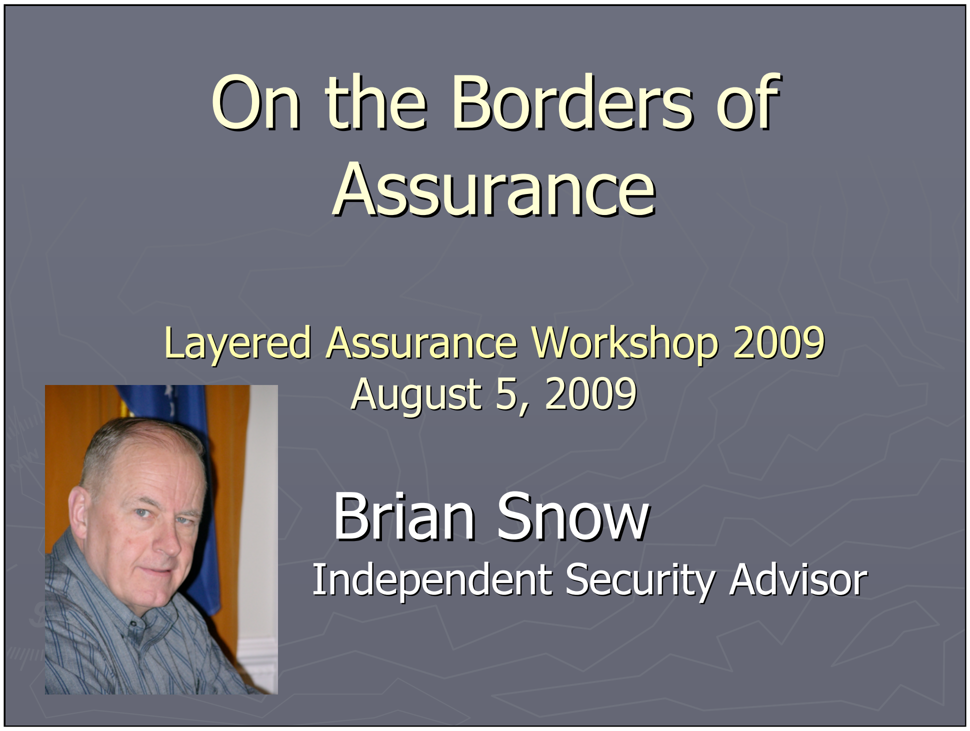


On the Borders of Assurance

Layered Assurance Workshop 2009
August 5, 2009

Brian Snow
Independent Security Advisor

Good afternoon! It is a pleasure to be here, if only by tele-presence.

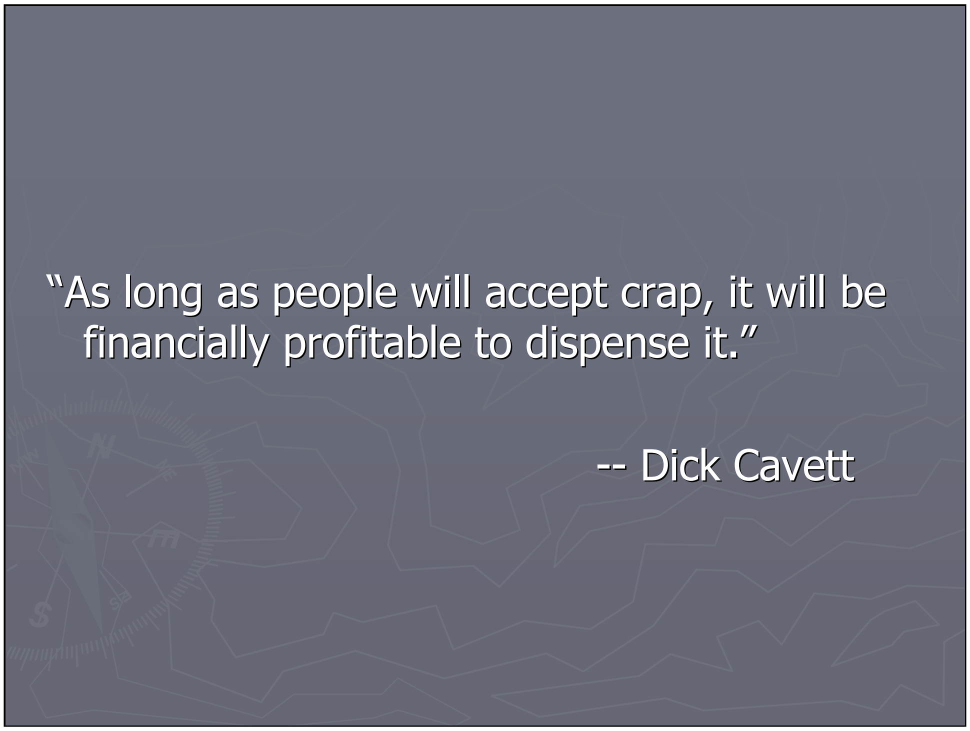
I've spoken often on the need for Assurance at other Conferences, but it was only one topic of many on their agendas. To address a workshop focused entirely on Assurance is refreshing indeed!

