

Appendix B



California State University, Chico
Office of the Vice Provost for Information Resources

Information Security Office 2008/2009 Annual Report

August 2009

Introduction

Information security is a campus wide responsibility. To that end the Information Security Office continues to work with the campus community to secure system and network resources, and protect the confidentiality of student, faculty, and staff information. In 2008/2009 we participated in and responded to an information security audit. Our responses included the publication of a number of new standards and procedures, new compliance reports and the initiation of a number of new projects. We also continued to offer awareness and training programs. Finally, implementation of appropriate tools and technologies continue to better secure campus desktops, servers, our network and confidential data.

This annual report highlights some of the key activities related to information security in the 2008/2009 academic year. The report also briefly describes projects to be pursued in the 2009/2010 academic year.

2008-2009 Information Security Activities

Information Security Audit

In 2008, the California State University (CSU) Board of Trustees initiated audits of the information security capabilities at all CSU campuses and the Chancellor's Office. Over an eight week period between May and July the Office of University Auditor (OUA) and KPMG audited the CSU, Chico campus against the ISO 17799 standard. At the informal exit conference we were presented with 28 preliminary findings which in general indicated a need for consistent implementation of security best practices and controls across the campus. These findings are summarized by five key observations:

1. *Information Security Policy* - The campus should implement an information security policy which explains principals, standards and compliance requirements.
2. *Governance Structure* - The existing campus governance structure to approve and communicate information security policy and standards and assess our compliance with laws, policies and regulations does not appear to be working effectively.
3. *Decentralized Servers and Applications* - Campus decentralized servers and applications (critical and non-critical) are not secured appropriately.
4. *Web Application Security* - Change management procedures for web application development require improvement.
5. *Technical Controls* - The campus lacks some technical controls.

Addressing findings related to the information security audit resulted in changes to standards, processes and procedures, some technical changes and ultimately a more secure computing infrastructure and more secure campus information. All audit findings were closed before our six month deadline of May 7, 2009.

Awareness and Training

Raising awareness regarding information security and ultimately changing employee behavior is the single most important thing we can do to better secure our environment. The following activities were coordinated by the Information Security Office in support of security awareness and training:

- Updated the Information Security Plan to take into account the current environment and increase the maturity level of the campus related to security.
- Continued to offer awareness programs and training courses for new and current employees, see **Table 1** below.

- Rolled-out the CSU information security awareness training program to the campus in April 2009. As of June 30th, 40% of faculty, 74% of staff and 24% of student employees have completed the training.
- Revised the information security website and Confluence wiki to make resources easier to find.
- Facilitated eight System Security meetings to discuss audit findings/remediation plans, our risk management and security strategy and best practice resources available to campus.

2008/2009 Information Security Internal Training Metrics			
# Events	Event Type	Attendance	Total Hours
2	Protect Yourself/Campus from Cyber Threats Training	43	4
11	New Hire Orientation	82	3
8	System Security Meetings	297	8
4	Foundstone Vulnerability Management Training	30	5
		<u>452</u>	<u>20</u>

Table 1

Both the 2007 and 2009 Faculty and Staff Information Technology Surveys included questions regarding information security. As a result of the efforts spent on communications regarding confidential data and security awareness, both faculty and staff indicated a high level of awareness about protection of confidential data and information security. The survey showed that 72% of the faculty and 87% of the staff surveyed agree that they know how to protect confidential information and 86% of the faculty and 90% of the staff surveyed indicated they knew who to contact for information security questions. These results are up slightly from the 2007 survey. See **Figure 1** below.

