

Remarks to CISSE Colloquium on the Importance of Information Assurance Education to
Colleges and Universities

Michael T. Wood
President

Capitol College
Laurel, Maryland

June 7, 2006

When Vic asked me to make these remarks to you, and represent the many excellent higher-education leaders in pressing the case for information-assurance education, I did not hesitate to agree. Vic is a consummate motivator. I was also an easy mark, since I come from a tradition of serving two small colleges invested in helping Vic, and his colleagues, to achieve the IA-education mission. I led the academic affairs of Walsh College, one of the second wave of NSA-designated Centers of Academic Excellence. Then, two years ago, I moved to Capitol College, one of the earlier-designated CAEs and now one to have been re-designated at the advanced level. Leadership in IA education has been a source of pride for me. I am proud of the curricula, the service and the leadership of IA through Jeff Recor and Nan Poullos at Walsh, and Dave Ward and Allan Berg and their many fine faculty at Capitol. My motives are multiple, and perhaps not pure. For, as a college president and American citizen, I approach the passion for educational excellence in this field from both altruistic and selfish interests. More on that later.

First, why the bother? Why *should* educational leaders think about IA? Why do I invest at least some mental energy in it? One reason is simply because the importance of the field of information assurance as an academic enterprise is huge and growing. Communications technology has advanced astronomically. The threat of terrorism across the world will be with us for a very long time. I can think of nothing needing as much innovation and educational attention as information and infrastructure protection, except perhaps for technology and policy as they apply to human health care, and the globalization of human affairs as we relate to more developed China and India.

Information Assurance is of strategic national importance. It is a focus that will not be a fad. It is a discipline of emerging identity and maturity, with evolving sub-disciplines in prevention and control. At the same time, we must also realize that IA as an academic field is still new. We educators, and the NSA and DHS are actually defining an emerging and somewhat unknown field, even as world events force our attention to it. IA is not your grandfather's "engineering;" it's not even your father's "computer science." It represents a complex problem requiring quick, practical, and reliable solutions. IA is born of real-world exigencies, not just neat academic ideas.

As I consider IA, I am reminded of a book entitled “Thinking in the Future Tense,” by cultural anthropologist Jennifer James. We need to be thinking in the future tense, to meet current threats and to anticipate new ones, when we know not from where they will come or what human or technical clothes they will wear. Paradigms will come and go. The ubiquity of the Internet virtually guarantees greater reach and variety of communication. Advances in broadband, wireless-plus and whatever comes next as a communication conduit almost guarantee future excitement and challenge. Increases in consumer knowledge and global information are boons to future economic development, even as they can also be threats to national defense. On balance, even as we debate issues of “net neutrality,” immigration, and legislation like the Patriot Act, I believe that the constructive focus on critical infrastructure and cyber protection can be seen as a positive development for free markets, economic growth, and social and national well being.

So, if you’ll buy in with me to the notion that IA education is critically important to our country’s future, how can we in academe help to make it strong and useful? In at least five ways, I think. Allow me to briefly elaborate on each.

- Slide 1 here -

Teach The Right Stuff. This is trickier than it may seem to many of us. As a non-professional, I do not profess to know exactly what the right stuff is. I submit however, that it involves healthy flavors of both theory and practice, of new concepts and new techniques, and integration of many traditional and new scientific disciplines. Effective IA professionals will know the history and etiology of the field, the technical nature of how things work and might work, newest ways of thinking about the endeavor. They will be researchers of new problems. They will need toolkits of practical, hands-on solutions. They should be able to diagnose and understand an IA problem and to fix it, and better yet, prevent its arrival.

What I think I do know is that the right stuff has to be multidisciplinary. Designing and implementing secure information infrastructures require new mixes of disciplines and faculties working closely together. Assuring information means gathering, storing and distributing it technically well. It also means managing it and understanding its place and uses in the broader social context. Among the many disciplines relevant and important to this new field are: computer science; informatics; mathematics; economics; management and organization; research and policy, and engineering and many of its specialties. Both the traditionally “hard” sciences of technology and the “softer” sciences of management and leadership are essential. It might even be argued that the broader and more truculent aspect of the IA problem is that of properly managing information, its proper collection and dissemination. At the same time, as more innovative communications technologies evolve, vulnerability understanding and technical solutions will be crucial to our safety.

I know that many of you already recognize this and are moving your academic programs to meet these needs and expectations, as the NSA CAEs program demonstrates. As an example, at Capitol, we have redesigned our information assurance degree into two

tracks, one for the more technically oriented professional, and one for the more managerially responsible organization member (And, of course, with overlap in foundation coursework, two integrated degrees can be had for less than the price of two taken separately). Similarly, in our thinking about our new Business and Technology Leadership Institute, we will be blending what we already have in our Critical Infrastructure and Cyber Protection Center, with new centers in Entrepreneurship and Informatics.

