U.S. National Cybersecurity

Understanding Cybersecurity Policy

William J. Perry
Martin Casado · Keith Coleman · Dan Wendlandt

MS&E 91SI
Spring 2004
Stanford University

Announcements

Announcements

- eForum
- Bios
- Speakers begin next week
- Readings will go out by weekend
- Special guests

Brief History of the Internet: What and Why

The Beginning

1967

- Defense Dept (through ARPA) funds ARPANET project
- ***Why?***
  - **An Inspiration:** Foster community among disparate research centers
  - **A Need:** Avoid wasteful duplication of computer resources → share instead
  - **Not:** For communication in nuclear incident
- Only government actually wants this; everyone else is ambivolent
- Government just says “build it”
- Design left to informal Network Working Group (NWG) made up of researchers, grad students, contractors, etc

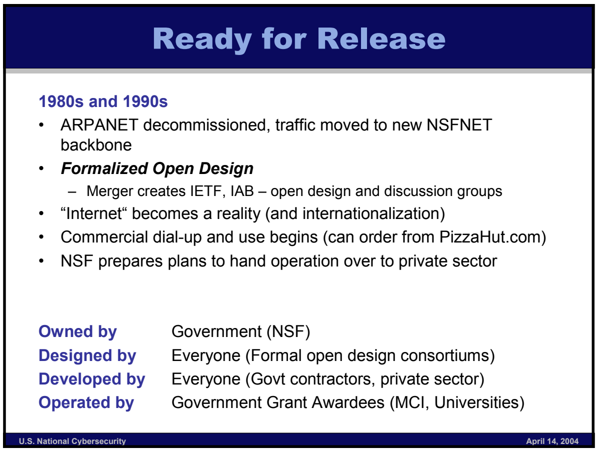
Owned by	Government (ARPA)
Designed by	Government Contractors (NWG)
Developed by	Government Contractors (BBN, Researchers)
Operated by	Government Contractors (BBN)

Opening and Commercialization

1970s & 1980s

- Communication turns out to be the killer use (e.g. Email)
- Surprise innovations driven by users (e.g. WWW, email)
- ***Competition in design***
  - Govt seeds design consortiums with competitors
  - Consortiums decide by consensus → generic platform
- ***MILNET/ARPANET split***
  - Military needs secure system, so it splits to preserve open ARPANET
- ***Govt as a VC***
  - $20 million fund for companies that implement TCP/IP into software

Owned by	Government (ARPA)
Designed by	Everyone (Open design consortiums)
Developed by	Everyone (Govt contractors, private sector)
Operated by	Government Contractors (BBN)

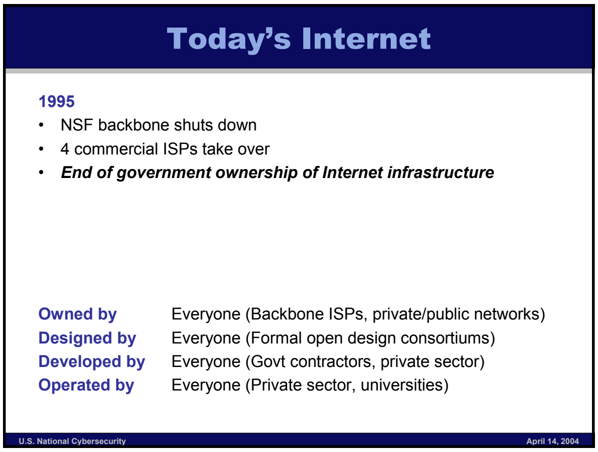


Ready for Release

1980s and 1990s

- ARPANET decommissioned, traffic moved to new NSFNET backbone
- ***Formalized Open Design***
  - Merger creates IETF, IAB – open design and discussion groups
- “Internet“ becomes a reality (and internationalization)
- Commercial dial-up and use begins (can order from PizzaHut.com)
- NSF prepares plans to hand operation over to private sector

Owned by	Government (NSF)
Designed by	Everyone (Formal open design consortiums)
Developed by	Everyone (Govt contractors, private sector)
Operated by	Government Grant Awardees (MCI, Universities)

