missing which had names and social security numbers of nineteen students from the professor's Winter 2006 ASCI 406 class. This incident was reported to the city police department for investigation of the crime.

B. Continue Migration of CMS PeopleSoft Student System

For further information contact: Tim Kearns

The installation and initial use of the Student Administration (SA) system continued. Application processing for new Fall 2006 students began in October in the new SA system with admission decisions continuing to be made. Consultation about the SA system continued for faculty members during the winter quarter with a meeting for department chairs/heads and deans on February 3 with approximately 40 in attendance and an open forum on February 10 attended by approximately 70 people.

C. Engagement/Participation at System Level in Ways that Benefit the Campus

For further information contact: Tim Kearns or Vicki Stover

University staff have been involved at the system level in various ways that benefit the campus. These include the Record Retention Project, the Campus ID Project, and the Information Security Officers (ISO) group. Cal Poly also participates in the CSU projects for Identity Management and improved network security (see Item K)

The Record Retention Project has developed a template for records and records series have been identified (e.g., Financial, Human Resources, etc.). The Financial Standards Advisory Committee has been assigned the responsibility to develop the financial records retention schedule. The personnel/payroll records retention schedule is in final review with CSU Human Resources and CSU Long Beach is making good progress developing the student records retention schedule.

Cal Poly was instrumental in raising the issue and identifying the need for a Campus ID in the PeopleSoft system. A Modification Approval and Design Request to CMS Baseline has been submitted jointly by East Bay and San Luis Obispo. A Campus ID would allow everyone on campus (including those not currently in the PeopleSoft System such as auxiliary employees) to be assigned a unique ID that could be used for identification in any system on campus.

The CSU Information Security Officers is a relatively new group. Last year an organizational structure was developed whereby campus ISOs would act as officers of the group. Vicki Stover, Cal Poly's ISO, was elected chair of the ISO group for 2006. During this year the ISO group developed security awareness and training, data retention, and access control policies and drafted policies and standards for data classification, roles and responsibilities, and patch management. The group continues to mature and is a valuable source for sharing information security practices as well as receiving important updates and training on information security.

Item K (page 6) provides additional information regarding technical benefits from participation at the system level.

D. Strengthen Awareness of Campus Constituencies

For further information contact: Vicki Stover

Reference: http://security.calpoly.edu/what_everyone/security_training.html

Information Security Forums were presented in the Fall and Winter Quarters last year. The first forum was on October 25 during National Cyber Security Awareness Month. This forum presented information on the following: Information Security Program, Responsible Use, FERPA, Human Resources Data, and discussion of key issues, including password requirements, records retention, the use of electronic recording devices, violation reporting, and security breaches. Prior to the forum, Ryan Matteson, Mary Shaffer, and Vicki Stover met with the dean and department heads/chairs of each of the academic colleges to introduce themselves, discuss their roles, review these topics, and to encourage faculty, staff and student attendance at the forum. Attendance was also encouraged through the computing advisory committees.

The second forum was on March 3, 2006. The focus of this forum was on passwords and changes that will impact all faculty, staff and students in the future. Approximately 75 – 80 people attended each forum.

In addition, an Information Security High Level Assessment was developed and endorsed by the Information Security Committee. The questions in the guide provide a reminder of the types and variety of practices which are necessary to protect information. Answers given provide a broad measure of the security awareness and preparedness in each area. This assessment is posted on the Campus Information Security website and will be presented at the Information Security Forum on October 27, 2006.

E. FERPA

For further information contact: Vicki Stover

Reference: http://www.ess.calpoly.edu/records/stu_info/ferpa.htm

The Family Educational Rights and Privacy Act of 1974 (FERPA) as amended is a federal law which is designed to protect the privacy of and limit access to the educational records of students. This means that institutions generally may not provide such information to others unless the student gives permission, or if the information constitutes “directory information” and the student has not placed a privacy restriction on disclosing this information. To assist students and campus departments, a release form was developed and approved which provides a student the ability to give written consent for a department to release specific information to others. Each Cal Poly department has the option of using the form to allow students to have FERPA information available in their department released to designated individuals. Some departments may not provide this service because of legal requirements (e.g., law enforcement or medical records) or department preference. This document will be presented at the Information Security Forum on October 27, 2006.

