

Appendix C



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

Information Security Office 2007/2008 Status Report

August 2008

Information Security Status Report

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 2007/2008, Security personnel spent the majority of their time preparing for the system wide Information Security Audit by conducting a self-assessment followed by document collection. The Security Audit began June 23, 2008.

The early goal of the CSU, Chico self assessment project was to identify, in advance, any potential audit findings. As the project matured, it became evident that an even more significant goal was being achieved. The campus was gaining a better understanding of the practices required to ensure confidentiality, integrity and availability of information and systems. Further, these processes and tools represent good information technology practice. Establishing new tools and processes to fill the gaps will mature information technology on the campus and ultimately enable CSU, Chico to provide better, more reliable information technology services.

Self Assessment

In fall 2007, CSU, Chico conducted a self assessment of its security environment across campus departments. A gap analysis was performed against the ISO 17799 standard. The ISO 17799 standard includes eleven security clauses collectively containing thirty-nine main security categories. Each main security category includes a control objective and one or more controls that can be used to achieve the objective. Overall there are hundreds of objectives and controls in the standard. The campus will use the gap analysis information to assist in risk assessment and prioritization of the controls.

Scope for the audit included systems defined as critical, and as such, the campus narrowed the scope of the gap analysis to approximately 150 of the 500 campus servers. A database was created to facilitate data gathering and reporting from twenty department managers. The department managers reported the maturity level of the control (identified by the ISO17799 standard) in their department, an explanation of the maturity level selected, and any audit evidence available to support their assessment. An industry standard Capability Maturity Model (CMM) was customized to meet campus needs.

Documentation Preparation

Six weeks prior to Chico's audit start date the Office of University Auditor sent two document request lists. To respond to these lists department managers from across campus, including the Auxiliaries, collected over 360 documents. Many of these documents were posted in the campus Wiki to enable departments with a more mature level of control to share their procedures with other departments working to increase their maturity level.

System Security

In 2007/2008 we continued to analyze border firewall exceptions and made significant progress to either eliminate exceptions or build rules which open only pinholes in the firewall. Over 50 servers had well-defined rules implemented, see **Figure 1**.

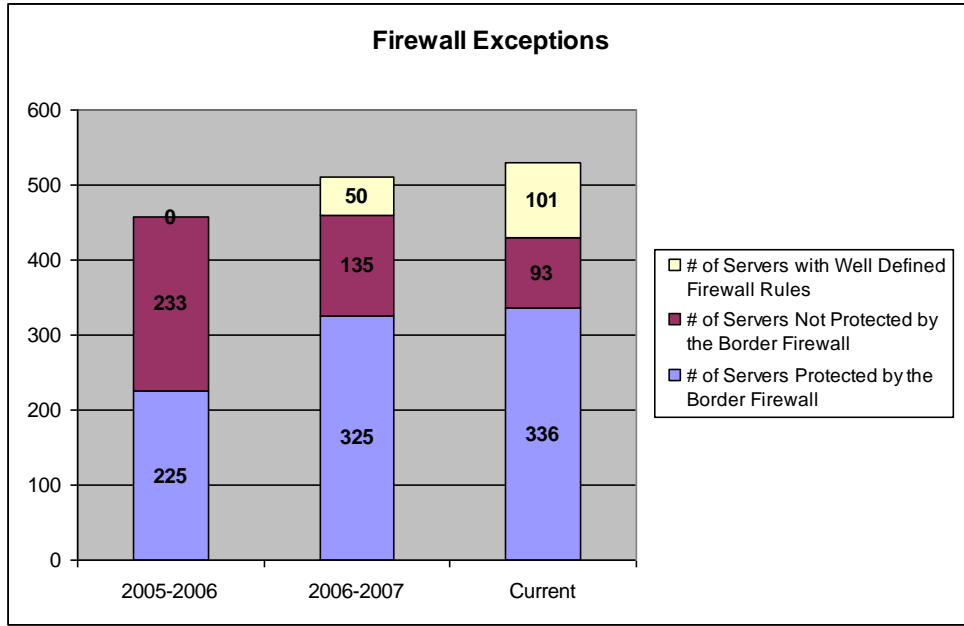


Figure 1

Awareness and Training

Raising awareness regarding information security and ultimately changing employee behavior is the single most important thing Chico can do to better secure its environment. The following activities in **Table 1** were coordinated by the Information Security Office in support of security awareness and training:

2007/2008 Information Security Internal Training Metrics				
# Events	Event Type	Attendance	Total Time (mins)	
2	Protect Yourself/Campus from Cyber Threats Course	33	180	
12	New Hire Orientation	80	165	
3	Security Processes	11	270	
1	Server Manager Meeting	38	90	
1	Web Application Security Meeting	30	90	
3	Vulnerability Management Training	8	180	
		200	975	

Table 1

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

2007/2008 Information Security External/3rd Party Training Metrics			
# Events	Event Type	Attendance	Total CPE Credits
1	SANS Web Application Security	11	154

Table 2