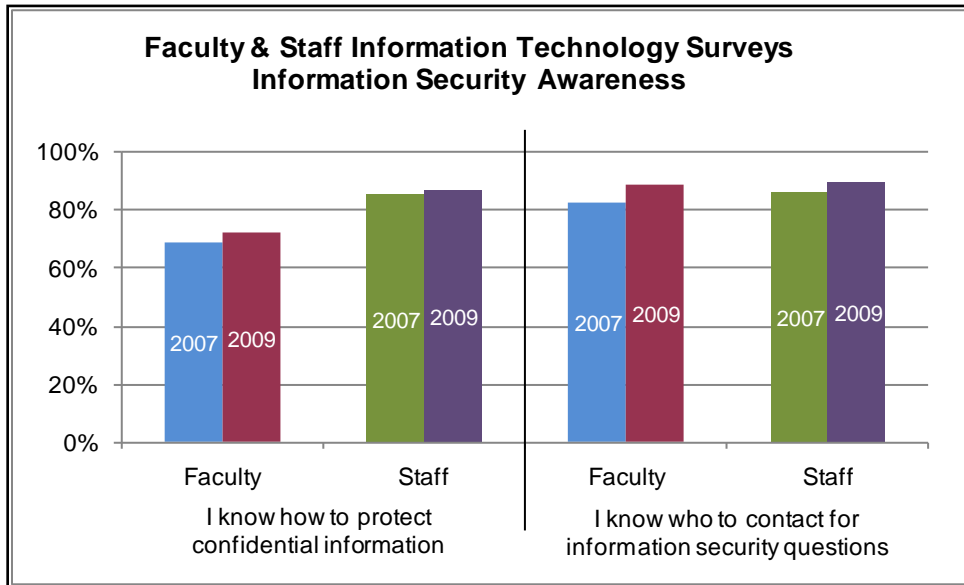


Figure 1

In order to stay current on trends in information security, investments in technical training are a necessity. In 2008/2009 our Information Security Analyst attended two week long external/3rd party technical training courses, SANS Hacker Techniques, Exploits & Incident Handling and Encase Computer forensics.

Policies, Standards, Guidelines, and Best Practices

A number of new standards were implemented this year to tighten campus security and respond to the information security audit. Our efforts to improve campus information security are supported by the Revised Policy on Use of Computing and Communication Technology for Faculty, EM 07-01 and the Policy on Use of Computing and Communication Technology, EM 97-18.

- *Server Security Baseline Standards* improve security of centralized and decentralized systems. Servers are classified into one of three risk categories, and the application of security controls is proportional to the risk category identified.
- *Vulnerability Management Baseline* standards set a timeframe for technical staff to identify and remediate vulnerabilities on campus servers. Timeframes are based on data from three separate sources, including the server risk category, with the idea that servers which present the most risk to campus should be addressed first. These standards are created to work in tandem with the Server Security Baseline Standards.
- *Application Code Development Standards* require documented testing procedures, procedures for user acceptance and deployment, procedures to ensure web application source code is protected, controls for migration of systems between development and production environments, and a requirement to review applications for security vulnerabilities prior to deployment.
- *Account Management Standards* ensure that access to campus information systems and protected information is only provided to those having a specific need for access in order to accomplish an authorized task and is based on the principles of need-to-know and least privilege.
- *Password Management Standards* clearly communicate required password construction criteria and password change schedules.
- *Data Classification and Protection Standards* provide guidance on the storage and transmission of protected information.
- *Remote Access Standards* include requirements for devices remotely connecting to the CSU, Chico internal network via a virtual private network.
- *Credit Card Security Standards* require campus departments (both state and auxiliaries organizations) taking credit or debit cards for payment to notify the Information Security Office and conduct a yearly self assessment. This standard is intended to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).

Security Infrastructure

The Information Security Office works in conjunction with campus technical departments to insure the security of campus systems and confidential data. The Security Infrastructure section of this report is logically separated into Application, Desktop, Network and Server areas. Currently there are over 450 servers, 3000 desktops and 500 lab machines on the campus network. The responsibility for securing this infrastructure is shared by a number of departments, both within and external to Information Resources. Key initiatives were accomplished across all areas that contributed to increasing the overall security posture of the campus:

Application

- Analyzed multiple vendor applications prior to implementation to identify possible information security risks (e.g., Now Print, Numara Footprints, etc.).
- Reissued more than 60 wildcard Secure Socket Layer (SSL) certificates prior to their certificate expiration date.

Desktops

- Implemented Microsoft SMS to replace LANDesk for remote management and patching of machines.
- Implemented an automatic screen saver lock on Windows machines to ensure computers are not available when users leave their desk.
- Implemented Microsoft System Center to ensure a better understanding of the current desktop environment and for secure remote software distribution.
- Documented a standard for remote access to the internal campus network via the Virtual Private Network (VPN) to ensure remote devices meet minimum security requirements.
- Documented guidelines for desktop computer software installation to clarify requirements when installing unsupported software.

Network

- Implemented additional VPN groups with our existing Cisco VPN to limit access to critical systems in preparation for implementation of the Intrusion Detection/Prevention System.
- Implemented additional security features as part of the ITRP 1 project.
- Documented a number of new procedures, including procedures for network device configuration audits, implementation of new network devices, rogue wireless access points audits and network log review.
- Assessed the security posture of 34 campus modems, resulting in the disconnection of 12 modem lines and the reclassification of 11. The security posture of the remaining 11 campus modem lines is appropriate given the risk level of the systems to which the lines are connected.
- Tested the use of Cisco Clean Access (CCA) to assure the security of remote machines connected to the internal campus network via the Virtual Private Network (VPN).
- Analyzed border firewall exceptions and made significant progress to either eliminate exceptions or build rules which open only pinholes in the firewall. Approximately 80 open firewall exceptions have either been closed or well-defined rules have been implemented. See **Figure 2** below.