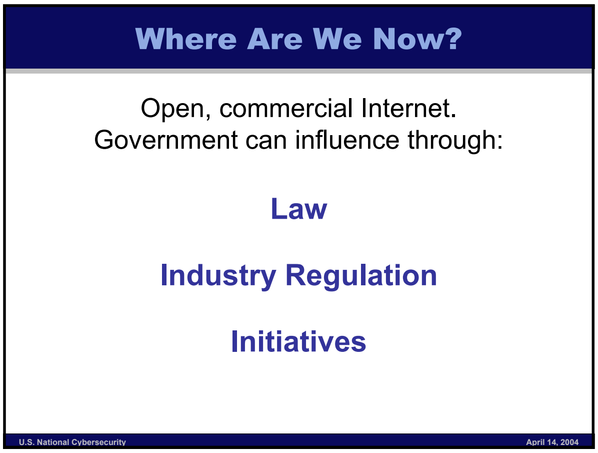


Today’s Internet

1995

- NSF backbone shuts down
- 4 commercial ISPs take over
- ***End of government ownership of Internet infrastructure***

Owned by	Everyone (Backbone ISPs, private/public networks)
Designed by	Everyone (Formal open design consortiums)
Developed by	Everyone (Govt contractors, private sector)
Operated by	Everyone (Private sector, universities)



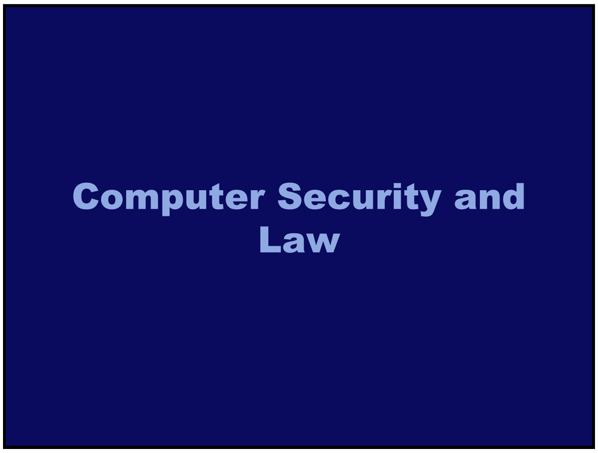
Where Are We Now?

Open, commercial Internet.
Government can influence through:

