

# Appendix D



**California State University, Chico**

## **Information Security Office 2005/2006 Annual Report**

June, 2006



## Introduction

Information security protects the valuable resources of an organization. It is a campus-wide responsibility. CSU, Chico is actively applying best practices as critical information systems multiply and threats propagate. The Information Security Plan established in fall 2004 addresses the substantial risks CSU, Chico faces today and outlines the roles, responsibilities, and policies designed to address these risks.

The Information Security Office works with the campus community to secure system and network resources and protect the confidentiality of student, faculty, and staff information. This annual report is a summary of the activities related to information security in the 2005/2006 academic year. The report is organized into the following sections: Awareness and Training, Security Infrastructure, Incident Management, Confidential Data, CSU Activities and Organizational Development. The report also briefly describes projects to be pursued in the 2006/2007 academic year.

## 2005/2006 Academic Year Activities

### *Awareness and Training*

The security events at CSU, Chico of the past couple of years, especially the security incident requiring the notification of the compromise of confidential data, have resulted in increased interest, understanding and support of security measures. The campus community is hearing about information security from multiple sources and understands more than ever that security threats are real and we are not immune. The following activities were coordinated by the Information Security Office in support of security awareness and training.

- Organized a Microsoft Security Onsite two-day training event for System Administrators. Over 40 technicians and managers from across campus participated in the event.
- Held two Server Manager Meetings to discuss data confidentiality, network and data center security, desktop security, new password policy and tool, server security procedures and guidelines, and incident handling. Over 50 server administrators attended these sessions.
- Facilitated two small group training sessions for 16 server administrators on System Security Worksheets. This worksheet aids system administrator in securing their systems and can be found at <http://www.csuchico.edu/inf/security/ServerWorksheet20060315.doc>.
- Facilitated two small group training sessions for ten server administrators on Analyzing Vulnerability Scan Results. Two types of scans were covered, one that is run by the system administrator and another more intensive scan that can be run by the Information Security Office to identify vulnerabilities in a system.
- Continually updated the Information Security Office website to provide the latest in security best practice information to campus staff and faculty.
- Distributed a series of communications regarding password security which covered password best practices, the new campus password restrictions and Chico Password Station tool.
- Distributed a series of communications about the use of confidential data including a brochure defining confidential data, a flyer with steps to protect confidential data and campus SSN Procedures and Guidelines. These documents can be found at <http://www.csuchico.edu/inf/security/>.
- Encouraged campus server administrators to attend the SANS Securing Windows Conference hosted at San Diego State University in August. At least four server administrators are currently planning to attend.

## ***Policies, Standards, Guidelines, and Best Practices***

Our efforts to improve campus information security are supported by the Policy on Use of Computing and Communication Technology, EM 97-18 [http://www.csuchico.edu/prs/EMs/EM97/em97\\_18.htm](http://www.csuchico.edu/prs/EMs/EM97/em97_18.htm). A number of new procedures and best practices were implemented this year to tighten campus security.

- Implemented stricter password requirements as well as the Chico Password Station tool to help faculty and staff users create/maintain stronger passwords.
- Implemented a procedure and database in partnership with the Environmental Health & Safety and Facilities departments to track the disposal of electronic devices to ensure that confidential data is removed from computers prior to their leaving campus. Thirty-four technicians have been trained and approved to perform these procedures.
- Implemented a procedure requiring all requests for static IP addresses and firewall exceptions to be reviewed by the Information Security Office.
- Reviewed the security of a number of vendor applications such as the Judicial Affairs Management System (JAMS) and Recreation Solutions IM Track and IMOnline to ensure the use of these vendor applications does not pose a significant security threat to the university.
- Documented enterprise data center procedures for Backup and Recovery, Patch Management and Change Management.

## ***Security Infrastructure***

The Information Security Office works in conjunction with campus technical departments to ensure the security of campus systems and confidential data. The Security Infrastructure section is logically separated into Network, Server and Desktop areas that are administrated by Network and Enterprise Server Operations and User Services.

### **Network**

- Purchased and installed a network access control solution for the residence halls to ensure that devices on the residence hall network are secure prior to gaining network access. Testing is underway to determine whether this solution may also be used for the wireless network.
- Developed a procedure to migrate servers to an even more secure DMZ firewall model and designed a mechanism to track the accompanying more complex firewall rules.
- Began an analysis of Intrusion Detection/Prevention System solutions for campus but decided to wait until the system-wide network security tool evaluation was complete before making a decision.
- Analyzed border firewall exceptions and reduced the number of exceptions from 286 to 233. For additional details see figure 1 in Appendix A.

### **Servers**

- Developed a number of new service offerings in Computing and Communications Services to enable campus departments to take advantage of application hosting, managed servers, hosted servers and co-location of servers in the data center. This effort is meant to leverage existing skills and infrastructure in Computing and Communications Services to benefit the campus community and secure campus systems and data. Currently less than 38% of campus servers are managed by Computing and Communications Services. For additional details see figure 2 in Appendix A.
- Updated the server registry to include information regarding confidential data stored on campus servers. See Appendix A for additional details regarding servers in the inventory.
- Initiated a project to better secure domain administrator accounts by implementing a multi-factor authentication solution. This solution will require domain administrators to use a login and

password, as well as a smart card (USB) to gain access to campus domain controllers.

- Initiated a project to implement a Public Key Infrastructure (PKI) to support multi-factor authentication of domain administrators and other information security initiatives such as encrypted e-mail and file storage.