-Slide 2 here-

Secondly, we can Grow Our Country's IA Capabilities. Especially as CAEs, we can take the lead to further develop the field, the outreach, and our leadership capabilities. Growing our capabilities means developing more teaching, research and technical-assistance capabilities among more people to serve increasing needs in federal and local governments and in business and industry. Only a few years ago there were no CAEs. On May 11, 1999, the first seven were established. One year later, the total jumped to 14. Now there are over 70. The growth rate has been not much short of phenomenal. Yet, as Vic would be the first to propound, 70 is still not enough to meet the challenge. We can educate and train more scientists, technicians and leaders. We can expand our degree and professional-development offerings from associate degrees through doctorates, both research-based and practitioner doctoral degrees. We can help more people become professionally certified through programs like the CISSP and SSCP. And, we can leverage education and training. Some of us are training people for certification exams and letting that certification also count toward an appropriate degree.

We can also expand our capabilities by involving those who sponsor and accredit us, so that the mantra of excellence in IA established by the NSA and DHS can be extended to the broader, peer-accredited, higher-education community. If the regional accrediting agencies, and those specialized accreditation organizations for fields like engineering and business recognize the identity and vitality of IA education, more colleges and universities might be energized to develop strong IA education programs.

There are places for schools of all sorts in the IA crusade. Small colleges can accentuate IA without having it buried under the program banners of larger, more traditional disciplines or schools; larger universities can emphasize more seminal theory-building and confirmation research; practical schools can build strong programs of technical assistance to government and industry. And, size doesn't really matter that much, if the spirit and drive to support IA exists. Key faculty and institutional leaders can give IA the visibility it needs and warrants.

-Slide 3 here-

Our third opportunity for strengthening IA education is to Form Alliances to strengthen and broaden curricula and service delivery. In Maryland, we have an active, working alliance of the CAEs, in which the respective program directors and faculties work together on issues of importance to the state and the federal agencies. In their endeavors,

the members of the alliance can carve out areas of work unique to their missions and capabilities so as to broaden the base and make the product richer, rather than competing.

Another regional alliance has recently begun with support from the National Science Foundation. CyberWATCH, led by our friends Ron Williams and Vera Zdravkovich at Prince George's Community College is bringing universities, community colleges, high schools and government leaders together to focus on developing future IA professionals.

Speaking of high schools, we can be reminded that interest and preparation for an IA career often begins in high school, or in middle school. It is in the formative educational phases that interests in STEM (Science, Technology, Engineering, and Mathematics) fields emerge, and foundations get built. We can work with those schools on programs of awareness, teacher training, and college bridge programs to ease the entry of young people into IA professions. At Capitol, for instance, we have specialized summer bridge programs of one to six weeks, where high school students learn fundamentals and acclimatize themselves to college. One program, called "NASA Prep," introduces young students to math, science, aerospace, and college life. Another called "Hispanic Awareness," brings young Hispanic students to campus to share and experience technical and scientific opportunities in college and the workforce. We might well think of IA education as a K-postgraduate phenomenon.

We might also consider outreach alliances to non-CAEs to solicit broader interest in the higher education community and to leverage the scarce resources of expertise and dollars that currently exist to support the educational mission. CAE-hood is very special. Still, it should not cocoon us. We should be the ones, who, through our professional affiliations, bring more colleges and universities into the fold. In our legitimate need to serve common yet often limited interests, our associations often miss opportunities to expand memberships to bring new light and bigger-picture solutions to our midst. We should better integrate the technical and the liberal arts schools, the public and the private schools, the not-for-profits and the for-profits. While our missions properly differ, it is our collective efforts that better America.

Finally, our alliances to get good things done must obviously include our government and corporate constituents. Whether they work with us to expand their workforce pipelines, or to perform projects, or to get specific training in skills required for their organizations, our success is ultimately measured in their success, and in that of their people.

-Slide 4 here-

That point leads to the fourth area where we can do more to further information assurance. We can implement activity-driven Information Assurance Centers on our campuses, like the IAC at Walsh College, the IAC at the West Chester University of Pennsylvania, and the new Critical Infrastructures and Cyber Protection Center at Capitol College. In those organization and business entities, we can distribute training and technical-assistance resources to the public, with the rigor and force of our faculty and academic standing. The Centers can also be an integrating force for diverse disciplines

and faculties at the schools. Through such centers our faculties could train specific companies or industry groups, help more people prepare for certifications, and offer technical advice on IA programs, technologies and audits. They could also serve as clearinghouses and disseminators of information, best practices, and new developments and threats on the IA front. These services might be especially helpful to groups of smaller organizations that might not have the awareness or internal capabilities to launch or monitor IA internally themselves. In addition to serving the public interest, such Centers could also benefit both the reputations and finances of our institutions – remember my “self interest?”

