

Appendix C



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

Information Security Office 2006/2007 Annual Report

Version 0.3
August 14, 2007

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 2006/2007 we hired an Information Security Analyst to help identify risks in our environment. We also worked with many departments to assist them in better securing their servers and confidential data. New procedures have been implemented so that security is considered prior to system implementation. Further, these new procedures have helped enable a number of new technologies which would have otherwise been too difficult or insecure to implement.

This annual report highlights some of the key activities related to information security in the 2006/2007 academic year. The report also briefly describes projects to be pursued in the 2007/2008 academic year.

2006/2007 Academic Year Activities

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:

- Facilitated a communication program in conjunction with National Cyber Security Awareness month in October to include posters, bookmarks, Orion ads, BMU message board ads and a website.
- Developed and delivered a New Hire Orientation security message/presentation and an information security course as a part of the Supervisory Certificate program.
- Facilitated two System Security/System Administrator meetings to discuss our risk management and security strategy and best practice resources available to campus. See **Table 1** below.
- Published Key Information Security Practices to help faculty and staff identify steps they can take to better protect campus information.

2006/2007 Information Security Internal Training Metrics			
# Events	Event Type	Attendance	Total Time (mins)
2	Protect Yourself/Campus from Cyber Threats Course	39	240
8	New Hire Orientation	85	120
2	System Security Meetings	43	90
4	Vulnerability Management Training	23	240
		124	690

Table 1

For the first time, the 2007 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 69% of faculty and 85% of the staff surveyed agree that they know how to protect confidential information. Additionally, 83% of the faculty and 89% of the staff indicated they knew who to contact for information security questions. See **Figure 1** below.

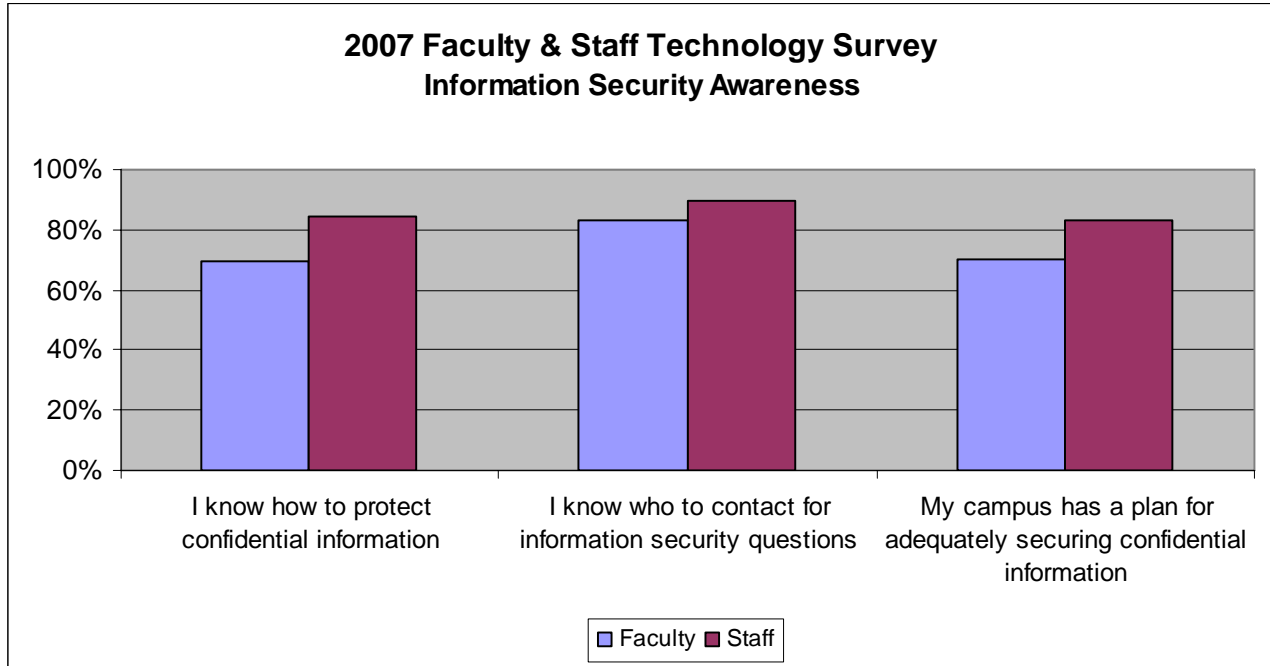


Figure 1

In order to stay current on trends in information security, investments in technical training are a necessity. **Table 2** below presents summary training metrics for some of the external/3rd party training attended by our technical staff.

