LAW 2009
Government Need for Assurance
Panel Moderator’s Intro: Government / Vendor Partnership for Assurance

How can it work?

Rance J. DeLong

“Best Commercial Practice”

Consider the standard End User License Agreement (EULA) for software:

- *“Manufacturer warrants that the SOFTWARE will perform substantially in accordance with the accompanying written materials”*
- *“Manufacturer's entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet this Limited Warranty “*
- *“Manufacturer disclaims all other warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose”*

“Best Commercial Practice”

Example of a common EULA disclaimer :

> *“The SOFTWARE PRODUCT may contain support for programs written in JAVA. JAVA technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of JAVA technology could lead directly to death, personal injury, or severe physical or environmental damage.”*

Don’t product vendors find this embarrasing?

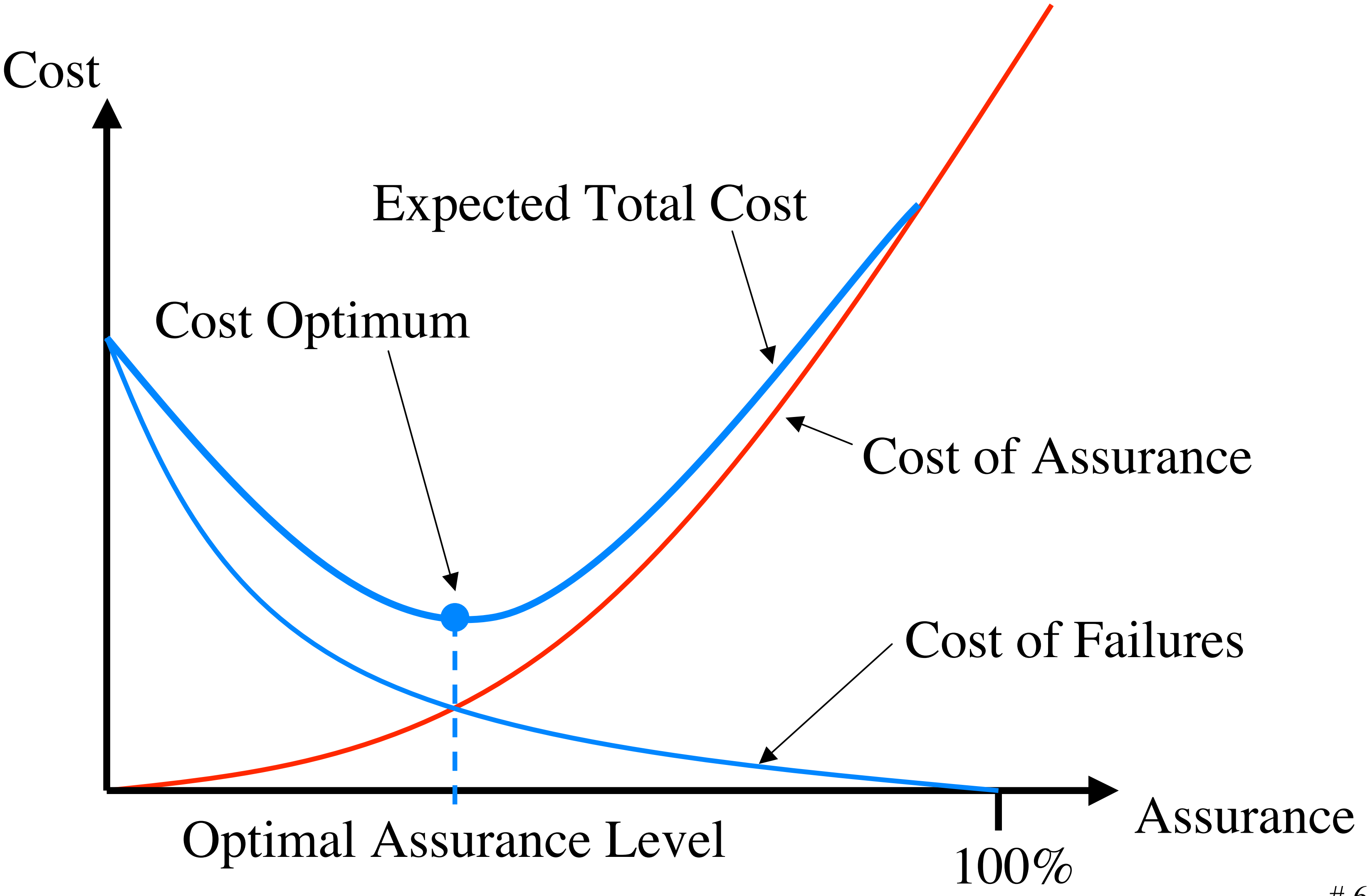
I do.