The other panelists have already given their talks in prior sessions, and I am sure you want to get quickly to the Question and Answer session; so I will be brief and discuss lightly only four topics that are not deep, but important for either the ADOPTION of Assurance processes by vendors and customers, or that address CURRENT GAPS in practice. These topics lie on the Borders of Assurance, if you will, not in the heart of assurance technologies.

But we do have to get users past the border before they will come on board and adopt such practices.

I'm sure most of us agree that getting customers to *adequately* address assurance is a hard sell; Dick Cavett gave one reason for this,

(next slide - 2)



“As long as people will accept crap, it will be financially profitable to dispense it.”

-- Dick Cavett

Or more politely translated, “Market Pressures are hard to overcome”…

But this only results in the following picture of a user’s stance when using un-assured products!

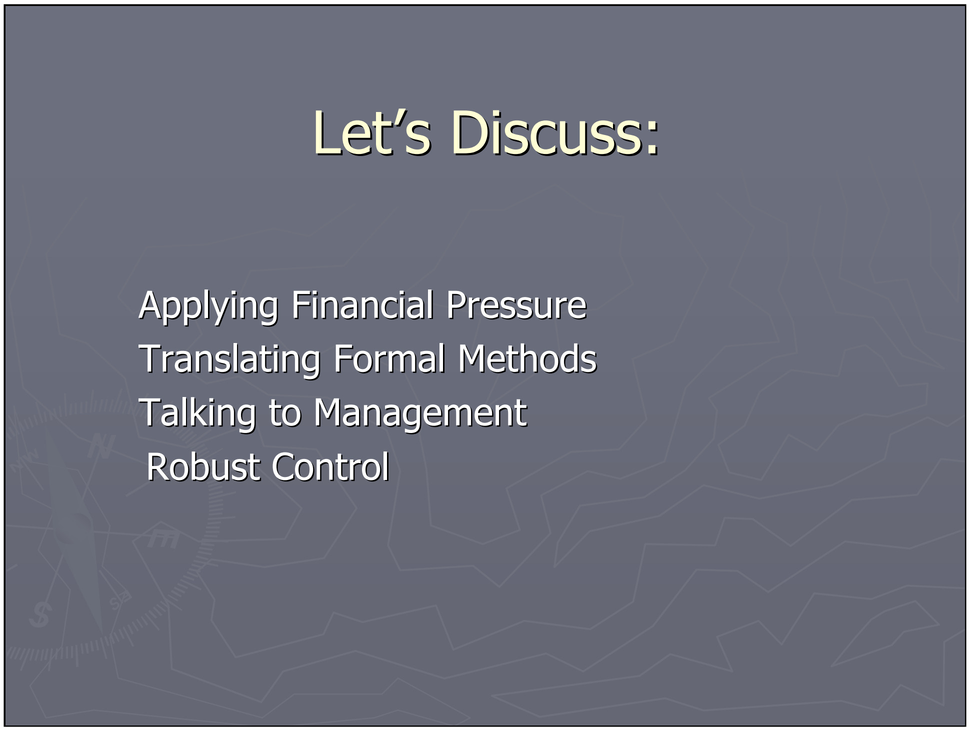
(next slide – 3)

Could we take a moment to review your risks?