-Slide 5 here-

The fifth and final suggestion I would like to share with you is that we can probably do more to Practice On Our Own Houses. Within just the past week, the information-security vulnerability of colleges was highlighted in a news report on WTOP Washington radio, and Sacred Heart University’s computer system was hacked to the tune of risking information compromise for about 135,000 people. In the CNET article describing the Sacred Heart event (news.com.com/2100-7349_3-6077212.html, May 25, 2006), it was stated “Universities are easy pickings for data thieves, or so it seems to critics. Dozens of schools have suffered electronic intrusions during the past two years...” The affected schools include some fairly big names, like Ohio University, Notre Dame, and the University of Southern California. None of us are immune. And, we are juicy targets for a lot of information about a lot of people.

It is not that we do not recognize these vulnerabilities. Indeed, in almost any issue of Campus Technology, or Educause, you can read about the information-security imperative and the roles that Chief Technology, Academic and Executive Officers must play in the pursuit of defending personally sensitive information. And since, after all, we are the places where people get taught to protect information, one might think we should be good at the protection game. We are turning out the very professionals of the future who will be protecting information. Why not put them to work for us?

Two circumstances, I think, may have limited the extent to which we have been less than comfortable performing this surgery on ourselves. One is the rich tradition of academic freedom, which requires a degree of openness unlike national security and proprietary corporate interests. The other limiting factor is a matter more common to many other enterprises, the aversion to risk. Future doctors need to practice on cadavers. Future IA professionals need to practice on “living” IT systems. But simply put, letting our people, whom we educate to be good, hack away at us, represents perceived risk to many university leaders. I am reminded of a fellow college administrative officer (whom I admire and respect, by the way) who would ask me if I knew that our IA students and faculty were “practicing” by hacking the college’s system. The question, of course, implied that they should not be doing so. The rejoinder is that the students must be capable of fixing it after they (or real villains) break it.

That little story from yesteryear suggests that to be able to practice more on our own houses, we need to enter the world of another big T word that is not Technology. Technology can help protect separations between operating and practice systems. And, while we try to better protect the Internet, we can use it more widely to educate more people online who might not be present on our campuses. Since we invest so heavily in technologies to enable the learning process, we might invest as intensively in systems to safeguard our information. We may also need to better *trust* (that other T word) IA faculty and students to do things right and protect the institution. We should involve the CTO actively in the education process. And, we can better trust ourselves to take the advice we so readily offer to others. At Capitol, we recently granted thesis credits to graduate students who worked on strengthening our own information systems' security.

I return to my initial questions – Why bother? Why us? – and to my initial premise that the answers are both altruistic and selfish. The altruistic call to serve the public interest, is pretty much up to us as individuals. Nonetheless, altruistic motives can be fostered, as can the intrinsic *values* of the way of life we cherish in a free society. In fact, I would submit that to avoid confronting the occasional conscience-jarring question – “are we educating the next Bin Laden?,” we need to complement the technical education of information protection, with value education about the philosophy, culture and society that we are protecting. We need to trust that we are educating for the greater common good, at the risk of helping an eventual enemy. And, we need to support the broader higher-education community. As colleagues, we can help new institutions to become CAEs. In so doing, we might also enhance public perception of higher education's value. We have a professional obligation to ourselves and to the nation to nurture CAEs.

The selfish interest lies in my assumption that IA education will make our colleges better -- richer in expertise, richer in financial resources, and richer in the eye of public accountability. There are tangible benefits to society and to our colleges from having IA programs. At Capitol College we have over 250 master degree candidates in IA. That, for us, is a pretty good number of paying, or tuition-reimbursed students. Our IACs can also bring us revenue from training and technical services. Our successful work for government agencies and companies can bring us broadened community support. It is in our interests to do this.

However, doing it won't happen magically by itself. Somebody needs to make it happen. And, we can. I'll close with a reference to another book, the popular bestseller “Freakonomics,” by the economist Steven Leavitt and his collaborator Stephen Dubner . In explaining why you shouldn't expect your realtor to get the marginal dollar for you, and why public school teachers and sumo wrestlers (among others) cheat, Leavitt concludes that “it's all about incentives.” People do what they are incentivized to do, what the system supports, what rewards or sustains them. That's a pleasing realization. Because you and I -- presidents, provosts, deans, and chairs -- have access to incentives for our people. Whether it's in the budgets we provide or the words of organizational support we convey, we provide the leadership and incentives for what we want to see done. So, we can choose what programs, activities, or constituents to serve.

I think information assurance education is a most worthy focus for our support, and I hope you all do too. And, if you are here without your leaders who control the incentives, take this message back to them. Together we can promote CISSE among our own and other colleges and universities. We can provide financial and motivational support. We can champion the laudable cause and make good things happen.

Thank you.