## **Desktops**

- Implemented second generation Microsoft Update Server (WSUS) to provide rapid desktop security and Microsoft Office updates to campus. See figures 1 and 2 in Appendix B for additional details regarding WSUS.
- Implemented McAfee ePolicy Orchestrator (ePO) to centrally manage both Macintosh and Windows desktop anti-virus software. Each desktop with an agent reports back to the server every 15 minutes regarding its anti-virus software status. This solution includes a silent spyware component. Increased McAfee installs by 250 machines, 93% are at currently level of .DAT coverage. See figures 3 and 4 in Appendix B for additional details regarding McAfee ePO.
- Increased the number of Windows and Macintosh desktops in the Chico domain to 2117 and 190 respectively. Systems in the domain can have security policy applied centrally in minutes if necessary.
- Began applying security updates to Macintosh OSX machines automatically.
- Upgraded 95% of campus desktop machines running Windows XP to Service Pack 2. Continued to upgrade desktops from Windows 2000 to XP. 20% of campus desktops still run Windows 2000 however the majority will be replaced or updated with this desktop computer replacement cycle.
- Conducted a pilot test using DeepFreeze in public computer labs to improve patch management and security of systems.

## **Incident Management**

Improvements in security 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. The following activities were undertaken to improve our incident management capability.

- Managed approximately 20 desktop security incidents involving malicious programs such as Trojans and root kits. The number of desktops impacted by viruses is not included in this number
- Managed approximately 11 server security incidents, involving 30 servers. Of these servers, two contained confidential data. Forensic analysis found that this data had not been accessed during the compromised thus eliminating the need for notification.
- Implemented a cross-department Forensics Lab in partnership with UPD and USRV.
- Presented the high-level incident handling procedures to campus Server Administrators with emphasis on contacting the Information Security Office immediately if a compromise is suspected. Any changes made to a system after a compromise is suspected could result in more challenging, if not impossible, forensic analysis.

## **Confidential Data**

The Information Security organization's overarching goal is to protect the confidentiality, integrity and availability of information, systems, and network resources. In March 2005, six strategies were identified to protect decentralized confidential data. The following was accomplished in 2005/2006 to support these strategies. For additional details, see Appendix C.

- Converted the majority of campus systems from the use of SSN to Chico State ID (PeopleSoft EMPLID) as the primary identifier for students, faculty and staff.
- Updated the server registry database to include information regarding confidential data stored on campus servers and identified a number of unregistered servers.
- 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 Computing and Communications Services trained system administrators.
- Began an analysis of enterprise and department databases containing confidential data. The objective of the analysis is to determine where confidential data is located, where it is sent from/to and how it is being protected. In addition, we will validate that access to confidential data is approved, tracked and audited in a consistent manner across campus.
- Distributed a series of communications about the use of confidential data including a brochure defining confidential data, a flyer with steps to protect confidential data and campus SSN Procedures and Guidelines. These documents can be found at <http://www.csuchico.edu/inf/security/>.

## ***CSU Activities***

In January 2005, Janice Lim was appointed at the CSU's new Senior Director of Information Security Management. Janice provides policy leadership for the campuses and the Chancellor's Office to ensure that information in the CSU is handling according to best practice and legal obligations. Janice began having regular meetings of the campus Information Security Officers in the spring 2005. This group has accomplished the following in the 2005/2006 academic year.

- Established a charter for the group, the Information Security Advisory Committee, with the charge to advise the CSU Senior Director of Information Security Management and campus constituents on standards, policies and practices related to the selection, funding, deployment, management and assessment of information security in support of system-wide and campus-based academic and administrative groups.
- The CSU, Chico Information Security Officer was elected to serve as the committee's Secretary for the 2006 calendar year.
- Established working groups to develop system-wide policies for Acceptable Use, Access Control, Data Classification, Patch Management, Records Retention, Roles and Responsibilities, and Security Awareness. Policies are in a variety of stages of development and review.
- Held three face to face and one conference call meeting as a group, in addition to a significant number of policy working group sessions via conference call.

## ***Organization Development***

As stated in the introduction, the Information Security Office's mission is to work with the campus community to secure system and network resources, and protect the confidentiality of student, faculty, and staff information. The following actions have been taken in 2005/2006 to better prepare the organization to fulfill its mission.

- Hired a Technical Security Analyst to take the lead in the development of the technical security architecture and facilitate our incident handling processes.
- Sent the Technical Security Analyst to a six-day SANS Security Essentials Training course and obtained corresponding GIAC certification.
- Scheduled a five-day Encase Forensics software training course for the Technical Security Analyst and one of the User Services Field Technicians to attend in July 2006.
- In the process of hiring an Information Security Analyst to take the lead in identifying where confidential data on campus is stored and how it is protected.
- The Information Security Officer and Technical Security Analyst attended the 4<sup>th</sup> Annual Secure IT Conference in spring 2006.

## 2006/2007 Academic Year Goals

### ***Awareness and Training***

- Develop and implement a communication plan for National Cyber Security Awareness Month in October.
- Develop a series training courses, in partnership with campus data authorities/stewards, for staff, faculty, and student employees regarding data confidentiality.
- Hold two Server Manager Meetings in the summer 2006, fall 2006, and spring 2007 to continue our efforts to share information security best practices.
- Facilitate additional small group training sessions for server administrators on topics such as Hardening a Windows Server, Hardening a Linux Server, and Intrusion Detection at the Server/System Level.
- Facilitate a small group training session for managers/system owners to provide them the knowledge necessary to ask the right questions of their system and applications administrators regarding information security of their systems.
- Continually update the Information Security Office website to provide the latest in security best practice information to campus staff and faculty.