It is clear that the fellow is not aware of the risks he is facing!

So how can we improve the situation, and get more assurance in sensitive products and processes?

(next slide - 4)



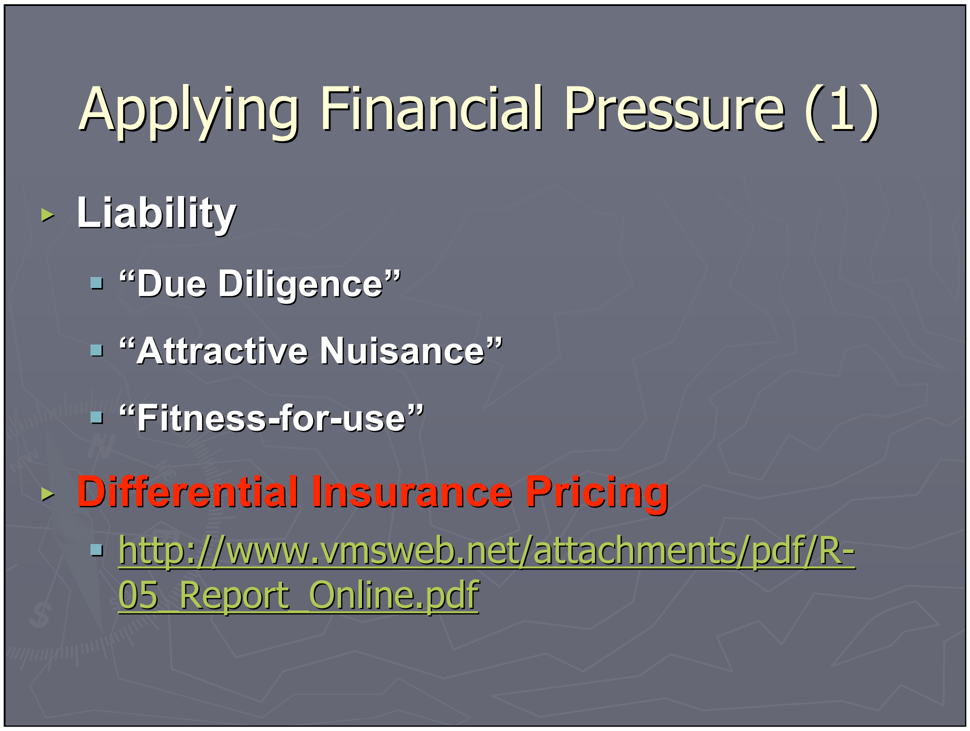
Let’s Discuss:

Applying Financial Pressure
Translating Formal Methods
Talking to Management
Robust Control

Specifically, let’s discuss these four topics:

Applying Financial Pressure	(Through law and Insurance Costs)
Translating Formal Methods	(speak English to customer),
Talking to Management, and	(Use Business terms, not geek-speak)
Robust Control.	(as well as robust primary functions)

(next slide - 5)



Applying Financial Pressure (1)

- Liability
  - “Due Diligence”
  - “Attractive Nuisance”
  - “Fitness-for-use”
- Differential Insurance Pricing
  - http://www.vmsweb.net/attachments/pdf/R-05_Report_Online.pdf