Why do vendors have to hide behind disclaimers?

What prevents us from improving our practices and producing dependable and assured systems?

The Assurance Cost Function

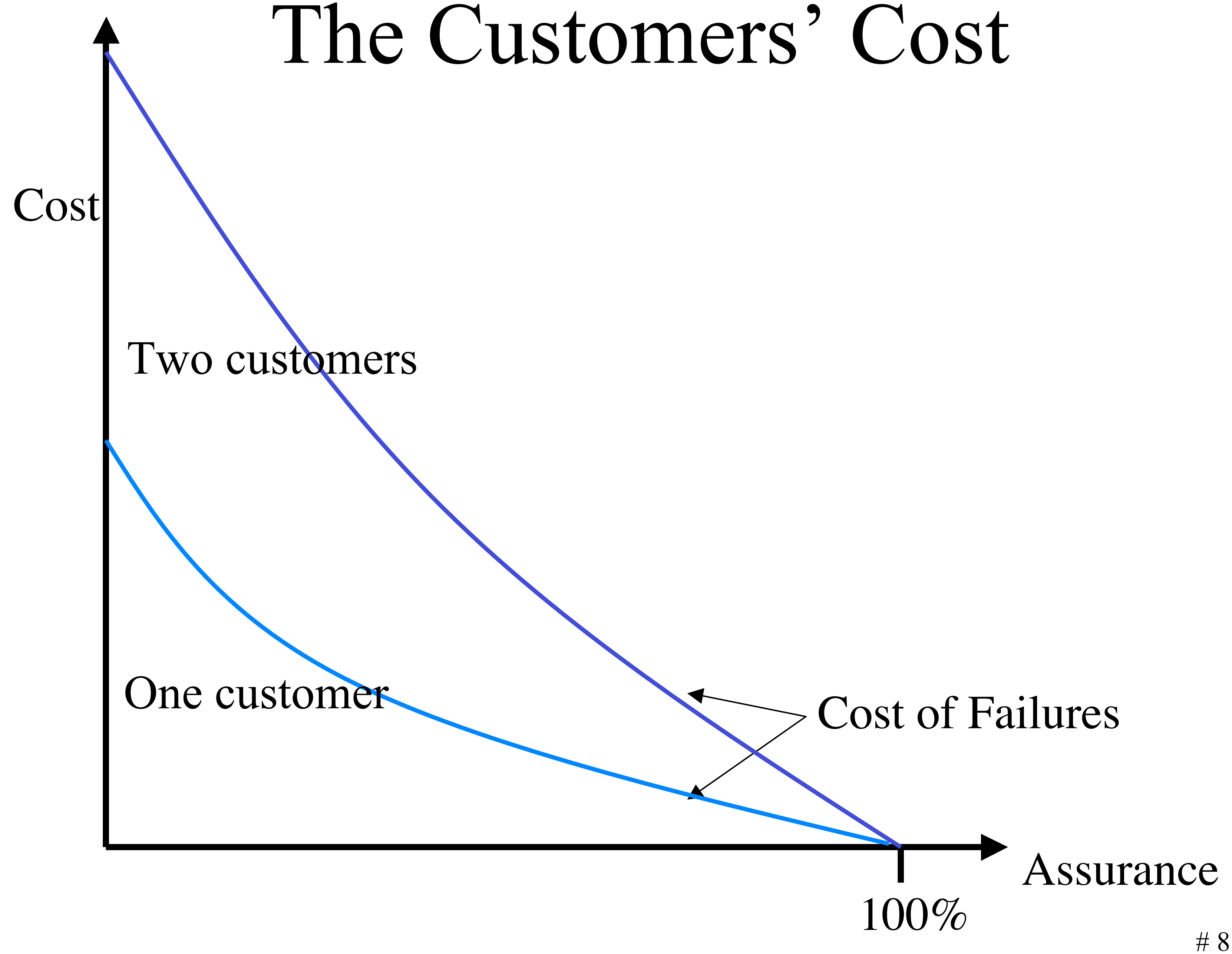
aka the “security cost function”