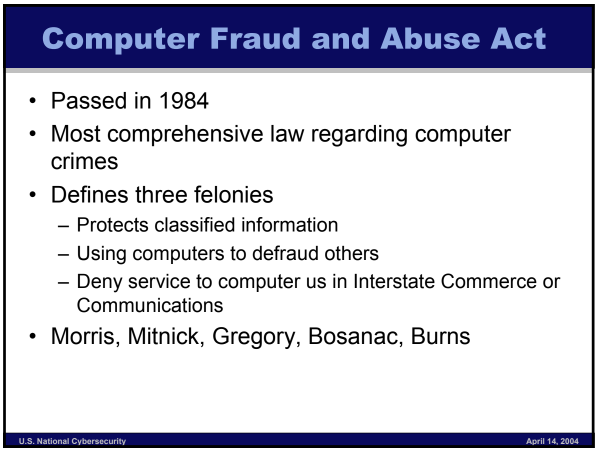
Law

Industry Regulation

Initiatives

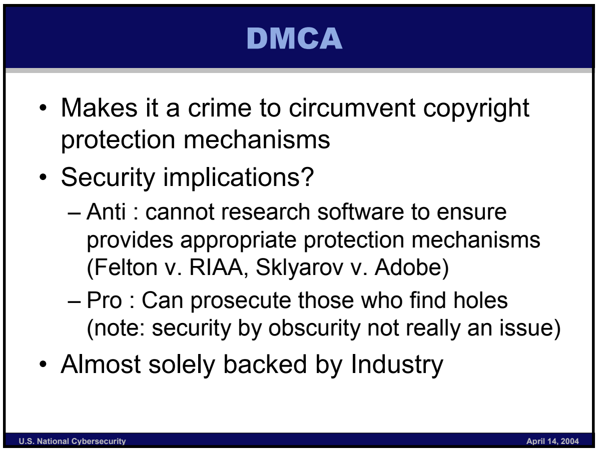


Computer Security and Law



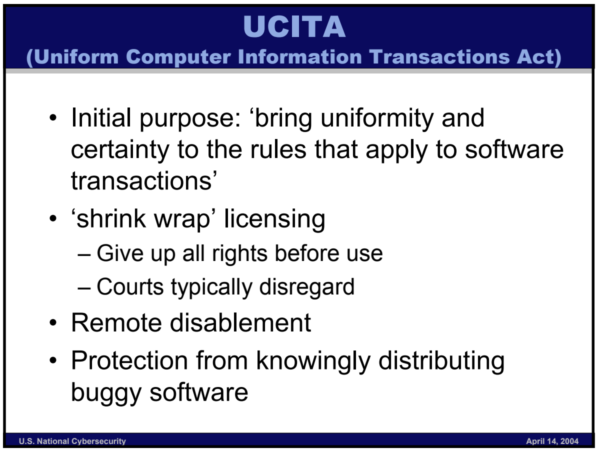
Computer Fraud and Abuse Act

- Passed in 1984
- Most comprehensive law regarding computer crimes
- Defines three felonies
  - Protects classified information
  - Using computers to defraud others
  - Deny service to computer us in Interstate Commerce or Communications
- Morris, Mitnick, Gregory, Bosanac, Burns



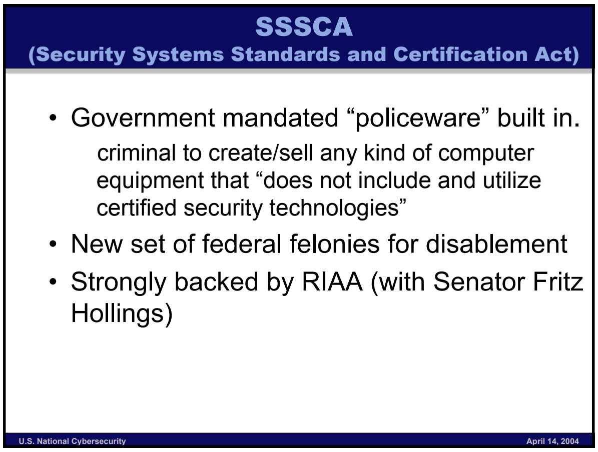
DMCA

- Makes it a crime to circumvent copyright protection mechanisms
- Security implications?
  - Anti : cannot research software to ensure provides appropriate protection mechanisms (Felton v. RIAA, Sklyarov v. Adobe)
  - Pro : Can prosecute those who find holes (note: security by obscurity not really an issue)
- Almost solely backed by Industry



UCITA
(Uniform Computer Information Transactions Act)

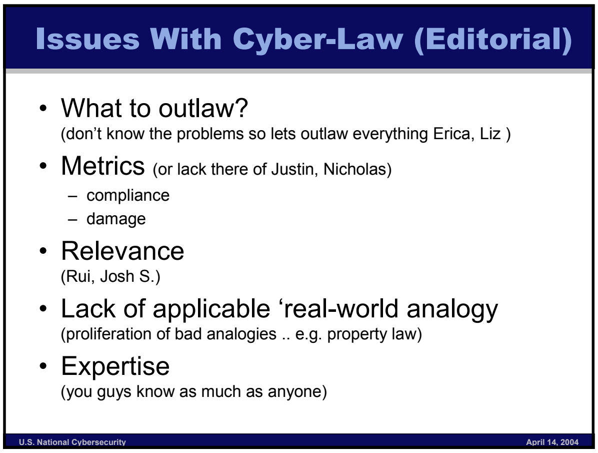
- Initial purpose: ‘bring uniformity and certainty to the rules that apply to software transactions’
- ‘shrink wrap’ licensing
  - Give up all rights before use
  - Courts typically disregard
- Remote disablement
- Protection from knowingly distributing buggy software



SSSCA
(Security Systems Standards and Certification Act)

- Government mandated “policeware” built in.

  criminal to create/sell any kind of computer equipment that “does not include and utilize certified security technologies”
- New set of federal felonies for disablement
- Strongly backed by RIAA (with Senator Fritz Hollings)



Issues With Cyber-Law (Editorial)

- What to outlaw?

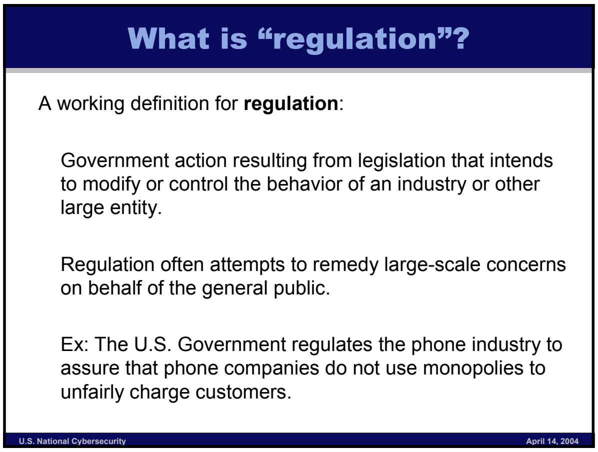
  (don’t know the problems so lets outlaw everything Erica, Liz)
- Metrics (or lack there of Justin, Nicholas)
  - compliance
  - damage
- Relevance