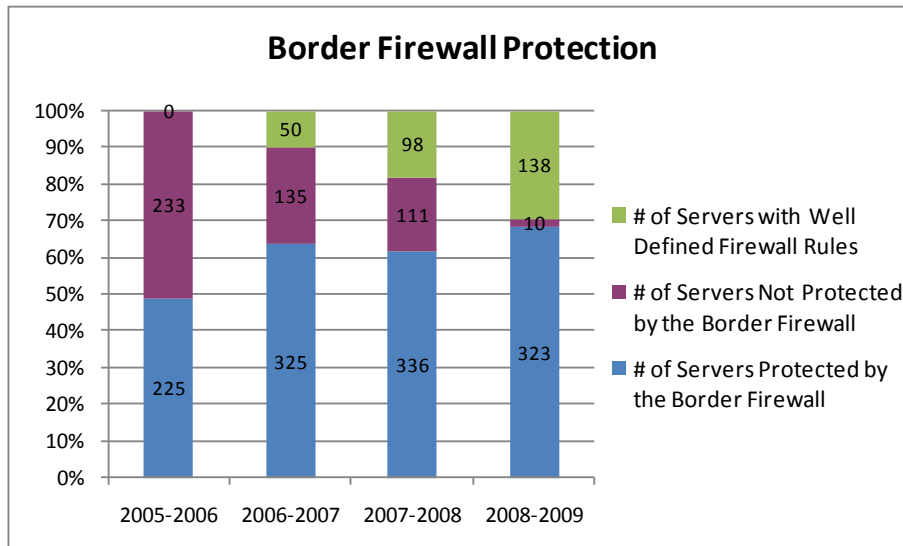


Figure 2

Servers

- Began a regular schedule of auditing and vulnerability scanning campus servers utilizing McAfee Foundstone.
- Developed a Server Risk Report in INSIGHT to provide information for technical staff and server owners about the security posture of campus servers for which they are responsible. The report utilizes data from both OMNI (server inventory) and the McAfee Foundstone Vulnerability Management System, and uses an algorithm to calculate weighted risk scores for campus servers. Servers are assigned a risk score and risk category (high, medium and low), see **Figure 3** below for totals in each category over the first six months of 2009.

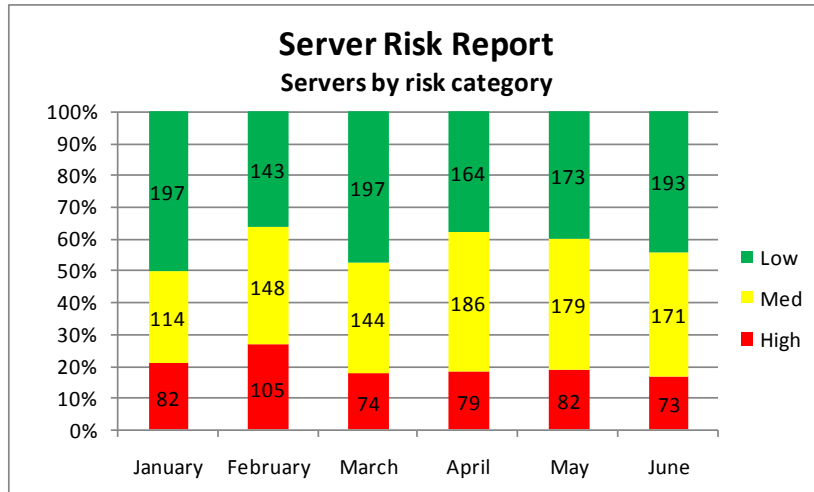


Figure 3

- Developed an initial Server Risk Dashboard to provide an overview of the security posture of campus servers by division and department.
- Continued to move department servers to Enterprise Systems (ESYS) to take advantage of co-hosting servers and co-location of servers in the data center. This effort is meant to leverage existing skills and infrastructure in ESYS to benefit the campus community and secure campus systems and data. See **Figure 4** below regarding the growth of co-host and co-managed services.