F. Credit Card Regulations

For further information contact: Vicki Stover

A meeting was held with entities on campus that utilize credit cards. The purpose of this meeting was to discuss current regulations regarding credit card security and to determine next steps. Each entity reported on their current actions and, what, if any, appropriate steps they would be taking to ensure compliance with credit card security requirements when necessary.

G. Handling of Unsolicited Commercial E-mail (SPAM)

For further information contact: David Ross

Reference: <http://email.calpoly.edu/spam/index.html>

Each year, the campus has seen a steady increase in SPAM e-mail being sent to Cal Poly e-mail addresses. This represents both a productivity drain and a security risk. Users who receive unwanted e-mail must spend time managing the continuous flow of these messages. Additionally, a growing number of these messages are "phishing" (i.e., scam) e-mails which attempt to mislead recipients into providing sensitive information.

Many steps have been taken during the past year to minimize the number of SPAM messages coming onto campus and the associated threats. In summer 2005, Information Technology Services (ITS) upgraded the campus e-mail gateway used to scan all

incoming messages. This upgrade improved the process used to identify SPAM, increased the percentage of SPAM messages identified, and has reduced the number of legitimate messages incorrectly identified as SPAM.

Additionally, a number of specific rules have been implemented to stop obvious SPAM messages, such as messages sent to Cal Poly e-mail lists from non-Cal Poly addresses. This has prevented thousands of unwanted messages per day from reaching Cal Poly e-mail users.

ITS continues to investigate improvements in SPAM monitoring technologies as well as upgrades to allow users to individually set SPAM filtering options.

H. User Authentication

For further information contact: Ryan Matteson or David Ross

Reference: <http://my.calpoly.edu/>

Strong authentication of users is a critical element in protecting information and resources from unauthorized access. With the increase in campus services provided via web-based technologies, ITS considers authentication for campus web resources as part of an overall authentication strategy. This strategy has been implemented through centralized usernames and passwords and deployment of a web-based central authentication service in 2003 as part of the campus portal, my.calpoly.edu.

Since deployment of this service, ITS has assisted numerous campus organizations in integrating their web sites with the service. In the past year, Housing and Residential Life, College of Architecture, Orfalea College of Business, Cal Poly Corporation, Career Services, and Robert E. Kennedy Library have integrated additional service offerings with the central authentication environment. ITS also advised other CSU campuses in the design and implementation of this technology.

Use of the authentication service has doubled since the previous year with more than eight million authentication transactions occurring from July 1, 2005 to June 31, 2006. Growth is also reflected in a 40% increase in the number of users; a large majority of campus students, faculty and staff used the service this year. The efforts in this area reduce the likelihood of compromised passwords and unauthorized access to data by implementing a single set of authentication technologies and practices. Additionally, users benefit from simplified interaction in which they provide a password only once in order to access a variety of campus web-based applications.

ITS will continue to assist campus offices in efforts to integrate new applications and services to increase manageability and reduce risk.

I. Data Center Firewall Implementation

For further information contact: Johanna Madjedi

Firewall technologies provide a mechanism to control the flow of information within a network. ITS has implemented a set of redundant firewall appliances to further protect IT services central to Cal Poly such as e-mail, Blackboard, the data warehouse, the campus identity management and directory services, and the student ID card system. While a campus perimeter firewall has been in place for some time, this new layer of

firewall technology provides an additional layer of protection against attacks originating from on campus.

Prior to this implementation, firewall functionality was implemented on a per-server basis, adding complexity to configuration and security maintenance on each server. Moving this protection mechanism to a firewall appliance designed specifically for this purpose reduced the risk of misconfiguration which might lead to vulnerabilities. Additionally, a firewall can implement the protection rules with more sophistication and better performance, reducing the burden on the servers themselves.

Placement of data center servers behind this new firewall environment is in progress and expected to be completed by mid-fall 2006. This model is in alignment with the CSU Standard Network Architecture (<http://tis.calstate.edu/Standards/Standards.shtml>).

J. Health Center Data Protection

For further information contact: Johanna Madjedi (network) or David Ross (database)

The Health Center data network was upgraded to meet CSU standards and also configured to implement a departmental firewall. This aids in protection against unauthorized access by campus and external hosts. Additionally, database instances used by the Health Center containing confidential patient information have been incorporated into the ITS environment. This ensures that database maintenance and access security are implemented in a manner consistent with other sensitive campus databases, and provides an example for how central IT security technologies may be leveraged to improve security throughout the campus.