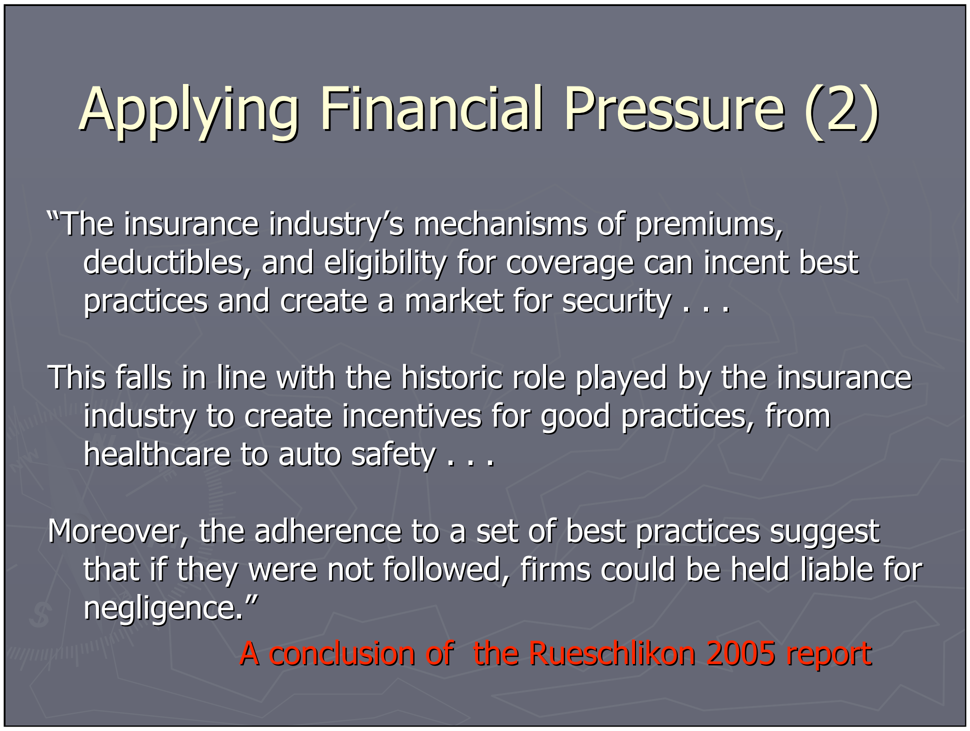
Applying Financial Pressure:

Liability can apply pressure to improve, but frequently only after-the-fact.

The sea of lawsuits for lack of due-diligence, for providing an attractive nuisance, or for not being fit-for-use give plenty of evidence for this.

But the last item, Differential Insurance Pricing, is interesting…

(next slide - 6)



Applying Financial Pressure (2)

"The insurance industry's mechanisms of premiums, deductibles, and eligibility for coverage can incent best practices and create a market for security . . .

This falls in line with the historic role played by the insurance industry to create incentives for good practices, from healthcare to auto safety . . .

Moreover, the adherence to a set of best practices suggest that if they were not followed, firms could be held liable for negligence."

A conclusion of the Rueschlikon 2005 report

One of the most promising recent occurrences in the insurance industry was stated in the report of Rueschlikon 2005 (a major conference serving the insurance industry). Many participants felt that,

"The insurance industry's mechanisms of premiums, deductibles, and eligibility for coverage can incent best practices and create a market for security . . . This falls in line with the historic role played by the insurance industry to create incentives for good practices, from healthcare to auto safety . . .

Moreover, the adherence to a set of best practices suggest that if they were not followed, firms could be held liable for negligence."

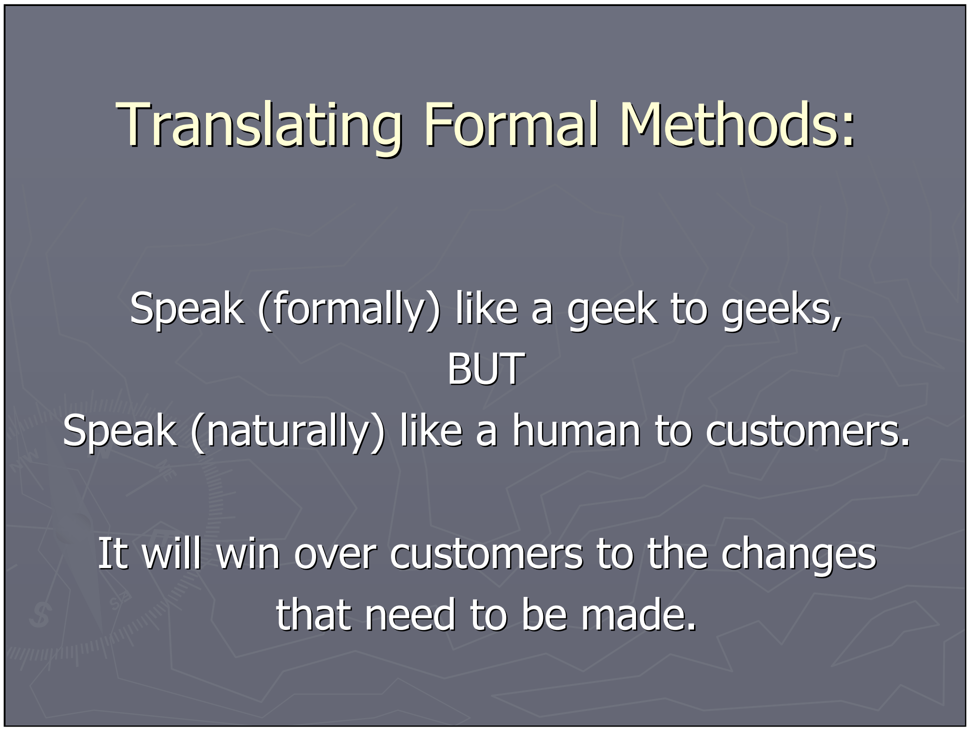
Bluntly, if your security product lacks sufficient robustness in the presence of malice, your customers will have to pay more in insurance costs to mitigate their risks.