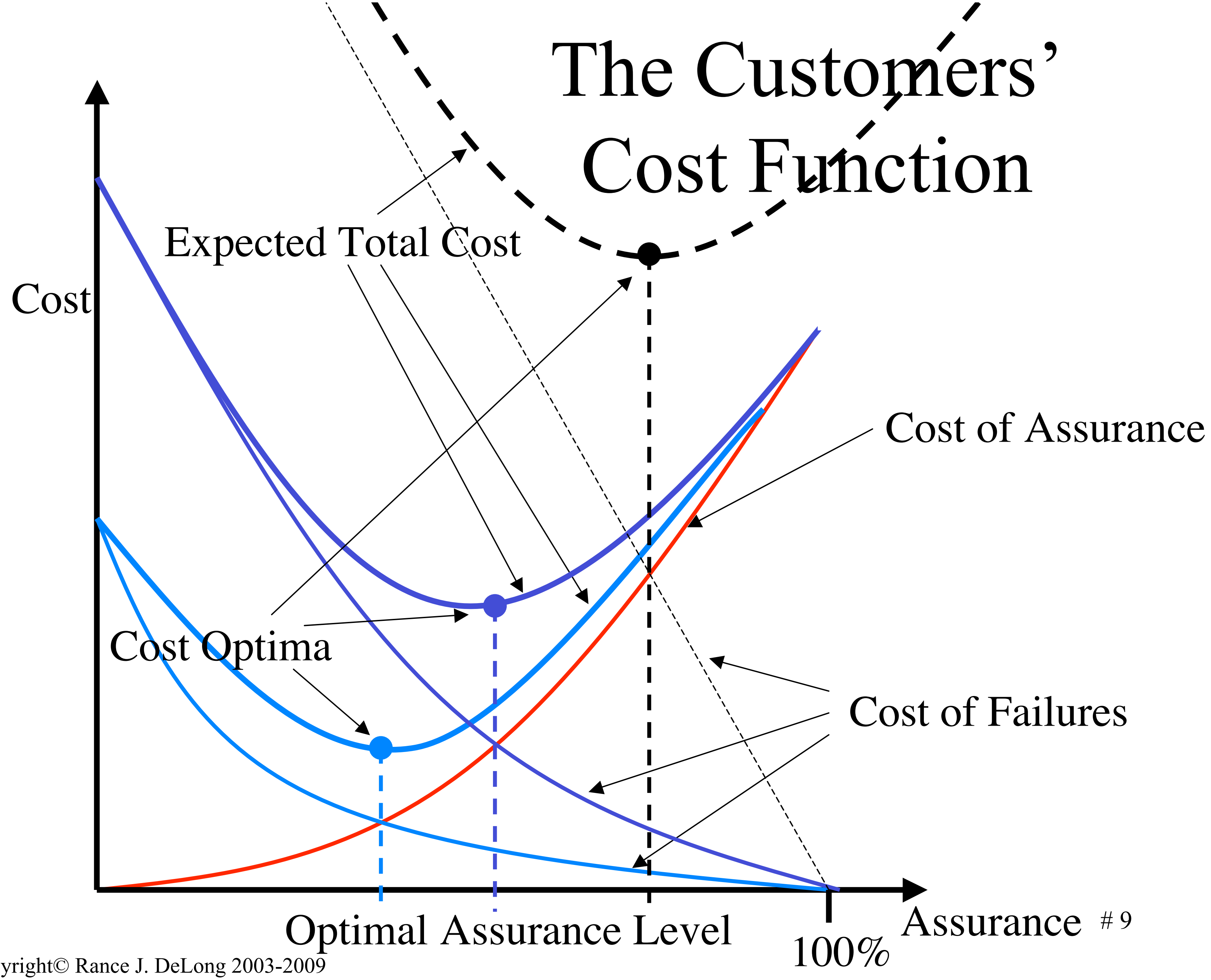
Seems simple enough … what's the problem?

- The model works ***within*** an organization
- Otherwise the costs are not coupled!
- Why do products not have better assurance?
- Product ***vendors*** pay the "Cost of Assurance"
- Product ***users*** pay the "Cost of Failures"

The Customers' Cost



The Customers' Cost Function



Why don’t customers ***demand*** better security?