2006/2007 Information Security External/3rd Party Training Metrics			
# Events	Event Type	Attendance	Total CPE Credits
2	CISSP Training & Certification	2	88
5	SANS Training	11	384
1	McAfee Foundstone Training	2	32
		<u>13</u>	<u>504</u>

Table 2

Policies, Standards, Guidelines, and Best Practices

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. A number of new procedures and best practices were implemented this year to tighten campus security:

- Published a Data Classification and Protection Standard to classify data according to its sensitivity to loss or harm from disclosure.
- Updated the Server Security Procedures and Guidelines to provide system administrators with best practices for securing servers.
- Implemented Vulnerability Scanning Procedures and Guidelines to provide a common set of requirements for vulnerability scans of campus servers.
- Implemented a procedure which requires all new systems to be analyzed using the new streamlined System/Security Worksheet to identify possible risks with the system.

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 is logically separated into Network, Server, Desktop and Application areas. Currently there are over 500 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.

Application

- Completed Phase 2 Implementation of Chico Password Station to integrate Generic Accounts, provide streamlined notifications, and more secure methods for faculty and staff password resets.
- Developed and implemented a “Password Station” like application for student password self service.
- Analyzed six vendor applications prior to implementation to identify possible information security risks (e.g., EMT Connect, SmartPublisher, etc.).
- Implemented a system to issue wildcard Secure Socket Layer (SSL) certificates to support secure communications between workstations and servers. Use of this wildcard certificate eliminates the need to purchase individual certificates for every server/application that requires secure server communication channels saving over \$10,000 in 2006/2007.
- Consolidated the purchase of non-wildcard SSL certificates for Information Resources.

Desktops

- Extended the use of the McAfee ePolicy Orchestrator (ePO) to the LABS domain for virus management of PC labs.
- Implemented McAfee Host Intrusion Protection (HIPs) within the ePO to protect faculty and staff PC desktops against zero-day and non-“viral” threats.
- Reduced the non-Windows XP SP2 population down to less than 5% of domain level machines.
- Achieved 99.2% SP2 coverage for User Services-managed Windows XP desktops by the end of Fall 2006.

Network intrusion attempts blocked (Feb '07 thru June '07)	2,124
IPS distinct signatures detected (Feb '07 thru June '07)	47
IPS events blocked (Feb '07 thru June '07)	9,948
Viruses blocked/remediated (all of 2006/2007)	202,617

Network

- Began planning and attended training on the new network security tools to be implemented in 2007/2008 as a part of the ITRP2 project. These tools include a new Juniper firewall, VPN, and an Intrusion Detection/Prevention System.
- Implemented 21 VPN groups which limit off campus access to critical campus systems to authorized personnel (e.g. Student Health, Enrollment Management, Associated Students, and Enterprise Systems, etc.).
- Analyzed border firewall exceptions and made significant progress to either eliminate exceptions or build rules which open only pinholes in the firewall. Approximately 100 open firewall exceptions have either been closed or well-defined rules have been implemented. See **Figure 2** below.