How the insurance industry will measure best practices and measure compliance are still to be worked out, but I believe *differential* pricing of business disaster recovery insurance based in part on quality/assurance (especially of security components) is a great stride forward in bringing market pressure to bear in this area – and such differential pricing *is* under consideration.

I really believe the insurance industry can be, and is willing to be, a major player in rating the quality of assurance technologies and processes used in various products, and using those ratings to adjust insurance costs for using certain products. For those of you with contacts in the Insurance industry, please help keep up the pressure to move in this direction.

Insurance costs are a recurring expense for business, tracked by the CEO's and CFO's of major firms, and if some one-time expenditures in development can reduce this recurring cost, attention will be paid…

(next slide - 7)



Translating Formal Methods:

Speak (formally) like a geek to geeks,
BUT
Speak (naturally) like a human to customers.

It will win over customers to the changes
that need to be made.

I have long been a champion of formal methods in assurance work, even when it was expensive (starting from the 60's through the early 70's) but I will have to speak gently here, and seek comment from others on the panel in their turn, since I haven't delved deeply into the heart of the technologies for a couple of decades.

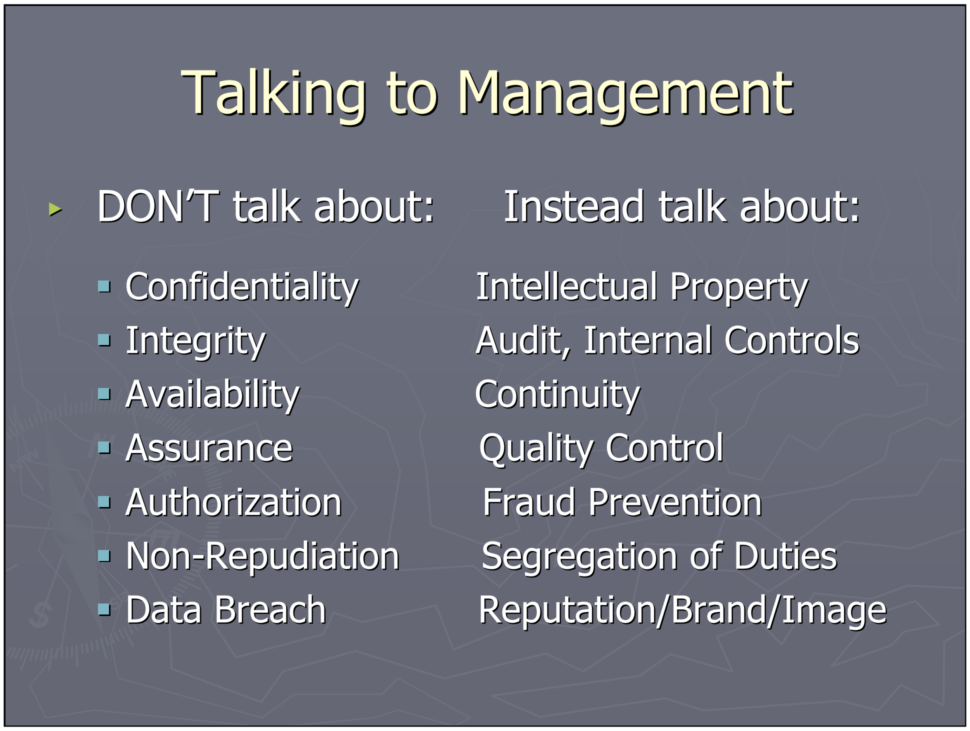
However, I would like to report an interesting experience from those early years in DoD.