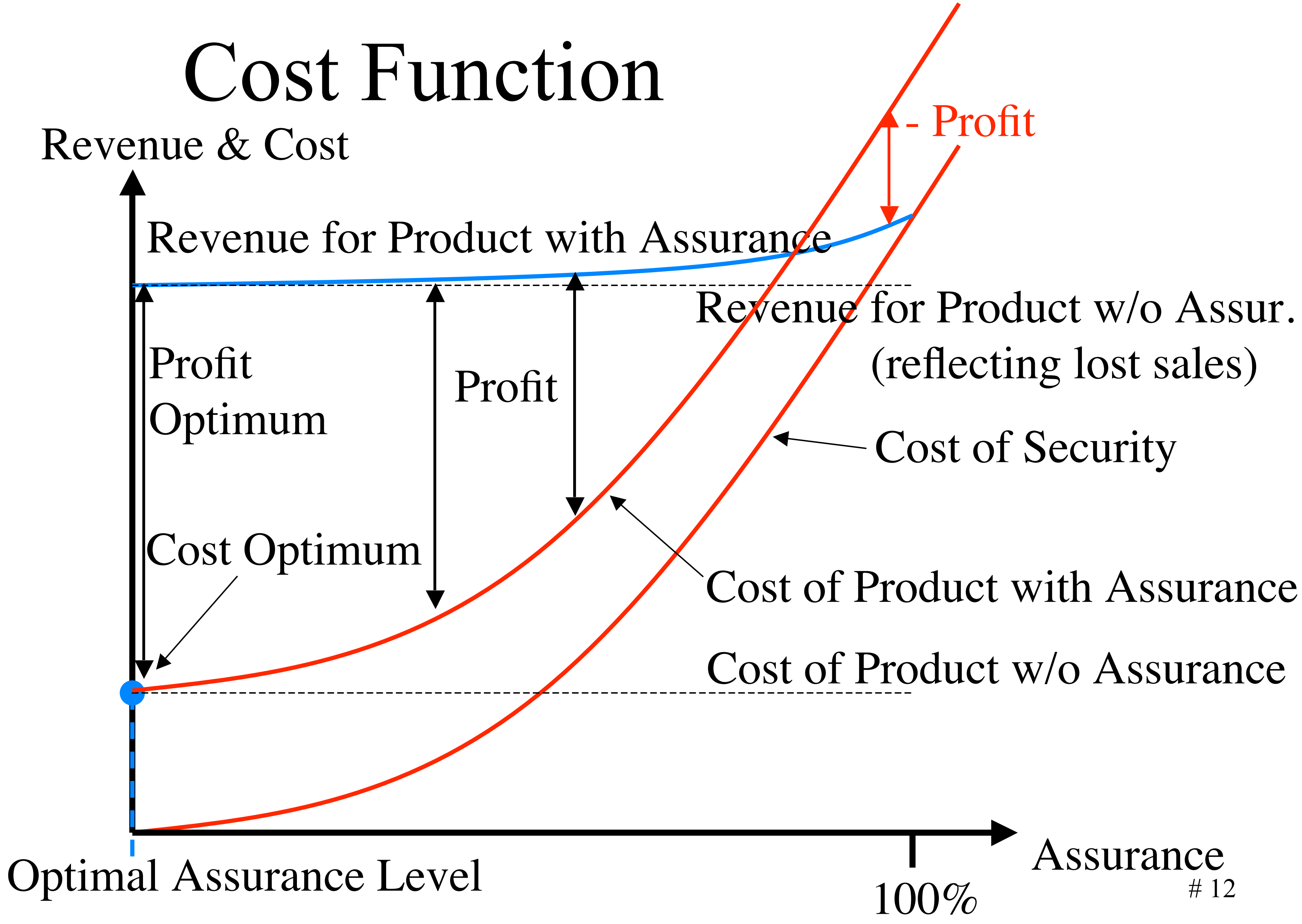
- They do:
  - In a wimpy, whiny, resigned kind of way
  - Not in a way that gets results

- The customers’ “pain” is ***distributed***
  - They don’t exercise collective bargaining power
  - It’s a case of divide and conquer (by the vendors)