### ***Policies, Standards, Guidelines, and Best Practices***

- Create/update and communicate best practice procedures for Backup and Recovery, Patch Management, Change Management, Data Retention, and User Access Management to campus application and server administrators.
- Update Server Security Procedures and Guidelines to reflect current best practices.
- Participate in a review of the process for separating employees to ensure all proper actions are taken to disable/remove/update user access to campus information resources.
- Review the security of new vendor applications to ensure the use of these applications does not pose a significant security threat to the university.
- Review and update the Information Security Plan originally approved in fall 2004.
- Develop wireless network security standards and guidelines.
- Develop requirements and procedures for access to secure campus file storage solution.

### ***Security Infrastructure***

#### **Network**

- Evaluate the network access control solution implemented for the residence halls to determine whether it may also be used for other campus networks, especially the wireless network.
- Begin migrating campus servers to an even more secure port-based firewall model and develop a mechanism to track the accompanying more complex firewall rules.
- Evaluate the feasibility of implementing a DMZ in our network for specific campus systems.
- Evaluate the system-wide solution selected for Intrusion Detection/Prevention and determine an appropriate implementation approach.
- Continue to analyze border firewall exceptions and reduce the number wherever possible.
- Implement a solution for secure wireless access to support the more comprehensive no cost wireless

network rollout.

- Implement VPN groups to better segregate and secure selected users and systems. Investigate utilizing information in LDAP to dynamically assign users to the groups.
- Begin the analysis of IPSec as a solution to secure information on the network.

## **Servers**

- 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
- Migrate campus systems to the application hosting, managed servers, hosted servers and co-location service offerings in Computing and Communications Services. This effort leverages existing skills and infrastructure in CCSV to benefit the campus community and secure campus systems and data.
- Continue to update the server registry and develop a web-based database solution for tracking and updating this information.
- Implement a multi-factor authentication solution for domain administrator accounts. Evaluate the effectiveness of the solution and consider a rollout to a larger group of server administrators.
- Implement a Public Key Infrastructure (PKI) to support multi-factor authentication of domain administrators. Evaluate its usefulness for other information security initiatives such as encrypted email and file storage.
- Begin a regular schedule of auditing and vulnerability scanning campus servers utilized an automated scanning solution.
- Develop an implementation plan for secure storage of confidential information for specific targeted departments.

## **Desktops**

- Continue to increase the number of Windows and Macintosh desktops in the Chico domain.
- Continue to increase the number of McAfee installs on campus.
- Migrate all Windows 2000 users to Windows XP.
- Continue to upgrade campus desktop machines running Windows XP to Service Pack 2 or other new service packs.
- Evaluate DeepFreeze pilot test results and identify approach to improve patch management and security of public computer lab computers.

## ***Incident Management***

- Improve our ability to manage desktop and server security incidents using best practice incident handling procedures as well as our new cross-department Forensics Lab.

## ***Confidential Data***

- Convert remaining campus systems from the use of SSN to Chico State ID (PeopleSoft EMPLID) as the primary identifier for students, faculty and staff.
- Continue 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 Computing and Communications Services trained system administrators.
- Continue the 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.
- Develop a standardized procedure to ensure that access to confidential data is approved, tracked, and audited in a consistent manner across campus.
  - Continue to distribute communication messages about the use of confidential data.
  - Research a tool to enable faculty and staff to search their systems for confidential data.

### ***CSU Activities***

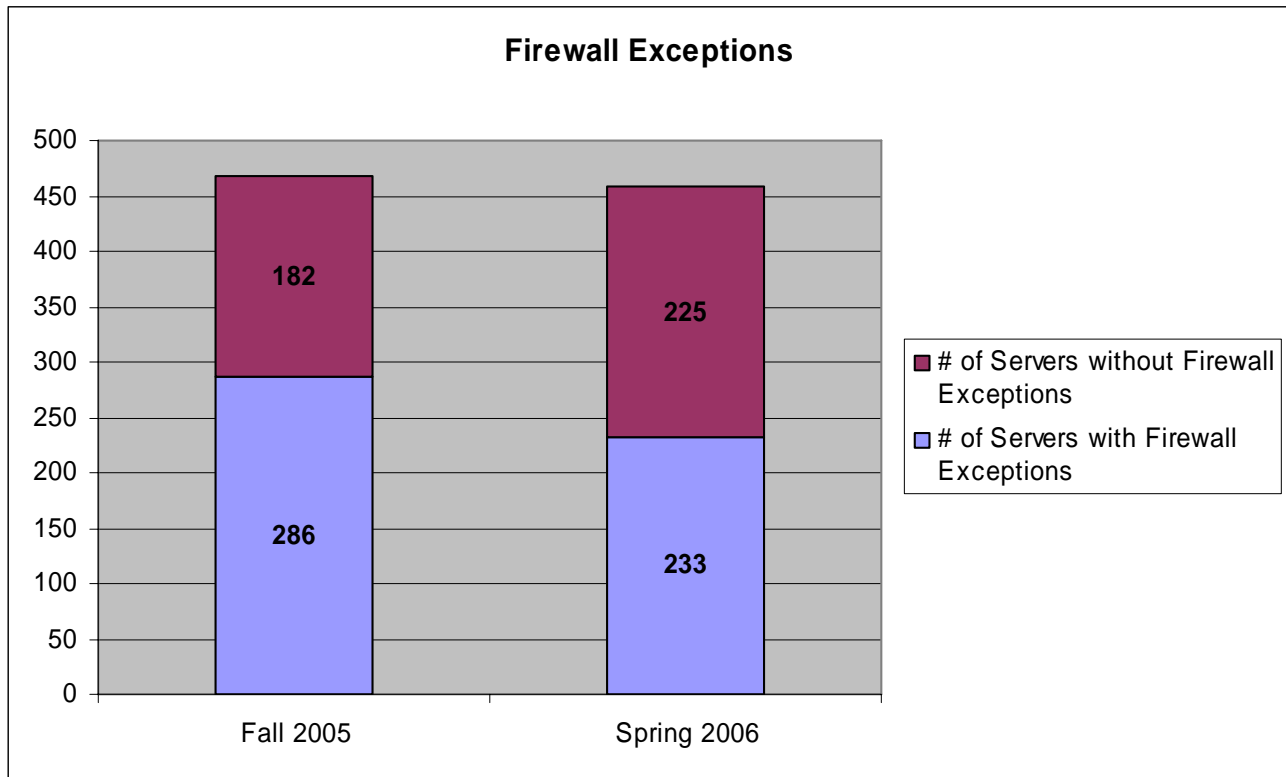
- Attend a meeting of the Information Security Advisory Committee once per quarter and serve as the committee's Secretary through the 2006 calendar year.
- Continue participation in working groups to develop system-wide policies for Acceptable Use, Access Control, and Data Classification.
- Chair a working group regarding data encryption.
- Participate on a committee to discuss security requirements of ITRP2.