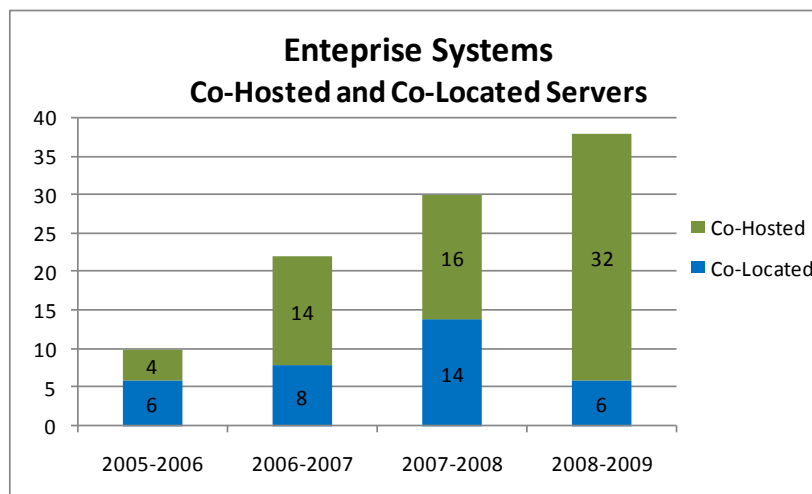


Figure 4

- Documented a procedure for enterprise systems log review to assist in identifying potential network vulnerabilities and breaches on campus systems.
- Implemented host intrusion detection (HIDs) agents on data center servers to assist in monitoring and responding to potential threats on campus systems, McAfee HIPs on Windows servers and OSSEC on RedHat LINUX servers.

Incident Management

Improvements in security infrastructure, procedures, awareness and training all contribute to a solid information security program, however as new threats emerge there will continue to be incidents which require response. Our goal is to limit the severity of these incidents and to manage them consistently according to industry best practice. In 2008/2009 we continued to see a decrease in the number of desktop and server incidents. The Information Security Office is handling an increasing number of account compromises and continues to investigate ways to better secure accounts.

Our current ability to report on the number of possible events and actual security incidents managed is limited. This will be a focus of 2009/2010, with Footprints used for incident management and tracking.

Confidential

Protection of confidential information is a primary goal of the Information Security organization. Several key tasks were accomplished in 2008/2009 to protect confidential information:

- Continued to ensure that information in our server registry database, OMNI, is accurate and up-to-date. **Figure 5** below illustrates the percentage and number of campus servers containing confidential data as self-reported in OMNI. In the 2005/2006 and 2006/2007 reporting periods OMNI only captured confidential versus non-confidential information. Since then, we began to capture the actual ‘level’ of protected information contained on these servers. The data below for 2008/2009 labeled as ‘confidential information’ is actually protected level 1 (personally identifiable) information such as Social Security Numbers and Credit Card Numbers.

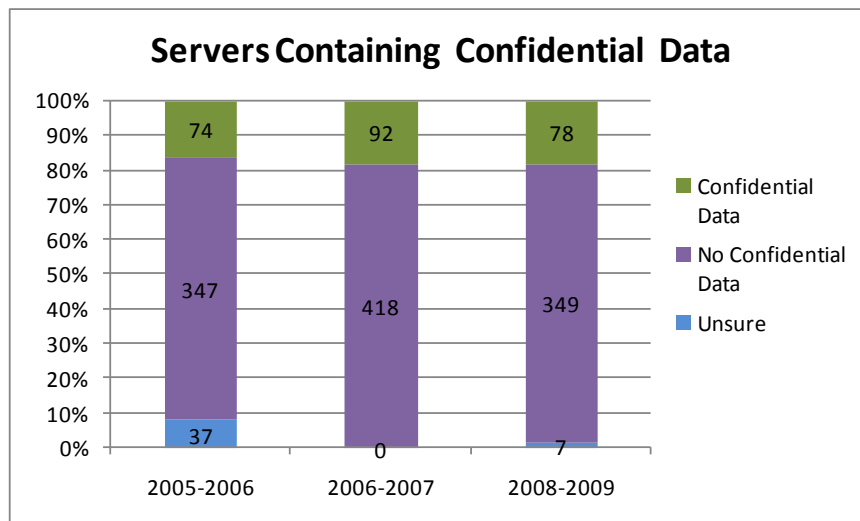


Figure 5

- Continued to move campus decentralized databases and servers containing confidential data to the data center so they can take advantage of the physical security of the data center, the full suite of enterprise server management tools (back-up, monitoring, scanning) and operation by Enterprise Systems trained system administrators.
- Conducted a survey to identify the presence of protected level 1 data on desktops. **Figure 6** includes results from the 1342 campus responses.