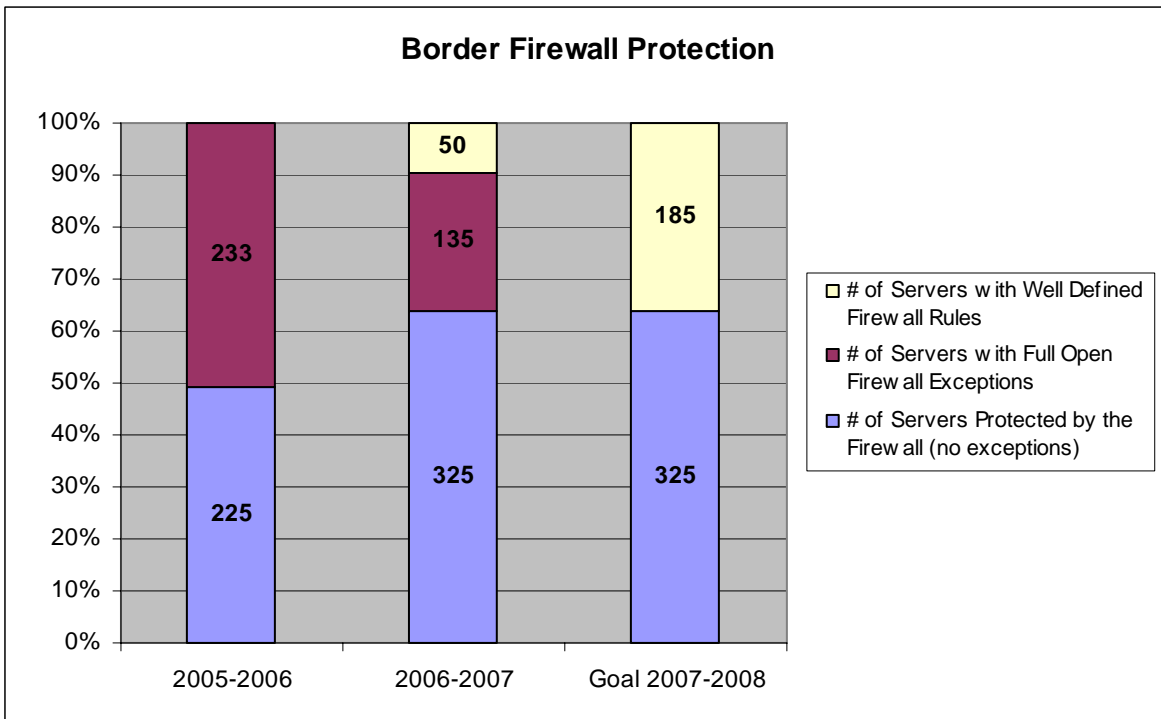


Figure 2

- Implemented Cisco Clean Access (CCA) for RESNET and University Village and to verify the security of machines before they can connect to the network. Over 1800 student machines are protected by CCA greatly reducing trouble tickets and calls related to viruses/works/malware. CCA is also used for wireless access, improving ease of user authentication and eliminating requirement for VPN-based access.
- Implemented the framework to facilitate IPSec to encrypt network communication between enterprise servers and campus desktops. Enabled IPSec/Encryption for desktops connecting to the Bay file share and the Oak print servers.

Servers

- Developed and implemented OMNI, a self-service database, for tracking campus servers. The number of servers tracked in OMNI increased from 458 in 2005/2006 to 510 in 2006/2007.
- Implemented McAfee Foundstone for vulnerability scanning campus systems.
- 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 3** below regarding the growth of co-host and co-managed services.