### ***Organization Development***

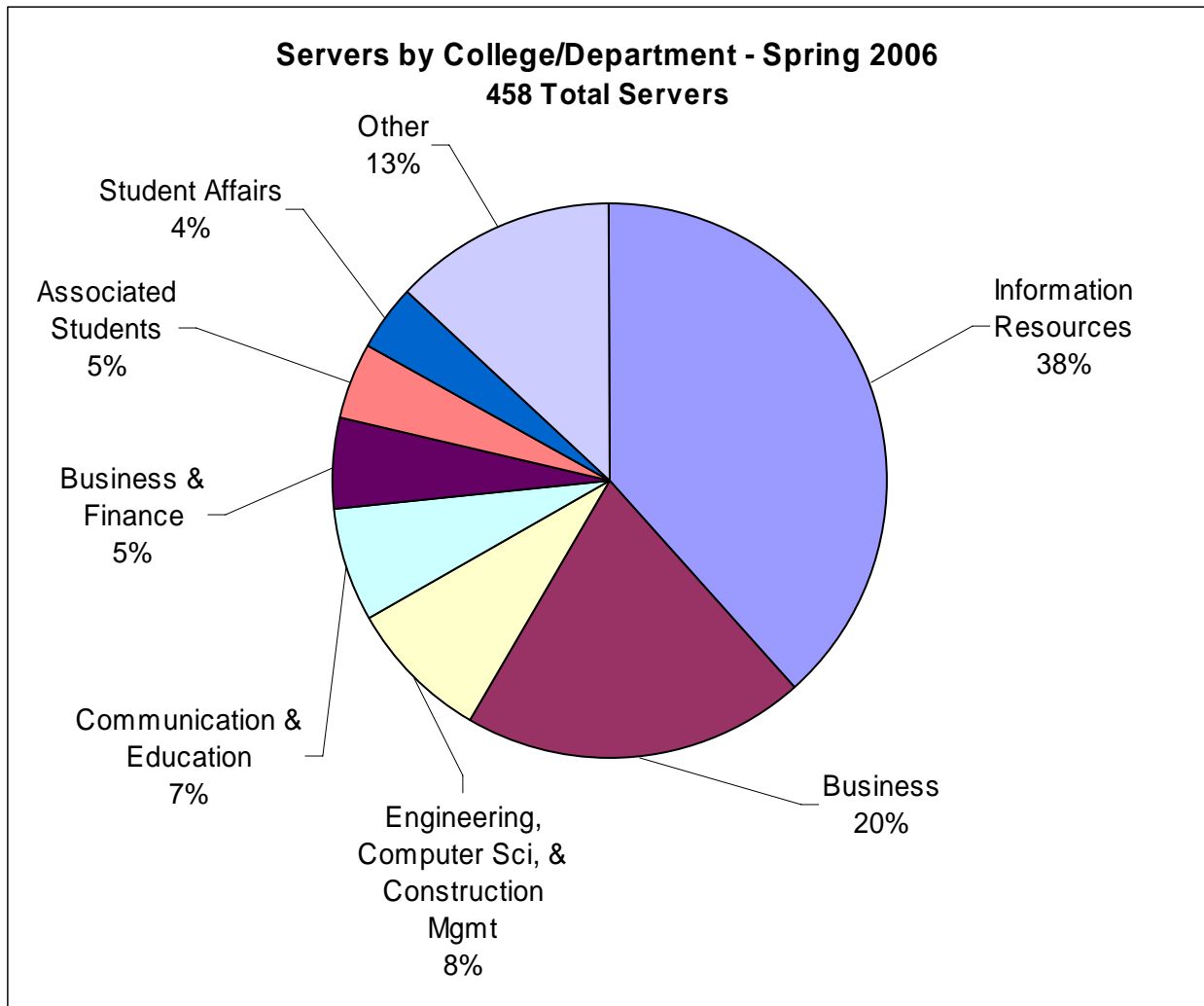
- Hire the Information Security Analyst to take the lead in identifying where confidential data on campus is stored and how it is protected and evaluate their training and development needs.
- Send the Technical Security Analyst to a six-day SANS Securing Windows course.
- Send the Information Security Analyst and Technical Security Analyst to a SANS course, topic to be determined.
- Send the Technical Security Analyst and one of the User Services Field Technicians to a five-day Encase Forensics software training course.
- Send the Information Security Office staff to either the 5<sup>th</sup> Annual Secure IT Conference or the Educause Security Conference in spring 2007.

