



Fermilab

Computer Security Summary

We have two basic duties in Computer Security -- to protect the mission of the lab from disruption and to perform due stewardship of the government's resources we operate. The first is integrated into our lab management and relatively clearly defined. The second is not. Defining "due stewardship" is a major function of the CSExec and Computer Security organization. As often as not this function includes redirection of counterproductive mandates from the DOE.

Our basic strategy has been to focus on controlling access to our resources rather than what can be done with them. Our general lab policy is "default allow" specifically to allow maximal freedom for researchers. This leads to our initial focus on strong authentication.

The recent efforts on monitoring and focussed reminders/instructions has been very effective in incremental improvement to our overall posture. Bulk scans or generalized guidance has been less effective.

Our incident response capability is world class and widely respected in DOE and among our collaborators. Maintaining the caliber and capabilities of this group is essential to our strategy of "reactive defense". This strategy is what allows us to avoid overly focusing on what COULD happen and keep a localized priority.

The strong move toward distributed analysis systems for the current generation experiments (CDF/D0/Babar) and requirements for LHC, means the system scope now extends beyond a single lab environment. We must participate in systems development for Grids. We must articulate our requirements and provide interfaces from local infrastructure/policy to a common framework.

Dane and Matt