K. CSU Network Security Design Standards

For further information contact: Johanna Madjedi

Reference: <http://nta.calstate.edu/ITRP2.shtml>

Cal Poly has been a participant in the review of the CSU's Network Security Design Standards as well as the evaluation of a number of security-related technology products (e.g., firewalls, virtual private network solutions, and intrusion detection services) to be implemented at all CSU campuses in the future. Once deployed, Cal Poly will be able to augment its firewall services with virtual private network (VPN) and intrusion detection system (IDS) services in the next fiscal year. Virtual private network functionality will enable authenticated and encrypted access from off-campus locations to applications on campus, reducing the risk of confidential data being compromised on the public network. Intrusion detection system functionality will provide information regarding suspect traffic patterns that may indicate a network incident in progress such as a virus attack or denial of service attack. This will reduce the likelihood of a service impact as many attacks will be detected and responded to before serious service degradation occurs.

L. Server Patch Schedules

For further information contact: Johanna Madjedi

Unauthorized access to computer systems is most often achieved through known vulnerabilities in operating systems, application code or easily guessed passwords. Operating system patches to correct service issues or remove these vulnerabilities are released on a periodic basis by the vendor. Operational practices have been implemented within ITS to ensure that operating system patches are installed on a regular basis on

centrally managed servers supporting critical university applications and services. This greatly reduces the risk of unauthorized access via vulnerabilities in the operating system.

Servers from Sun Microsystems (approximately 50 machines) are scheduled for patch installations every six months, Linux based hosts (approximately 40 machines) are scheduled for patches every quarter and automated patching tools are used for Windows servers (approximately 50). Notifications from operating system vendors regarding any patches to address critical security vulnerabilities are evaluated at the time of notification. Based on the risk assessment and timing of the notification, these patches are scheduled on an ad hoc basis or rolled into the normal patch maintenance cycle.

M. Secure Transmission to the Mainframe

For further information contact: Johanna Madjedi

The campus mainframe system is used to support the legacy student information system. This environment is being replaced by the CSU CMS PeopleSoft Student Administration implementation. Decommission of the legacy system for Cal Poly is scheduled for early 2007. ITS has implemented an encrypted access method for user access to the mainframe. This reduces the risk of confidential student data being compromised during transmission over the network prior to decommissioning of the legacy system.

N. Information Security Committee

For further information contact: Vicki Stover

Reference: http://www.security.calpoly.edu/contacts/info_secure_comm.html

The Information Security Committee met monthly during FY 2005/06. The mission of this committee is to ensure the security (confidentiality, integrity, and availability) of information in the University's custody, regardless of format, by preventing unauthorized access to and use of all information and protecting confidential and sensitive information; requiring university-wide compliance to applicable laws, regulations, policies and practices; reviewing and recommending security policies and procedures; and promoting sound information security practices.

The Information Security Committee provides a forum for discussion and resolution of campus information security issues. During the fiscal year the following issues, among others, were discussed: student data integration, campus ID, student assistant security, release of FERPA data, risk assessment, passwords, record retention, use of social security numbers, CMS Security, CALEA, and Information Security Program review,

The committee is an ad hoc committee and has no formal campus recognition. Formal recognition has been requested.

III. Goals for FY 2006/07

Following are brief descriptions of projects that have been identified to be undertaken in FY 2006/07 that will support continuation of our efforts in the area of security.

A. Increase Security of the Campus Wireless Network

For further information contact: Johanna Madjedi or Ryan Matteson

Reference: <http://wireless.calpoly.edu/cca.html>

Planned changes to the campus wireless network will be rolled out in phases, with each phase implementing additional verification steps for a device to be allowed onto the network. Password-based authentication will be deployed first, allowing new campus users to gain access to the network more easily than is possible with the current manual registration process. This will be followed by phases which will provide verification that current anti-virus, anti-spyware, and operating system security patches are in place. Insecure machines will be automatically quarantined and users will be provided with instructions on how to bring their computers into compliance. Together these changes will improve the reliability of the network, reduce the potential for security incidents, and allow for growth of the campus wireless network.

B. Update Campus Password Standards and Processes

For further information contact: Tim Kearns or Ryan Matteson

Reference: http://servicedesk.calpoly.edu/accounts_passwords/passwordexpiration.html

Campus password standards and processes are developed based on the requirement to provide both appropriate protection for resources and usability for campus constituents. Changes this year will improve password effectiveness by ensuring each password is periodically reset, while also providing users and support staff with additional functionality to ease the management of passwords.