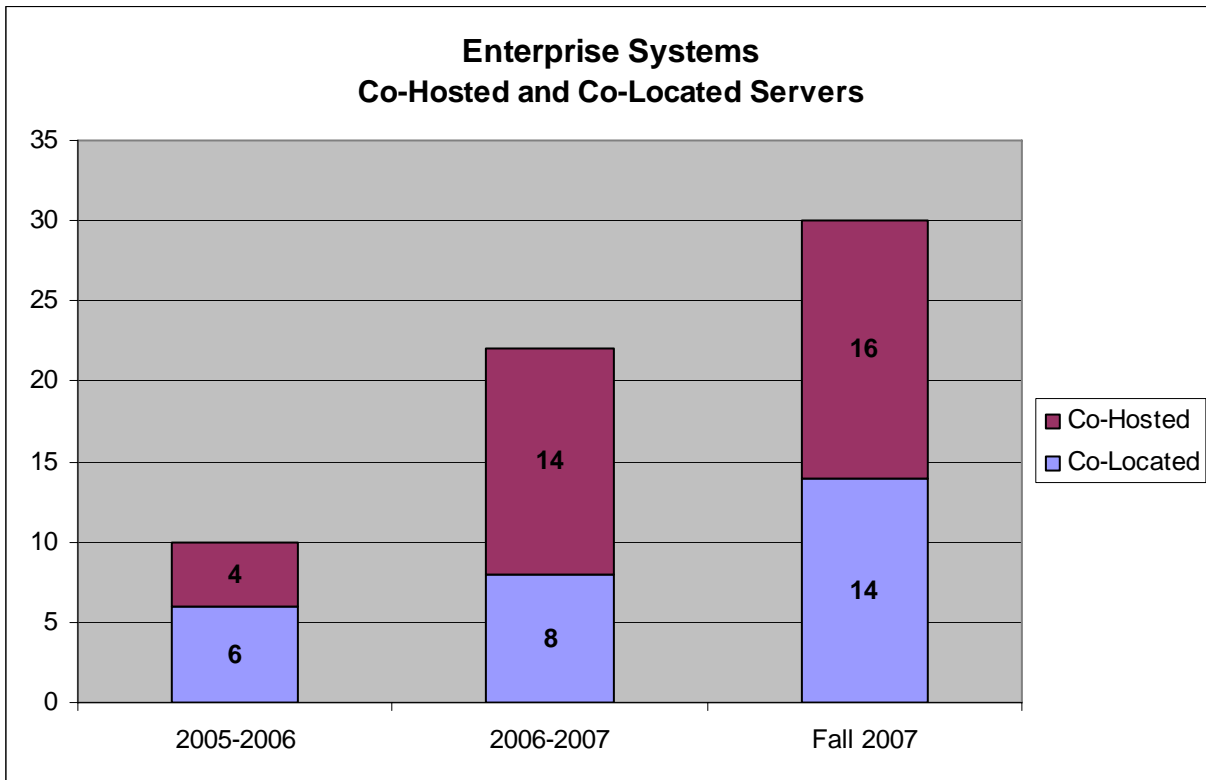


Figure 3

- Created an ESYS-secure configuration to include weekly vulnerability scans, encrypted backups, Dell OMSA hardware monitoring, Nagios hardware and application monitoring, maintenance windows and standard Change Request Form (CRF) usage.
- Completed System Security Worksheets (SSWs) on 66 systems to identify risks and develop mitigation strategies. An additional 30 SSWs are in process.
- Implemented Red Hat Enterprise Linux Satellite Server for centralized patching of Linux systems.

Incident Management

Improvements in security infrastructure, procedures, awareness and training all contribute to a solid information security program, but 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. This year we made very few changes to our incident management program. **Figure 4** below illustrates our trend in incident management.

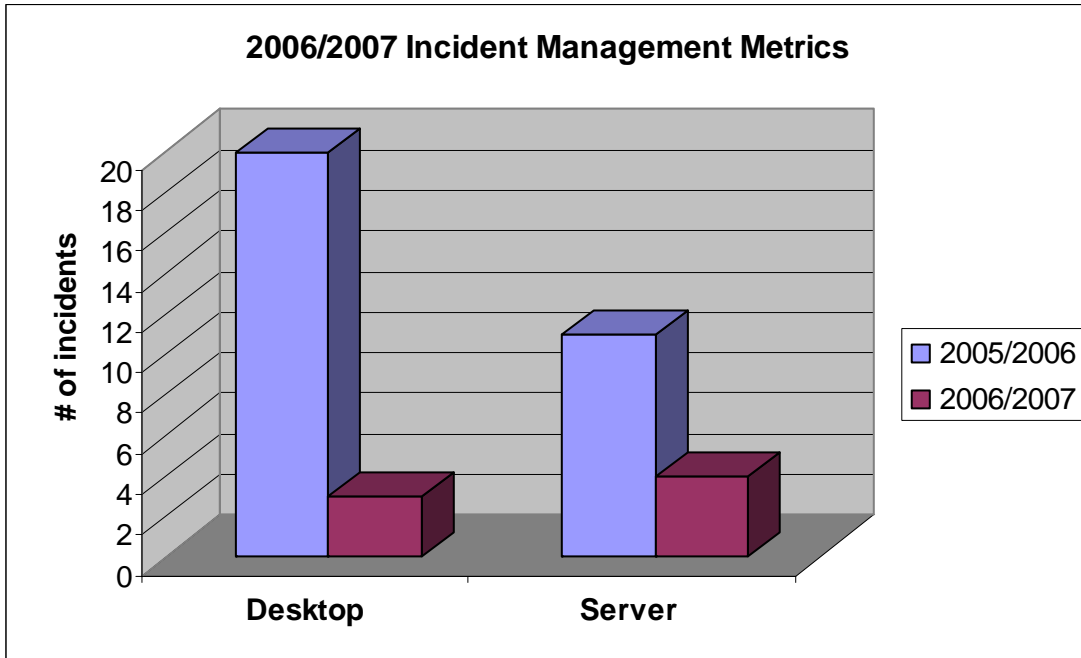


Figure 4

The number of desktop incidents continues to decrease in large part because of new tools (McAfee and LanDesk) used to manage desktop security centrally. Although the overall security of servers has improved this past year, the reduction in the number of incidents may be misleading. Many server compromises may not be reported to the Information Security Office, still more may go unidentified. These numbers also do not reflect investigation into possible events which did not turn into actual incidents.

