



# Meeting the CCC Information Security Challenge

Doug Cremer, Executive Director  
CCC Technology Center

# Challenges for Community Colleges

- Students – Peer-to-peer (P2P), Social Networking
- Academic Faculty – Open Access to Information, Academic Freedom, Strong Sense of a Right to Privacy
- Administrative Staff – Access to Critical Data, Regulatory Compliance Issues, Rapidly Evolving Standards of Expectation



# Community College Constraints

---

- Autonomy
- IT and Security Staff
- IT and Security Budget

# SAC Committee

- Under the Direction of TTAC, the System-wide Architecture Committee (SAC), in collaboration with FCCC and CCCCCO, initiated:
  - AT&T/HP External Vulnerability Scans (33)
  - McAfee Internal Scans (23)
  - PlanNet Assessment of AT&T/HP “Scrubbed” Findings
  - SAC then reviewed findings and solutions, recommended a range of security technology solutions, and then worked with the FCCC to develop preferred pricing for colleges



# Opportunities to Improve Security Posture

- Information Security Leadership
- College Information Security Strategy
- Perform Risk Analysis – Then Act to Improve
- Develop/Publish Security Policy or Executive Mandates
- Publish Operational Security Procedures
- Security Awareness Program

# Areas to Improve Security Posture

- Controls and Safeguards based on Risk
- Automatic Vulnerability/Patch Management
- Implement “Early Warning Systems”
- Incident Response Process
- Ability to Perform Self-Assessment
- PlanNet-developed “Road Map” addressing relative priority and timeframe

# PlanNet Findings – Top Vulnerabilities

- Use of “clear text” access methods. Consider using Telnet and HTTP with SSH or HTTPS
- Unnecessarily-open application service ports. Consider shutting down unneeded applications and blocking network access to the ports by utilizing and Access Control List (ACL)

# PlanNet Findings – Top Vulnerabilities

- Using expired or invalidated SSL Certificates. Recommendation is to consider an automated certificate enrollment system or service
- ICMP - a network diagnostic protocol - is allowed and can be used to perform a reconnaissance attack to learn more about the campus' network and hosts. Campus should consider blocking ICMP or filtering certain ICMP message types such as ICMP timestamps



# Security Quick-Start Guides

- Developing Information Security Leaders
- Security Policy Development
- Information Risk Assessment
- Vulnerability Management
- Security Awareness Program for Users
- Developing and Incident Response Capacity

# Security Quick-Start Guides

- Developing “Self Assessment” and Compliance Checking Capabilities
- Developing Information Security Architecture Model
- Selecting the Right Safeguards (Technology Acquisition Techniques)
- Developing an “Early Warning System”

# Information Security Web Presence on CISOA Website ([www.cisoa.org](http://www.cisoa.org))

- Policy and Procedure examples solicited from CISOA Membership via CISOA List Serve have been reviewed and then posted in the members-only area of CISOA Website
- Quick-Start Guides have been added to the members-only area of the CISOA Website.
- Quick-Start Guides are being aggregated into a single Information Security Document for community colleges

# Contact Information

- Doug Cremer

[cremerdo@cccnex.net](mailto:cremerdo@cccnex.net) 530-518-9784

- Catherine McKenzie

[cmckenzi@cccco.edu](mailto:cmckenzi@cccco.edu) 916-322-0833

- Cassidy Smith

[csmith@plannet.net](mailto:csmith@plannet.net) 714-982-5840



California Community Colleges

--

Meeting the Information Security  
Challenge

Questions?