We would get a specification from system engineers, which were flow charts with English phrases in the boxes (and some other materials). The formalists would translate the specification into a mathematical description, and use theorem provers and other tools to first show consistency -- and then that the result predicted by the formal model would actually match the expected outcome as stated by the engineers. Frequently the proffered specs were flawed, and corrections would be needed.

We learned not to wave equations in the customer's face; instead, we mapped the erroneous state back into English, and would talk with the client at that level. An "Aha" moment for the customer was usually quickly reached, and the suggested fixes would be applied. Formal methods could find flaws in specifications, but we still needed to convince the customer of the need for a change, and that required English.

Spending the time mapping back to English before talking with the customer seemed to save time, and avoided our bickering with the customer which frequently happened if we attempted to start with the equations. The equations found the problem, and could point to the solution. But the decision to change was a human one, and needed to be reached in human dialog.

(next slide - 8)



Talking to Management

DON'T talk about:	Instead talk about:
Confidentiality	Intellectual Property
Integrity	Audit, Internal Controls
Availability	Continuity
Assurance	Quality Control
Authorization	Fraud Prevention
Non-Repudiation	Segregation of Duties
Data Breach	Reputation/Brand/Image

On a related note, even when speaking in English, the choice of *which* particular words you use can be critical. So choose words carefully when **talking to management**:

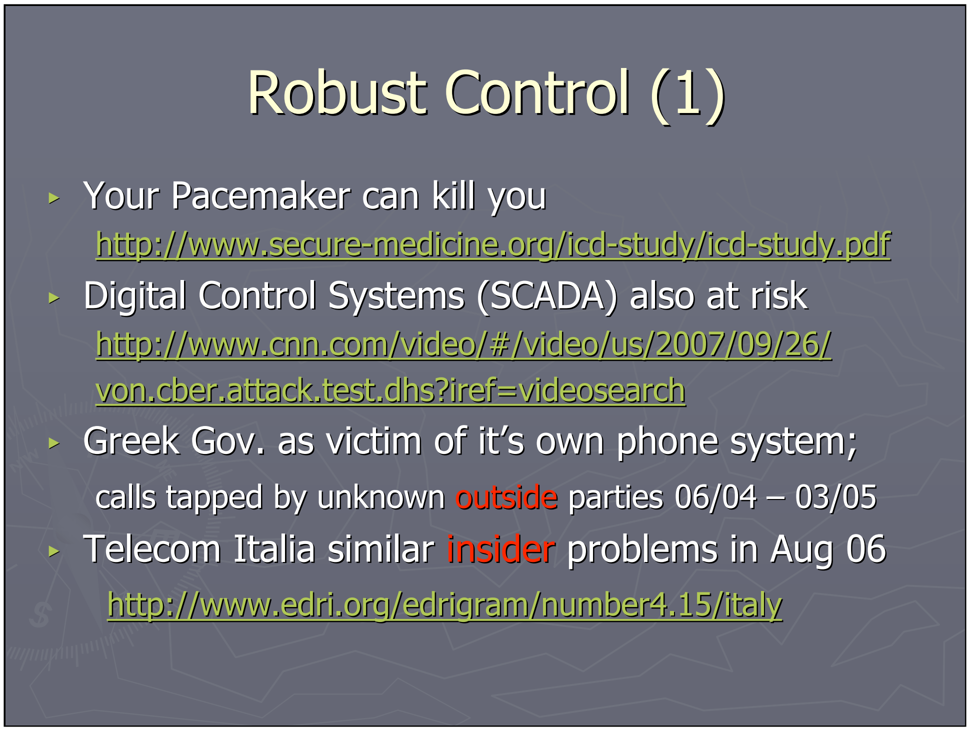
Security and Assurance need to be SOLD to managers and executives; use words that mean something to them when you brief them.