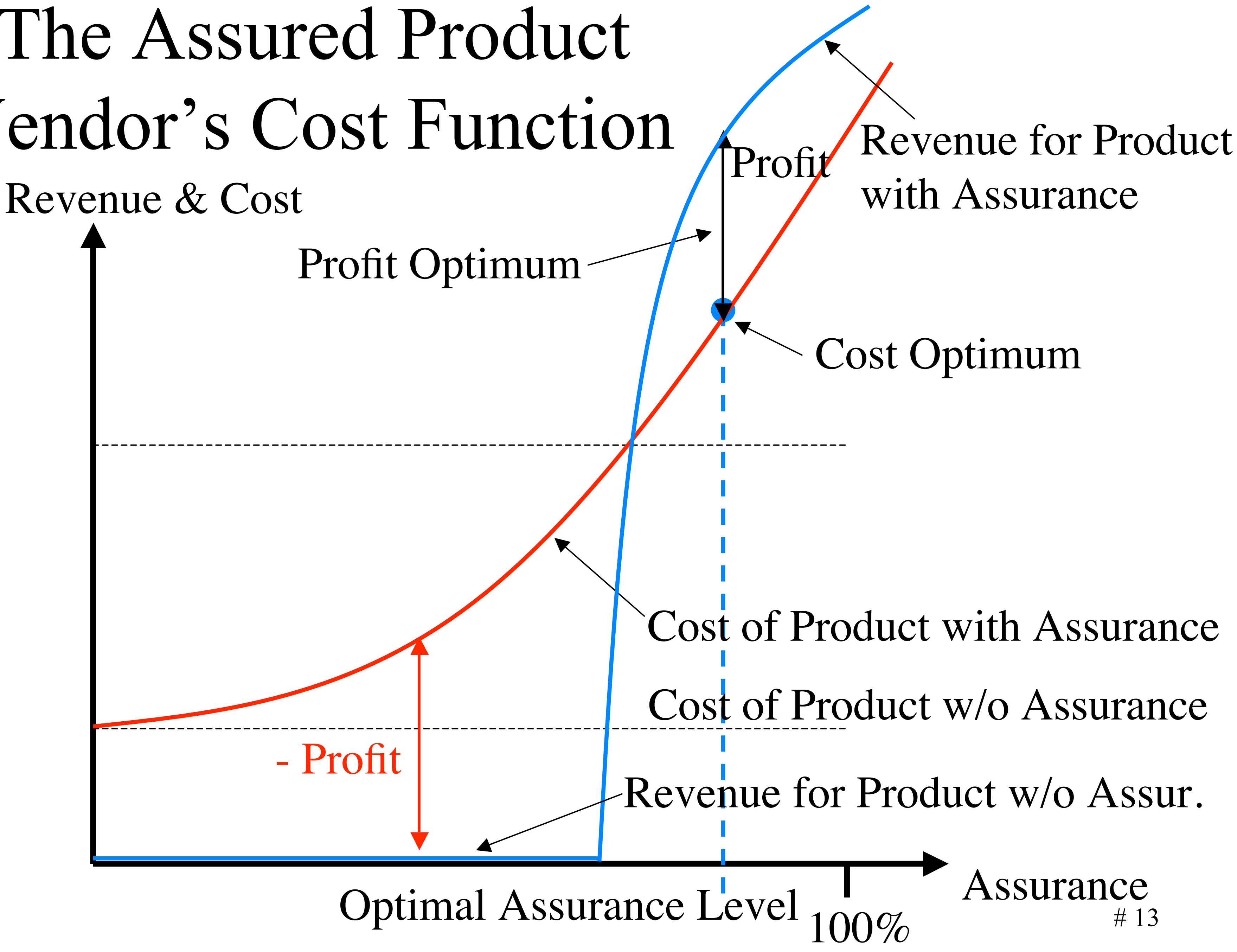
Let’s look at the vendor side

What are the vendors’ considerations?

The Product Vendor's Cost Function



The Assured Product Vendor’s Cost Function



Where’s the disconnect?

- Consumers and vendors have failed to distinguish between “products” and “products needing assurance”
- For such products there must indeed be ***no revenue*** for products of inadequate level of assurance.
  That is, consumers ***must not buy them***.
- It’s ***Supply*** and ***Demand***

Where's the disconnect?
The Demand: This *is* Changing

- Government acquisition rules have changed to require security-enabled products to be ***evaluated*** to a level commensurate with mission.
  - Jan 2000 National Information Assurance Acquisition Policy No. 11
  - Oct 2002 DoD Information Assurance Policy 8500.1
  - Feb 2003 DoD Information Assurance Implementation 8500.2
  - 2002 Federal Information Security Management Act (FISMA)
- The Upshot:
  - As of July 1, 2002 *"the acquisition of all COTS IA and IA-enabled IT products shall be limited only to those which have been evaluated and validated in accordance with criteria, schemes, or programs of the Common Criteria, the National Information Assurance Partnership evaluation and validation program, and the Federal Information Processing Standards validation program."*
- Therefore: There is ***No Revenue*** for inadequate security!

- NSTISSP #11 paired with the Common Criteria and FIPS is vital to the advancement of assured products.

How can you ***know*** if a security product is "good", and ***how good***?

- The question is ***not*** just academic
  - Judging from the avalanche of security alerts and compromise reports there is no lack of "bad security"
- *You have to measure something to control it.*
- It's difficult because of the nature of security
  - Few are qualified to make such a determination
  - Corollary: Few are qualified to create it
  - Consumers (and vendors) must rely on independent experts for objective assessment (evaluation)
  - If it's not ***built*** to be good no one can really tell if it is
- What's needed is ***Assurance*** ! In ***measurable*** amounts.