OREGON CYBER SECURITY

Prepared expert testimony by:
Greg Hutchins, PE
Stan Smith
Quality Plus Engineering
To: House Committee on Information Management and Technology

Who is Quality Plus Engineering?

Background:

Portland Oregon based Engineering company

- 800.COMPETE or gregh@QualityPlusEngineering.com

Greg Hutchins's background

- Reed/PSU engineering graduate
- Author of 12 books, including ISO 9000 (8 languages), Standard Manual of Quality Auditing, Value Added Auditing
- Oregonian bylined columnist (Hutchins 'On Jobs')
- Conduct technical, forensic, process, operational, cyber, and other operational assessments
- International authority on technology transfer and engineering work
- Author of more than 300 articles on assurance and technology

Partial Client List:

- Federal Aviation Administration (FAA)
- Bonneville Power Administration (BPA)
- Port of Seattle
- Coca Cola
- MI SWACO
- Freightliner
- First Data Corporation
- Microsoft
- Institute of Electrical and Electronic Engineers
- American Institute of Certified Public Accountants
- Boeing

Testimony Objectives

- Thank you for the opportunity to provide expert testimony on this critical Homeland security issue
- Provide context on cyber threats and solutions
- Testimony Objectives:
  - Present context of US at war
  - Identify US homeland security challenges
  - Impart ‘lessons learned’ of cyber security
  - Describe changing threshold of ‘due care’ and ‘due diligence’
  - Lesson Learned: We need to protect ourselves with the best capabilities we have in the state.

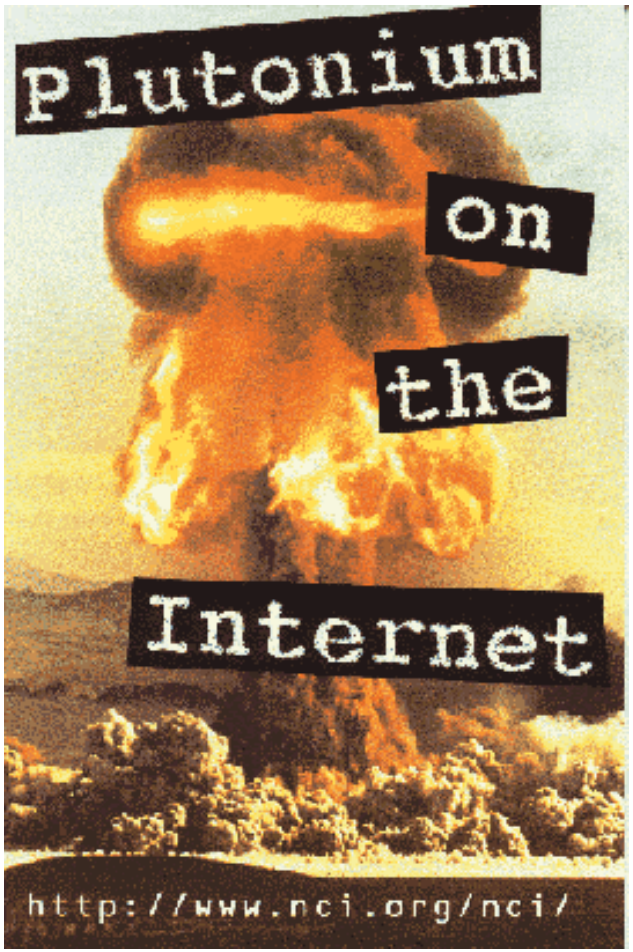
‘America at War’
Homeland Security

- Communication networks
- Data networks/Internet
- Water supplies
- Food sources
- Ports & shoreline protection
- Energy grids and fuel pipelines
- High density population areas
- Transportation networks
- Air space

Cyber Attack? Not If … When?

"I do think cyber warfare is a very real possibility. Cyber terrorism is, too . But for both cases, cyber war or cyber terrorism, the activity of the terrorist or the war makers is really part of a broader plan. They're really trying to use a computer attack as a way to augment or strengthen their primary attack."

John Hamre – Deputy Secretary of Defense, 1997 –1999.



Frontline; April 24, 2003.