  (Rui, Josh S.)
- Lack of applicable ‘real-world analogy

  (proliferation of bad analogies .. e.g. property law)
- Expertise

  (you guys know as much as anyone)

Cybersecurity Regulation



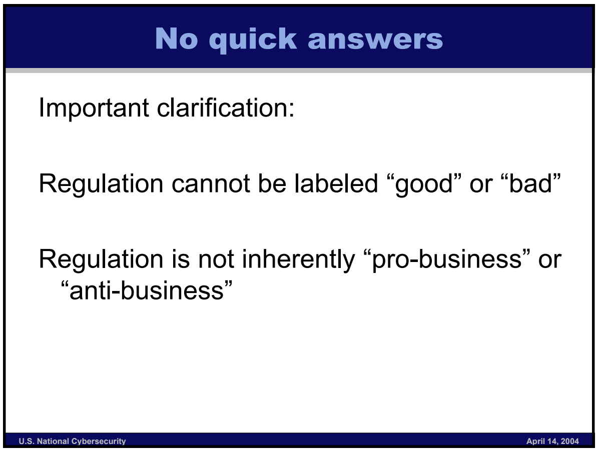
What is “regulation”?

A working definition for **regulation**:

Government action resulting from legislation that intends to modify or control the behavior of an industry or other large entity.

Regulation often attempts to remedy large-scale concerns on behalf of the general public.

Ex: The U.S. Government regulates the phone industry to assure that phone companies do not use monopolies to unfairly charge customers.

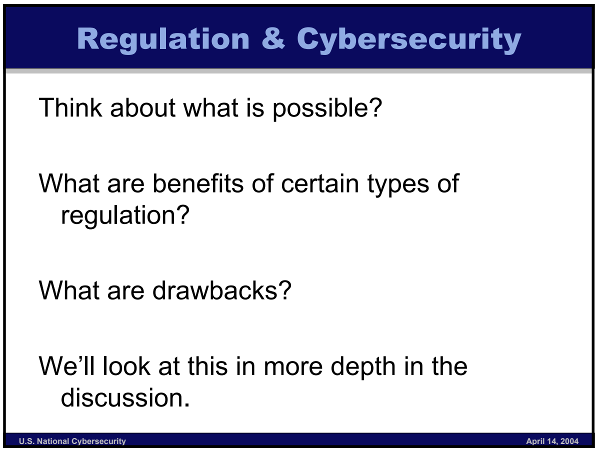


No quick answers

Important clarification:

Regulation cannot be labeled “good” or “bad”

Regulation is not inherently “pro-business” or “anti-business”



Regulation & Cybersecurity

Think about what is possible?

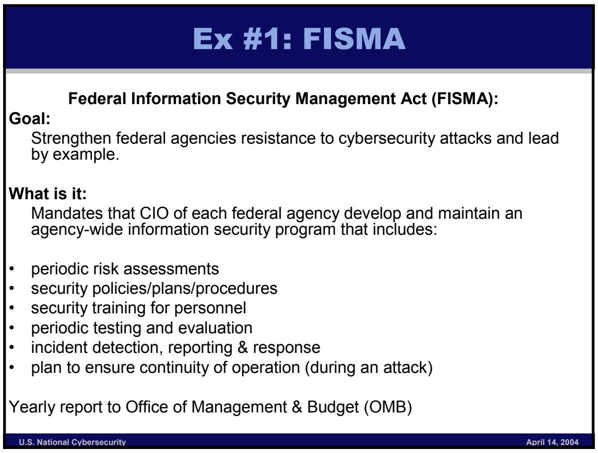
What are benefits of certain types of regulation?

What are drawbacks?

We'll look at this in more depth in the discussion.