C. Develop Long Term Campus Plan for Comprehensive Campus Security Services

For further information contact: Tim Kearns or Ryan Matteson

A long term campus technical plan is to be developed which will include VPN, firewall, intrusion detection and response, and vulnerability assessment monitoring.

D. Create Inventory and Document Existing "Shadow" Data Systems

For further information contact: Tim Kearns or Ryan Matteson

“Shadow” data systems will be documented utilizing the existing data access request process. Additional standards and guidance will be developed to minimize the potential for compromise. Specific focus will be on all campus systems that store social security numbers. Where appropriate, plans will be developed to move to alternate identifiers.

E. Development of Standards for Technical Staff

For further information contact: Tim Kearns or Ryan Matteson

The development of standards for technical staff will focus on ensuring that security requirements are documented and that implemented systems meet these requirements. This will include clarification of the roles of technical staff.

F. Strengthen Awareness of Campus Constituencies

For further information contact: Vicki Stover

Information security awareness will continue to be a high priority for the campus. The first Information Security Forum is scheduled for October 27, 2006. The forum will focus on the security of student data, but will also include a short “What’s New” briefing which will include an introduction to the Security High Level Risk Assessment document. The FERPA Release form will also be highlighted during the forum. Both documents are posted online at:
http://www.security.calpoly.edu/what_employees/index.html.

The retention of class lists by faculty that contain social security numbers has been identified as a high-risk issue. Faculty, deans, and department heads will be made aware of actions they need to take to eliminate this risk.

Additional security awareness training will be pursued based on the security awareness training policy documents and potential training programs developed and identified by the CSU Information Security Officer group.

G. Record Retention

For further information contact: Vicki Stover

The campus has volunteered to be a pilot campus for implementing the proposed retention schedules. A list of steps to be used during the pilot implementation has been drafted and is being reviewed by the CSU working group which includes representatives from Cal Poly. It is anticipated that the first series of retention schedules will be received by the campus this fall. In addition, best practice guidelines for campus disposition procedures and an official policy for retention of electronic media are to be developed.

H. CSU Information Security Officers

For further information contact: Vicki Stover

Active participation in the ISO group will continue. It is anticipated that policy development will be a major focus for this group this year and campus input will be valuable in shaping the policy development framework, principles, governance model as well as policies and related standards (see Item I below). The CSU ISO group is also actively pursuing educational awareness programs that could benefit the campus (see Item F above). The ISO group is also implementing training sessions at the quarterly meetings which are intended to assist the ISOs in fulfilling the requirements of their position.

I. CSU Policy Development

For further information contact: Vicki Stover

The campus is one of nine campuses participating in a campus security survey. The survey is being conducted by the Unisys Corporation who will provide assistance in developing a CSU security framework and plan based on an internationally recognized security standard, ISO 17799-2005, Code of Practice for Information Security Management. The consultants will be on campus the week of October 9, 2006. In addition, Cal Poly is participating in developing and evaluating a Request for Proposal

intended to secure consultants to help the CSU define, develop and implement CSU-wide security policies and related standards.

J. Complete Implementation of the CMS PeopleSoft Student Administration System

For further information contact: Tim Kearns

Remaining processes such as registration will be transferred to the new system. All student data will be transferred to PeopleSoft. Instructors will be trained on the new system. It is anticipated that the CMS PeopleSoft Student Administration System will be completely implemented by the end of Fall Quarter 2006. The use of an “emplid” -- instead of a student’s social security number -- as their primary identifier will be a significant step in eliminating potential security breaches of confidential information. Cal Poly will continue to develop a campus-wide security model, e.g., roles and responsibilities for appropriate access to data in campus systems, including PeopleSoft, the data warehouse, etc.

K. Participate in the System-Wide Security Plan Project

For further information contact: Vicki Stover

The CSU has awarded a contract to the Unisys Corporation to provide assistance with developing an enterprise-wide security framework based on internationally recognized security standard, ISO 17799:2005, Code of Practice for Information Security Management. The framework will be used as a foundation for a CSU-wide information security program that improves the University’s security posture and addresses the security challenges of the future. Nine campuses, including Cal Poly, have been pre-selected to participate in a survey to collect information about current security controls.