



**Summary Report of 3rd APRU IT Video Conference Session
on IT Security
Hosted by University of Southern California
February 9, 2010 (6 p.m. Los Angeles time)**

The 3rd APRU IT Video Conference Session on IT Security was hosted by University of Southern California on February 9, 2010. 16 APRU universities participated in the session.

Case studies on models, policy, access and privacy of information, security challenges and current solutions were presented by University of Southern California and National Autonomous University of Mexico. Participants included CIOs, IT managers in information services and network security experts.

University of Southern California asked what model would be best for higher education IT security. Threats and security issues were listed together with consequences of keyloggers and information stealers, and solutions to meet these challenges. Frauds involving electronic transfers of huge amounts of money from school district accounts, phishing and computer information theft in order to alter student grades. While solutions were proposed, the efficiency and functionality of deploying these solutions were evaluated.

National Autonomous University of Mexico (UNAM) shared its IT security challenges, campus infrastructure and strategies to minimize risks in systemic failures, information leaks and fraudulent misuse. UNAM advocated the prevention of risks at faculty, staff and administrative level, improved monitoring and incidence response, and implementing best practices in security features.

General discussion points included:

- challenges in both restrictive and open policy for wireless usage and responsibilities at the unit level
- setting up committees to guide policies and involvement of senior administration and faculty
- how security can sustain management styles of member universities aligned to each campus' strategic plan
- bottom-up vs. top-down approaches towards a network security culture, while preserving autonomy amidst governance parameters
- evaluation of security standards at senior administrator level
- identifying cultures, users and institution size when customizing security to work for individual campuses
- role of CIOs in advising various campus community sectors to buy into policies and central perspectives rather than technical preaching

- sharing of best practices in policy-making and information security measures
- resource management and allocation to reduce risks, creation of IT security awareness at various levels including engagement with other institutions and government organizations, user awareness through education and task force groups to develop collaborative approaches to security
- conducting security audits and benchmarking with external security standards
- security health checks to be encouraged but are not mandatory

List of participating member universities:

- Australian National University
- California Institute of Technology
- Chulalongkorn University
- Kyoto University
- National Autonomous University of Mexico
- National University of Singapore
- Peking University
- Tecnologico de Monterrey
- University of California, Davis
- University of Hong Kong
- University of Indonesia
- University of Malaya
- University of Oregon
- University of Southern California
- University of Sydney
- Zhejiang University