## Appendix A – Server Inventory Details

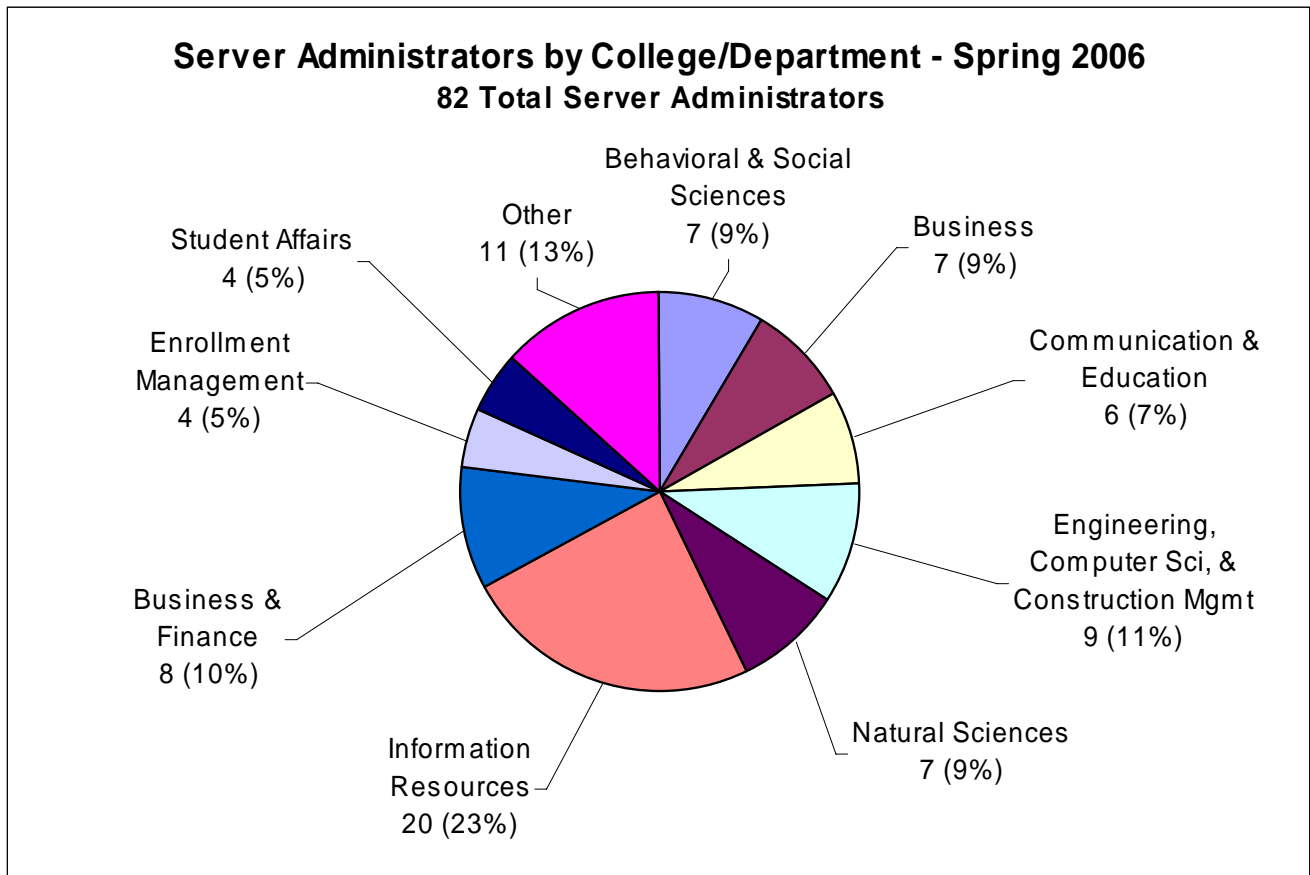
**Figure 1** - This bar chart shows the number of servers with and without exceptions (holes) in the border firewall. Over 50 exceptions were removed between fall 2005 and spring 2006. Work in 2006/2007 will be done to continue removing exceptions, as well as implementing further restrictions in the border firewall for the 233 servers that still have exceptions.