“Digital Pearl Harbor?”

“In 2010, information security will be much better than it is today. But between then and now, everything will get inconceivably worse.”

CIO Magazine, December 15, 2003

What's at Stake for Oregon?

The public safety logic goes like this:

Higher consequences of event **=>**

Higher overall risks **=>**

Higher security controls required **=>**

Higher standard of 'due care', 'due diligence,' and 'proficiency' are required

Higher Standard of 'Due Care' in Cyber Security

Pre 9/11

Compliance with laws

Conformance with policies, procedures, etc

Reasonableness

Acceptable level of risk

Due care

Due diligence

Post 9/11

Demonstrate compliance with intent/spirit of law

Demonstrate effectiveness/efficiency

Higher standard of due care and due diligence

Risk management

Emphasis on proactivity, prevention, prediction and even preemption

So, What Does Higher 'Due Care' Mean?

- Due care standard and requirements increased since 9/11 linked with terrorism, ie. nuclear, bio, cyber, etc.
- Specialists with technical degrees and many years of robust (deep/broad) experience in the specialty

Changing Nature of Due Care'

- **Due care** is "the care that a reasonable person would exercise under the circumstances; the standard for determining legal duty".
- **Due diligence** is "the effort a party makes to avoid harm to another party".
- **Conclusion:** Professionals assessing technical homeland security issues are held to a higher standard of 'due care.'

Does CPA License Meet Higher Standard of 'Due Care'?

- See attached opinion-editorial
- **Question:**
  - Does CPA meet the 'necessary and sufficient' threshold to conduct cyber security, bio terrorism, and other technology/scientific assessments?
- **No.** They can assess and attest to financial controls. They shouldn't assess controls outside their professional purview.
- **Reason:** Consequences of poor/lack of judgment are catastrophic!!!
- **Making the case**

Professional Proficiency of Accountants and Engineers

Oregon Certified Public Accountants

- Degree from accredited program
- CPA exam
- 1 year experience
- Approved to practice
- Years of experience to attest in vertical industry sector for Big 4[1]

1. Source: Oregon Board of Accountancy. 2005.

Oregon Professional Engineers

- Degree from accredited program
- Fundamentals in Engineering exam
- 4 years of professional experience
- Professional engineer exam
- Years of professional experience in computer science, software, etc.[2]

2. Source: Oregon Board of Engineering and Land Survev. 2005.

Certified Information Systems Auditor™ (CISA) Requirements

- Passing multiple-choice test
  - Minimum 5 years experience of IS audit, control, or security
- Substitutions:
  - 1 year experience met with 1 year of audit/IS experience or associate degree
  - 2 years experience met with BA/BS degree
  - 1 year auditing experience with 2 years teaching audit/control/security
- So what does this mean?
  - CISA = Person with Accounting BA with one year experience as auditor (not in IT) and 2 years teaching experience in audit/etc.
  - IT courses and computer knowledge classes are not part of the Oregon Board of Accountancy Core Competencies or required courses
- **Question: Does this meet the higher 'due care' standard for cyber security post 9/11?**

“But, I Got My IT Certification!”

“Yes, but…”

Technology and Engineering Professional Challenge:

- Half life of knowledge!
- Definition: Amount of time knowledge doubles in a profession. Professionals need to keep up.
- All technical professions have the half life of knowledge: ie. medicine, computer science, and all engineering disciplines
- **Takeaway:** If a software engineer does not retread every two years, he/she is functional toast. In cyber security, this may be 18 months or less.

Summary:
Cyber Risk Solutions for Oregon

- East coast corridor (NY, Boston, DC) perceives ‘US is at War!’
- Homeland Security is THE critical public policy issue confronting US.
- Cyber Security is the backbone of homeland security. Computers carry sensitive information.
- What does it mean for state of Oregon?:
  - Determine cyber risk.
  - Develop appropriate levels of controls for cyber security.
  - Monitor risks, intervene, and correct deficiencies on daily basis.
  - Use appropriate professionals to conduct assessments and provide assurance.

Alarmist? Maybe! But, the Consequences of Failure …

"What we didn't have but obviously needed was an alarmist."