Shared Responsibility of Cyber Solutions and Security

October 14, 2010

Dr. Vic Maconachy, VP for Academic Affairs and CAO
wvmaconachy@capitol-college.edu
Focus Point

• Cyber awareness campaigns and the development of public/private partnerships for effective cybersecurity messaging
• Some of our best lessons in life are not taught to us, but learned with guidance.
• I’d like to go back, but Bell Labs is now owned by Alcatel – a French company.
We are not in Kansas anymore!
It is NOT about Partnerships

- **Partnership = ROI**
  - It is comfortable
  - It often has determined end points
  - It is articulated

- **Relationship = Commitment**
  - Less defined
  - Deeper commitment
  - Goes the distance
  - More than $
It takes a village

- Government, Industry, Academia
The education issue is bigger than just IA

• The World Economic Forum ranks the United States 48th in quality of mathematics and science education.
• In 2000 the number of foreign students studying the physical sciences and engineering in the United States graduate schools for the first time surpasses the number of U.S. Residents.
• 69% of the United States public school students in fifth through eighth grades are taught mathematics by a teacher without a degree or certificate in math.
• 93% of U.S. public school students in fifth through eighth grade are taught the physical sciences by a teacher without a degree or certificate in the physical sciences.
• The U.S. ranks 27th among developed nations in the proportion of college students receiving undergraduate degrees in science or engineering.
• The U.S. ranks 20th in high school completion rate among industrialized nations and 16th in college completion rate.

Rising Above the Gathering Storm, Revisited: Rapidly Approaching Category 5. National Academy of Sciences
Do you recognize this landmark?

- The reactor building of Iran’s nuclear power plant, pictures here on August 20, is located about 750 miles south of Tehran.
“Iran Fights Malware Attacking Computers”
– By David E. Sanger
– Published September 25, 2010

- Stuxnet, which was first publicly identified several months ago, is aimed solely at industrial equipment made by Siemens that controls oil pipelines, electric utilities, nuclear facilities and other large industrial sites. While it is not clear that Iran was the main target — the infection has also been reported in Indonesia, Pakistan, India and elsewhere — a disproportionate number of computers inside Iran appear to have been struck, according to reports by computer security monitors.

- “Stuxnet has ability to “fingerprint” the computer system it infiltrates to determine whether it is the precise machine the attack-ware is looking to destroy. If not, it leaves the industrial computer alone.” (Christian Science Monitor)
The “Message”

- Until we, as a nation, recognize the current and future cybersecurity workforce as a VULNERABILITY, we will not respond with the sense of urgency our times require.
Follow Up

• Points of Contact
• Slides
• Websites

– For copies of slides, and links to references, pick up a reference card at the Capitol College display booth.