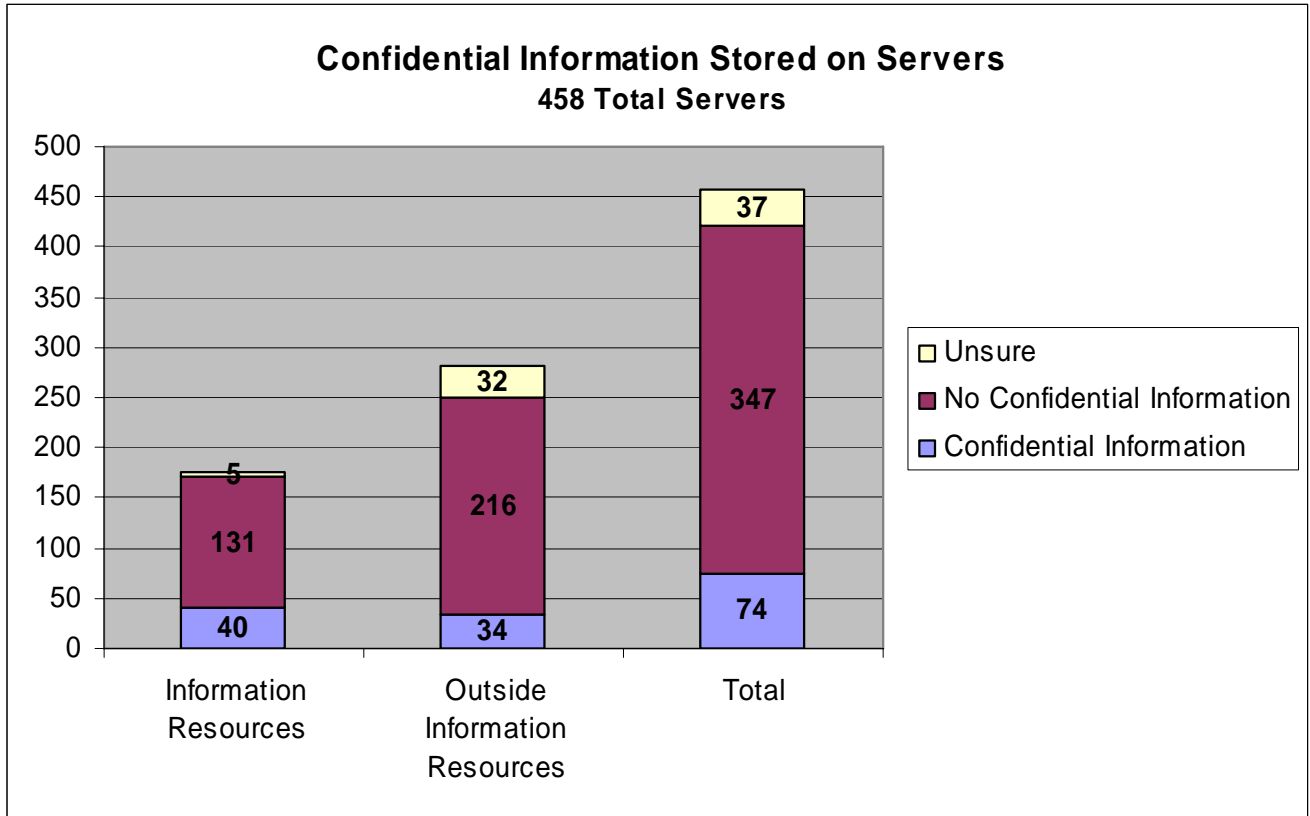
**Figure 2** - This pie chart shows the percentage of servers by college/department. Colleges/departments with less than 17 servers are grouped as other.



**Figure 3** - This pie chart shows the percentage of server administrators by college/department. Colleges/departments with less than 2 server administrators are grouped as other.

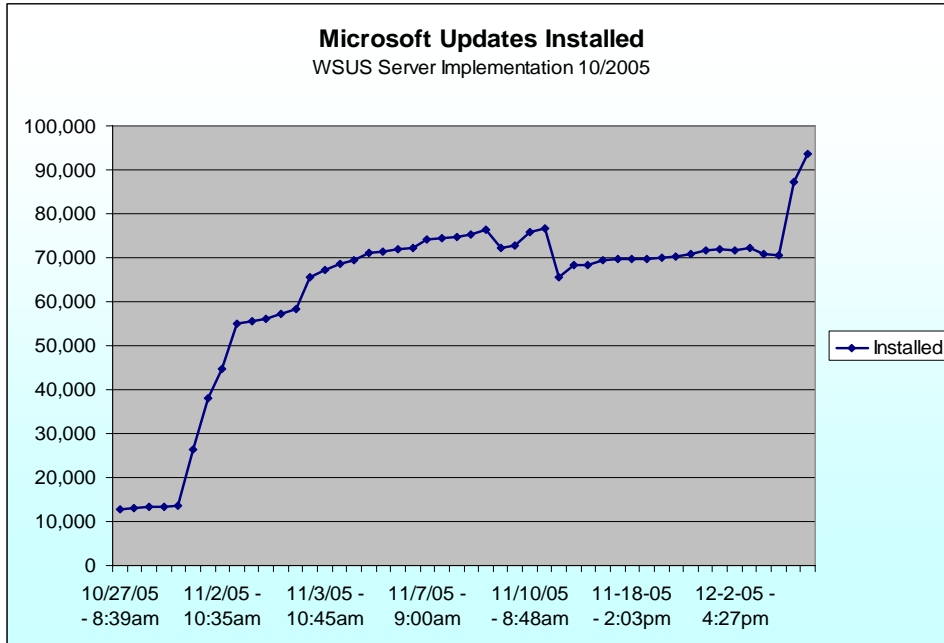


**Figure 4** - This bar graph shows the number of servers reported to contain confidential data managed by Information Resources and outside Information Resources. The breakdown of servers with and without confidential data for the entire campus is also displayed.