You can talk glibly about Confidentiality, Integrity, Availability, Assurance, Authorization, Non-Repudiation, Data Breech, DES, AES… and watch their eyes glaze over as they fidget in front of you.

Or you can use words and phrases like Intellectual Property, Audit, Internal Controls, Continuity, Quality Control, Fraud Prevention, Segregation of Duties, Reputation, Brand, Image… and engage them eagerly on their own turf, introducing your terms gradually as needed for nuance and clarification.

At least at the beginning of dialog, use words management understands to capture their attention and engage them. It will go easier after that…

(next slide - 9)



Robust Control (1)

- Your Pacemaker can kill you
  http://www.secure-medicine.org/icd-study/icd-study.pdf
- Digital Control Systems (SCADA) also at risk
  http://www.cnn.com/video/#/video/us/2007/09/26/ von.cber.attack.test.dhs?iref=videosearch
- Greek Gov. as victim of it's own phone system;
  calls tapped by unknown outside parties 06/04 – 03/05
- Telecom Italia similar insider problems in Aug 06
  http://www.edri.org/edrigram/number4.15/italy

Sensitive Sytems need Robust Control!

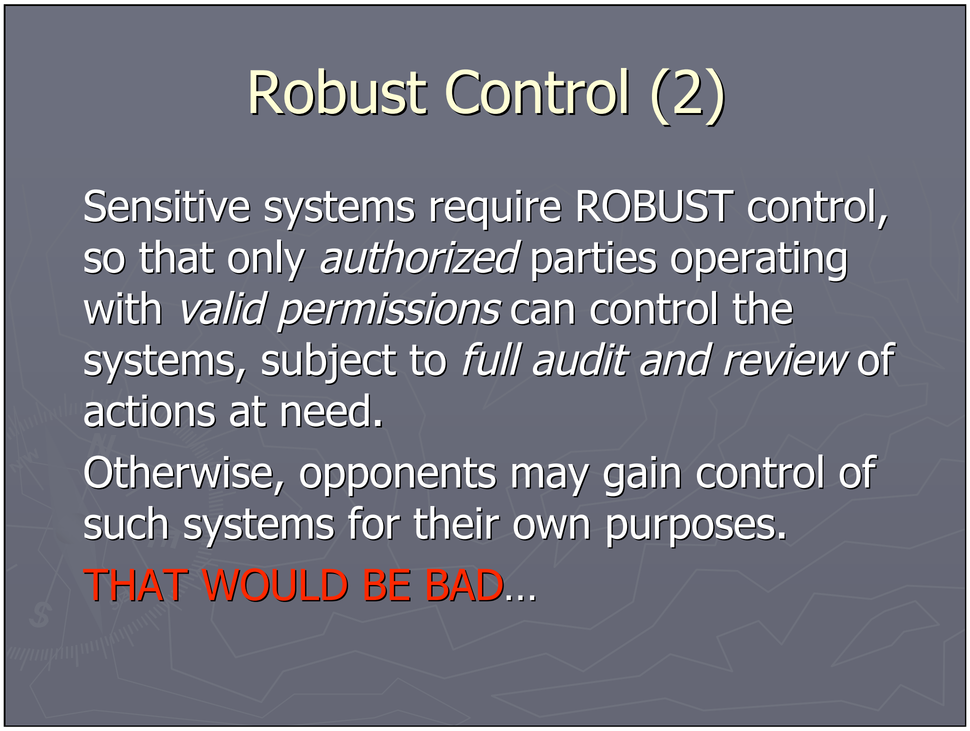
Medical devices, Army radios, Digital Control systems, Surveillance Systems, and other sensitive systems all require robust control, so that only authorized parties operating with valid permissions can control the systems, subject to full audit and review of actions at need.   This requires a mix of human processes and technology constraints! Otherwise, opponents may gain control of such systems for their own purposes.

Such attacks are not hypothetical! Let's look at specific examples.

Pacemakers with remote controls permitting monitoring by your doctor can kill you when controlled instead by an enemy! See: http://www.secure-medicine.org/icd-study/icd-study.pdf

DHS had the National Labs demonstrate an electric power generator's destruction via remote unsecured commands: see video at:

http://www.cnn.com/video/#/video/us/2007/09/26/von.cyber.attack.test.dhs?iref=videosearch



Robust Control (2)

Sensitive systems require ROBUST control, so that only *authorized* parties operating with *valid permissions* can control the systems, subject to *full audit and review* of actions at need.

