A Proactive Campus-wide Approach:  
Defending Cal Poly from Desktop, Mobile Computing and Network Attacks

The Problem and an approach to address it: Due to the significant increases in volume and the complexity of security related incidents, the negative impact on campus productivity and the cost to the campus community, and prompted as well by added regulatory/audit compliance driven measures, Cal Poly will need to start implementation of more proactive and specifically focused initiatives effective August 2004 to better protect our capability to support the instructional mission of the university. The campus-wide holistic approach recommended includes ASI, Foundation, State and Auxiliaries - and includes cross-functional processes to ensure effective diagnostics, communications, incident response and resolution times and to enable a proactive and systemic result.

The items outlined below are "best practices" adopted from internationally recognized security organizations (e.g. CERT, ISO, NIST, SANS), the CSU and UC systems and higher-education institutions that have successfully implemented similar, proactive campus-wide initiatives.

For this campus effort to be successful, active involvement from campus LAN Coordinators in establishing technical requirements is essential. Open forums and technical discussions will lead to consensus of "baseline standards" and "best practices". Initial discussions will commence August 2004 to assess which campus units are currently using automated operating system and update services for workstations, laptops and servers. Note: several key areas of the campus have already implemented desktop management and security processes. A campus framework will then be developed mobilizing the campus, prioritizing security threats, establishing toolsets, training and best practices and policy recommendations.

It should be emphasized that specific solutions exist to address "desktop management" and security, but Phase I technical standards and policies are not yet defined. Final affirmation and adoption of these technical standards and policies will occur through LAN Coordinators and campus computing committees (AACC, IACC, IRMPPC and SC3).

The immediate needs to harden the campus infrastructure in advance of Academic Year 2004-2005 (Phase I) will utilize existing resources and are best characterized as "Low Hanging Fruit". Phase I will commence beginning August 2004 and will be complete by December 2004 to accommodate faculty and staff that are not present during Summer Quarter. Medium-term prioritization (Phase II) will involve multiple levels of campus planning and feedback during Fall Quarter, with actionable paths forward defined no later than December 2004.

Phase I – Immediate Needs to Harden Campus Infrastructure: August-December 2004

1. Initiate means and processes to automate patching and update services for all on-campus workstations, laptops and servers, with priority actions being on Microsoft operating systems.

2. Implement managed anti-virus software for all on-campus workstations, laptops and servers, with priority actions being on Microsoft operating systems.

3. Implement desktop management account procedures as outlined in CSU “Guidelines to Security”. Specific examples include: account login and password management; use of screen savers and lockout; password expiration; single user account access vs. admin or shared account(s); turning off computer when leaving the office; and turning off unnecessary services and network ports.

4. Implement common "incident management" tracking (Remedy) in all technical support areas, to facilitate "end-to-end" communication and resolution of cross-functional service requests in an expedient manner and to permit campus-wide assessments of threats and vulnerabilities.

5. Conduct selected pilot(s) to validate updated campus-level security response team model and integrate "lessons learned" into hybrid campus model. Articulate resources required for sustainable policy and security training, documentation on roles, responsibilities, and standard toolsets for desktops, laptops, mobile computing and networks.
Discussion DRAFT

Phase II – Medium-Term Needs: Actionable Paths Forward Defined by December 2004

1. Identify, formalize and communicate criteria, processes and standardized toolsets to address security driven compliance measures in support of teaching, learning and administrative services.

2. Implement software standards for all campus workstation and laptop deployments, utilizing best practices from the Workstation Program and customized packages ("modular approach") for specific departmental needs. This includes refinements such as security and network settings and utilities to address malware, spyware, desktop firewall, encryption needs and other "root cause" security and service request issues based upon historical Remedy analysis.

3. Implement a single, unified Cal Poly Active Directory to ensure continuity in access to resources, workstation and laptop authentication, security standardization and software management.

4. Convert Open Access computing labs, Robert E. Kennedy Library and other campus “public access” terminals to an authenticated environment to access campus resources.

NOTES

LAN Coordinators: Working Group Recommendations and Next Steps

- LAN Coord sub-group meetings Wed 7/14 and Tue 7/27
- Larger LAN Coord meeting Tue 8/10

Add to Discussion Draft: Statement of need in “user speak” and “what are we trying to solve?” (aka don’t mandate a specific solution; meet minimum spec/standard and build on top of existing base image. Real challenges exist with variability of base images and specific college/departmental/division needs).

Points of Emphasis From LAN Coord Working Group:

- Start with needs, then policies and centralized implementation (consolidation).
- Anti-virus server debrief with LAN Coords was well received, affords decentralization (v9 handout)
- Phased approach vs. “big-bang” (increase success rates through proven pilots)
- Definition of terms (e.g. “desktop management”) is essential; ditto for best practices and policies
  - Control means different things to different people (e.g. operating system, application, core services)
  - Due diligence ties back directly to audits and best practices (e.g. CERT, ISO, NIST, SANS)
  - Standardization of configurations (e.g. passwords, naming conventions, network settings)
- Control and process points should be emphasized (e.g. when signing up for wireless access, install campus anti-virus site license software and demonstrate it’s operational using managed client)
- Further discussion is required on best practices, policies and identifying resource implications and recommendations by working group, larger LAN Coord group
- User experience: keep this in mind, balancing the preventative and holistic approach

Continued on next page
### LAN Coordinators: Working Group Recommendations and Next Steps - Continued

#### Examples of Phase I Activities (translated into “user speak”)

<table>
<thead>
<tr>
<th>Activity / Areas of Focus</th>
<th>Priority</th>
<th>Timeline</th>
<th>Why are we doing this?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated patching and update services for Windows operating systems</td>
<td>High</td>
<td>Start immediately (Aug ’04)</td>
<td>Most common source of attacks and exploits; easily prevented with existing technology that is available at now and at no cost.</td>
</tr>
<tr>
<td>Anit-virus software and managed clients for faculty, staff and students</td>
<td>High</td>
<td>Start immediately (Aug ’04)</td>
<td>Second most common source of attacks and exploits; easily prevented with existing technology that is available at now via campus site license.</td>
</tr>
<tr>
<td>Remedy service request and incident tracking</td>
<td>Med High</td>
<td>Start immediately (Aug ’04)</td>
<td>Expedite handling of complex and inter-related security attacks and virus outbreaks across campus.</td>
</tr>
<tr>
<td>Pilot to affirm validate campus-level security response team model with college/division</td>
<td>Med High</td>
<td>Prep for phased approach now; start Sep-Nov ’04</td>
<td>Test and refine framework; identify resources, roles, responsibilities, toolsets, best practices and policy recommendations.</td>
</tr>
</tbody>
</table>