Confidential Data

Protection of confidential information is a primary goal of the Information Security organization. In March 2005, six strategies were identified to protect decentralized confidential data. The following was accomplished in 2006/2007 to support these strategies:

- Implemented a new server registry database, OMNI. **Figure 5** below illustrates the percentage and number of campus servers containing confidential data as self-reported in OMNI. At this time OMNI does not indicate what level of protected information is contained on these servers. Capturing this information in OMNI is planned in 2007/2008 so that we can target the few remaining servers on campus which actually contain Level 1 (personally identifiable) information such as Social Security Numbers and Credit Card Numbers.

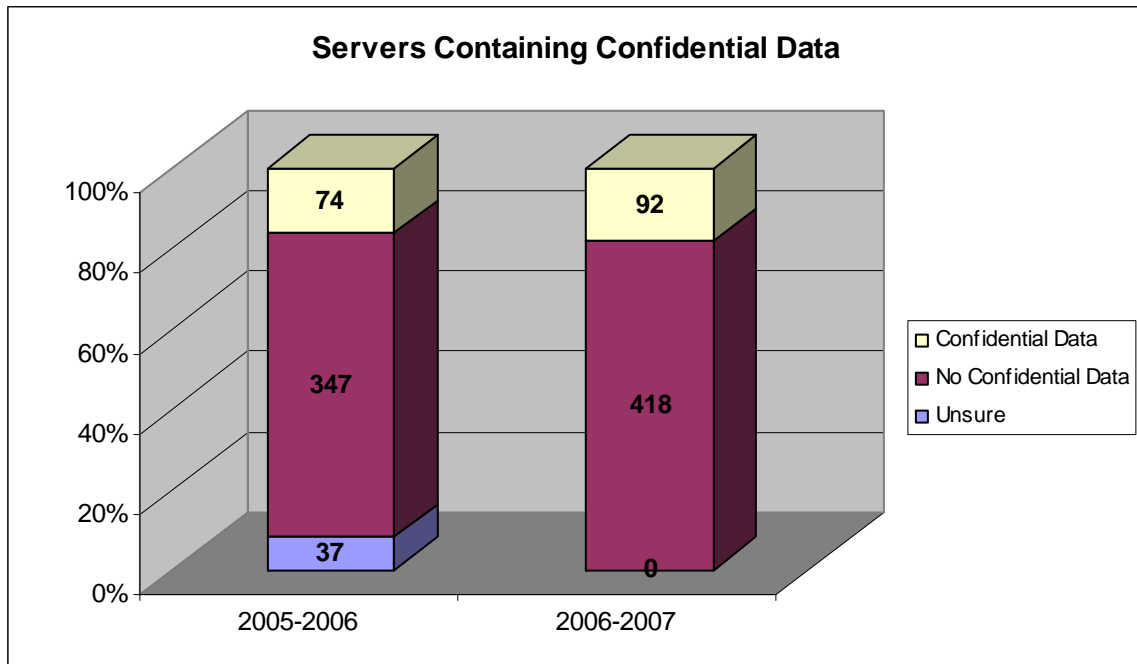


Figure 5

- Moved a number of 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.
- Began an analysis of enterprise and department databases containing confidential data to determine where confidential data is located, where it is sent from/to and how it is being protected.

CSU Activities

In 2006/2007 Janice Lim, CSU Senior Director of Information Security Management and the Information Security Advisory Committee worked on a number of initiatives. These include a Security Assessment by Unisys Consulting of nine campuses and the Chancellors Office against the ISO 17799 standard, the development of an RFP for a System-Wide Information Security Policy Development Project and the development of an RFP for a System-Wide Information Security On-Line Training Course.