Otherwise, opponents may gain control of such systems for their own purposes.

THAT WOULD BE BAD…

Repeating what I said earlier,

Sensitive systems require ROBUST control, so that only *authorized* parties operating with *valid permissions* can control the systems, subject to *full audit and review* of actions at need.

Otherwise, opponents may gain control of such systems for their own purposes.

(next slide - 11)

Could we take a moment to review your risks?

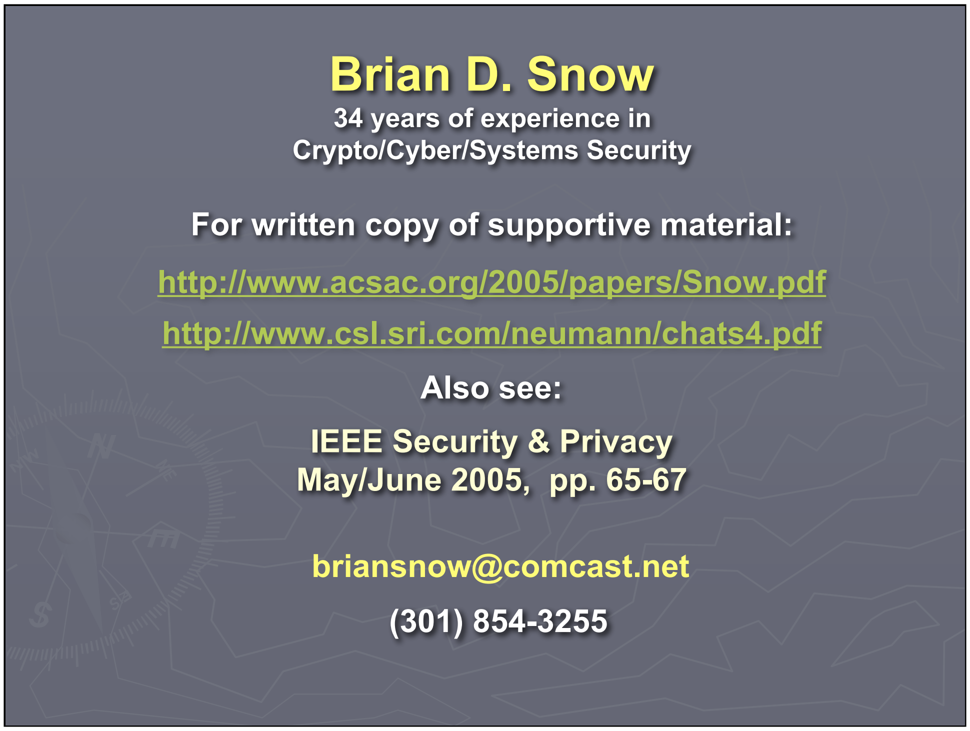
In summary,

If we can do any of these four things on the Borders of Assurance:

1. Get financial pressures appropriately aligned with research and development,
2. Translate results of Formal Methods to simple English for the customer,
3. Within English, use the right words when talking to management, and
4. Provide truly robust controls for sensitive systems,

Then we have a chance to get away from the situation shown in this picture and get to a better situation!

(next slide - 12)



Brian D. Snow

34 years of experience in
Crypto/Cyber/Systems Security

For written copy of supportive material:

http://www.acsac.org/2005/papers/Snow.pdf

http://www.csl.sri.com/neumann/chats4.pdf

Also see:

IEEE Security & Privacy
May/June 2005, pp. 65-67

briansnow@comcast.net

(301) 854-3255

Here’s contact data if you want it, and pointers to additional reading.

I’ve listed two of my papers on Assurance (7 and 4 pages long), and an excellent paper by Peter Neumann (236 pages of excellent detail) if you want to delve further.

This workshop has my permission to post these slides so you can easily click on the URLs, or read the notes pages for my spoken text.

Thank you for your attention, it has been a genuine pleasure speaking with you!

(KILL SCREEN)