### Increased IT Security

Recommendations for significantly strengthening IT security requirements are only made more urgent by the crippling events of August 2003 (Blaster, Sobig.F, Nachi, etc.), which are expected to set a new baseline for malicious security activity.

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Current Status</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| 1. Incident Response | For two years, the campus has had an incident response coordination team to coordinate handling of major IT security events. However, this model needs to be significantly revised to meet today’s challenges. | - Update campus network procedures to clearly define the isolation process, including communications and delegation of authority, for errant systems or networks.  
- Explore requirements to establish an emergency response team (CERT/FIRST). |
| 2. Campus Investment in Desktop Antivirus Software | Sophos antivirus software is now available for all campus computers and home computers. A communications campaign to increase awareness in the home user population and to help the transition from the old McAfee product for campus departments will begin this Fall. | - Move to require antivirus software on campus equipment (noting that there will always be exceptions), including definition of appropriate enforcement mechanisms.  
- Consider this funding model for other security products as appropriate. |
| 3. Scanning | a. Scanning the UCLA network for vulnerabilities is slated to be in place by end of Fall Quarter 2003. Scanning will look for vulnerabilities in computers, not at data or content.  
 b. Intrusion detection for the BOL modem pool is slated to be in place in Fall Quarter 2003.  
 c. Initial campus-wide intrusion detection deployment by end of Fall Quarter 2003. | - Set the expectation that the regular scanning and intrusion detection of the entire UCLA network is necessary.  
- Set clear responsibilities for remediation of errant systems. |

Thematic question: When do the needs of one research project, department or individual outweigh the needs of the entire campus and when does the good of the entire campus outweigh the needs of the individual, the academic unit or the department?