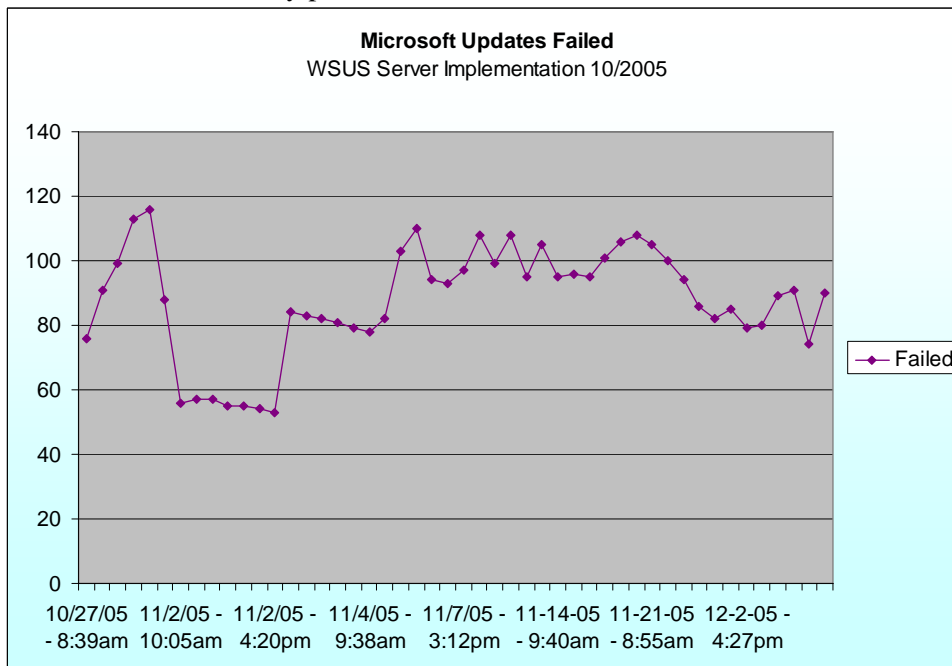


## Appendix B – Desktop Security Details

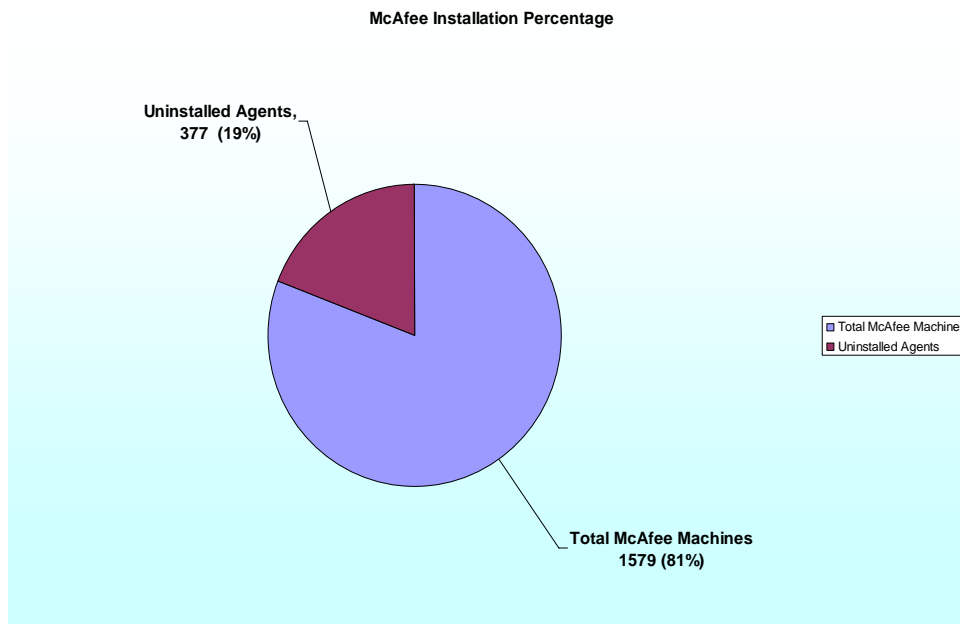
**Figure 1** - This line graph shows the number of Microsoft Updates that were installed via Windows System Update Server (WSUS) in the first six weeks following its implementation.