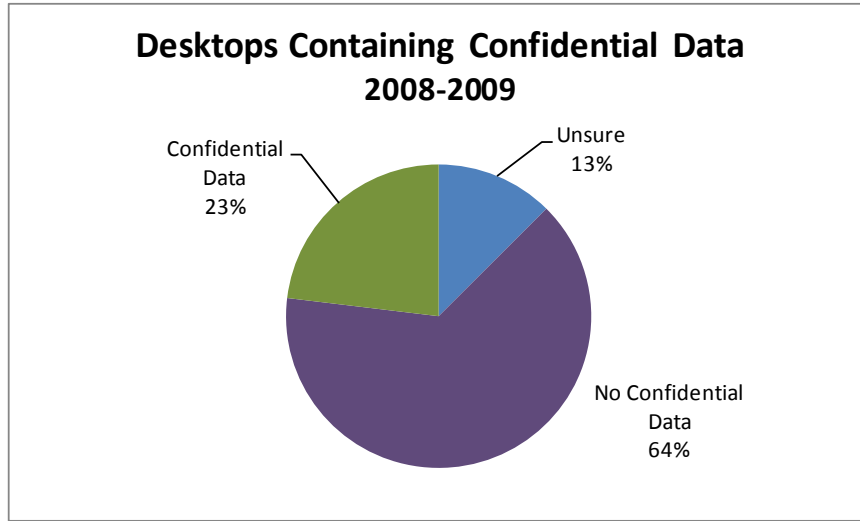


Figure 6

CSU Activities

The CSU is in the final review stage of proposed system-wide policies on Responsible Use and Information Security. As a complement to the Information Security policy, system-wide Information Security Standards have been drafted. It is expected that the policies and some of the standards will be issued by the Chancellor in 2009/2010.

2009-2010 Information Security Goals

The Information Security Office plans to continue taking a multi-faceted approach addressing training, governance, compliance, and technical measures across the campus community. This has proved successful in enhancing the security, confidentiality and integrity of campus data and these efforts will continue and grow in 2009/2010

Awareness and Training

- Continue to facilitate monthly System Security Meetings and attend all new hire orientation sessions.
- Offer quarterly McAfee Foundstone Vulnerability Management System training.
- Encourage additional faculty, staff and student employees to complete the CSU system-wide information security awareness training program. Increase the completion rate for student employees from 24% to over 75%.

Policies, Standards, Guidelines, and Best Practices

- Collaborate with campus application developers to develop strategies for implementation of the application development security standards.
- Implement system-wide policies on Responsible Use and Information Security, and Information Security Standards, when they are issued.

Security Infrastructure

Application

- Participate in the Remedy replacement project to ensure that security requirements are addressed and that the new service management system supports new security procedures.
- Implement Oracle's Enterprise User Security (EUS) to convert individual database logins to centralized authentication via a campus directory server (either Active Directory or OpenLDAP). EUS will centralize our Oracle database authorization structure and reduce DBA administration time required for overall user security of the database environment.

Network

- Implement a DMZ or multiple DMZs in our network for specific campus systems.
- Continue to analyze border firewall exceptions and reduce the number and scope wherever possible.

Servers

- Implement a Server Risk Dashboard in INSIGHT to provide an overview of the security posture of campus servers by division and department.
- Continue to analyze campus systems, in partnership with department technical staff and management, to determine risk of data compromise by evaluating the operating system, application, databases and network infrastructure.
- Continue current migration efforts to move campus services and systems to the Common Management environment offered by Enterprise Systems.
- Implement Microsoft System Center Operations Manager to provide automated maintenance and

vulnerability patching to Windows servers. Patches will be scheduled and pushed out to servers minimizing system administrator time and allowing each administrator to manage more servers.

- Evaluate the effectiveness of multi-factor authentication and consider a rollout to a larger group of technical staff.

Desktops

- Implement a solution for encryption of level 1 protected data stored on laptops.

Incident Management

- Refine existing procedures for e-Discovery, litigation holds and incident response.

Confidential Data

- Audit and ensure campus compliance with Payment Card Industry Data Security Standards (PCI DSS).
- Pilot an encryption/access solution for level 1 protected information stored on the campus file server Bay.
- Continue to move campus decentralized databases and servers containing confidential data to the data center.
- Develop a standardized procedure to ensure that access to confidential data is approved, tracked and audited in a consistent manner across campus.

CSU Activities

- Attend a teleconference of the Information Security Advisory Committee every other month.
- Continue participation in working groups to develop system-wide information security solutions.