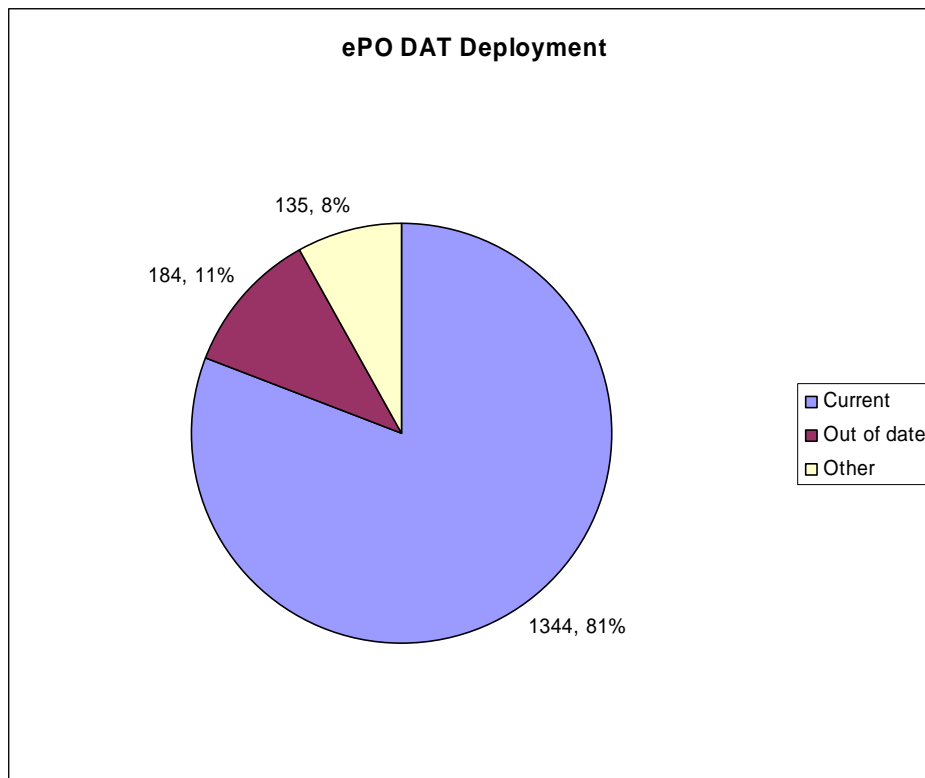
**Figure 2** - This line graph shows the number of failed Microsoft Updates during the first six weeks following WSUS implementation. Considering that on average 60,000 updates were successfully installed, failures around 100 are extremely positive.



**Figure 3** - This pie chart shows the percentage of machines with McAfee that have the ePO agent installed and are currently being monitored.



**Figure 4** - This pie chart shows the percentage of machines with the most current virus definition update file from McAfee ePO.



## Appendix C – Strategies for Security of Decentralized Information

1. **Elimination of Social Security number as unique identifier:** CMS/PeopleSoft Administrative systems eliminate the need to use Social Security numbers as the key identifier for faculty, staff, and students in all enterprise wide computing systems. Instead of SSN, faculty, staff, and students will use the CMS generated unique ID, which is referred to as the *Chico State ID*. Our goal is to convert all decentralized campus computing systems to Chico State ID as their key identifier by the end of fall semester 05.
2. **Server inventory and data identification:** To assure that campus confidential information is secure, it is essential to identify which servers on campus may contain such data. Our goal is to identify and classify servers across the campus by their level of security risk.
3. **Elimination of distributed confidential data:** Removal of confidential data from servers and desktops is the most secure method of assuring these machines will not directly disclose confidential data through a compromise. Our goal is to eliminate confidential data from distributed servers and desktops which do not have an absolute business need for such data. We will approach this problem through:
  - a security awareness plan
  - support for identifying and deleting confidential data
  - support for archiving confidential data in a more secure form
  - centralized storage for confidential data
  - providing alternate ways to deliver confidential data required for the business need of a unit (e.g. CMS/warehouse queries).
4. **Relocation of decentralized servers storing confidential information:** Information Resources provides a centralized secure environment with staff trained in advanced server management techniques. The goal is to work with units across campus to move servers with confidential data to a more secure central environment.
5. **Requesting/tracking of confidential information:** Campus data policies and procedures will be updated to provide a methodology for requesting all confidential data in electronic format. Requests will be subject to authorization, tracking, and auditing. Our goal is to assure this data is distributed only to secure servers where there is a business need for the data.
6. **Communication/training on security topics:** Communication and training are essential in maintaining data security, since the use of confidential data is spread across the campus. Our goal is to make the entire campus community aware of and active participants in maintaining a secure confidential information environment.

Strategy	Progress
Elimination of Social Security number as unique identifier	Converted the majority of campus systems from the use of SSN to Chico State ID (PeopleSoft EMPLID) as the primary identifier for students, faculty and staff. Some key systems (LDAP, Wildcat Card, etc.) continue to utilize SSN as the key identifier; however this should be phased out by the end of 2006.
Server inventory and data identification	The server inventory has been updated to include information regarding confidential data stored on the server. Used this information to prioritize the servers and are working with server administrators to better secure systems. Metrics have also been gathered based on data in the server inventory and can be located in Appendix A.
Elimination of distributed confidential data	Distributed a brochure and flyer regarding confidential data as well as SSN Procedures and Guidelines. Increased centralized storage space (on Bay) so that individuals and departments who can not delete data can move it to a more secure location. Working with units to eliminate the need for confidential data to carry out university business. Reviewing records retention policies.
Relocation of decentralized servers storing confidential information	Beyond the main enterprise data system (e.g. PeopleSoft, e-mail, directories, etc.) there are dozens of areas that have decentralized servers that may contain confidential data. See Appendix A. A half a dozen servers/systems have been relocated to the data center's physically and technically secure environment. Continuing to work through the list of identified servers. If confidential information can not be eliminated on distributed servers through business redesign, the servers will be moved to the data center.
Requesting/tracking of confidential information	Begun the work to document/track confidential data. Continuing this work will be the primary responsibility of the Information Security Analyst.
Communication/training on security topics	A number of training opportunities have been provided to server administrators including a two day Microsoft Security Clinic. Security is a component of CMS training classes. Security updates to the campus occur regularly through the use of campus announcements and information distributed the campus mailboxes. A security website <a href="http://www.csuchico.edu/inf/security">http://www.csuchico.edu/inf/security</a> is available to provide security best practices as well as current security policies and procedures. Planning is underway to take advantage of National Cyber Security Awareness Month in October. Training will also be developed for faculty, staff and student employees regarding data confidentiality laws, policies, and procedures.