Cybersecurity Regulation:

3 Examples



Ex #1: FISMA

Federal Information Security Management Act (FISMA):

Goal:

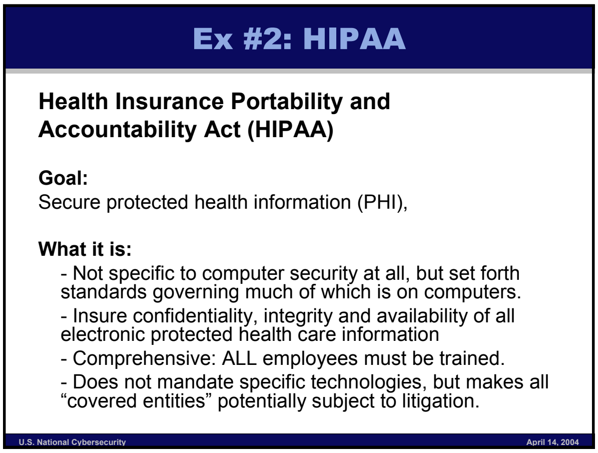
Strengthen federal agencies resistance to cybersecurity attacks and lead by example.

What is it:

Mandates that CIO of each federal agency develop and maintain an agency-wide information security program that includes:

- periodic risk assessments
- security policies/plans/procedures
- security training for personnel
- periodic testing and evaluation
- incident detection, reporting & response
- plan to ensure continuity of operation (during an attack)

Yearly report to Office of Management & Budget (OMB)



Ex #2: HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

Goal:

Secure protected health information (PHI),

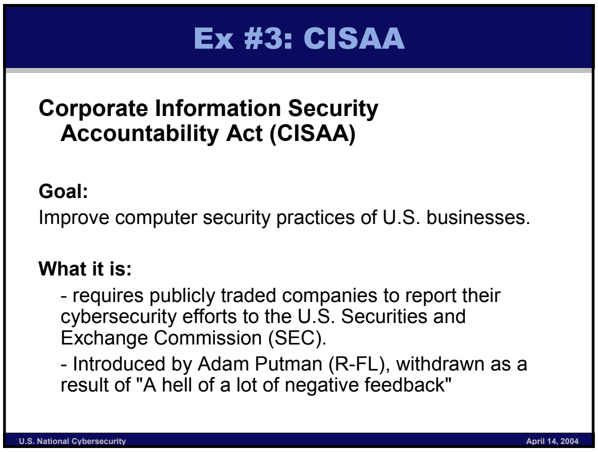
What it is:

- Not specific to computer security at all, but set forth standards governing much of which is on computers.

- Insure confidentiality, integrity and availability of all electronic protected health care information

- Comprehensive: ALL employees must be trained.

- Does not mandate specific technologies, but makes all "covered entities" potentially subject to litigation.



Ex #3: CISAA

Corporate Information Security Accountability Act (CISAA)

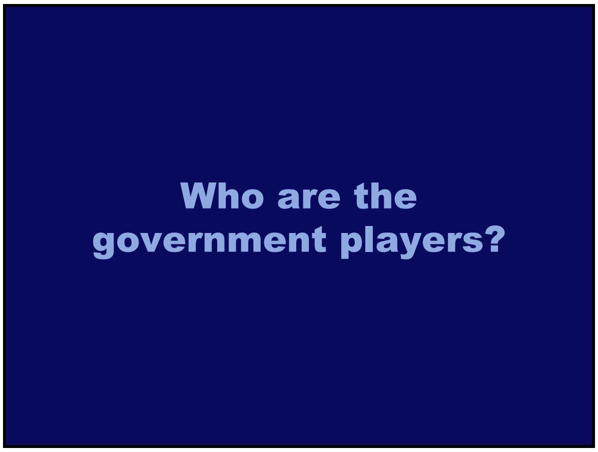
Goal:

Improve computer security practices of U.S. businesses.

What it is:

- requires publicly traded companies to report their cybersecurity efforts to the U.S. Securities and Exchange Commission (SEC).

- Introduced by Adam Putman (R-FL), withdrawn as a result of "A hell of a lot of negative feedback"



Who are the government players?

Gov't Cybersecurity: Then

1996:

President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP).

1998:

Clinton administration issued Presidential Decision Directive 63 (PDD63). Creates :

- National Infrastructure Protection Center (NIPC) in FBI

– Critical Infrastructure Assurance Office (CIAO) in Dept. of Commerce

2001:

After 9/11 Bush creates:

- Office of Cyberspace Security (Richard Clarke)
- President's Critical Infrastructure Protection Board (PCIPB)

Gov't Cybersecurity: Now

Nov. 2002:

Cybersecurity duties consolidated under DHS -> Information Analysis and Infrastructure Protection Division (IAIP) . Exact role of cybersecurity unclear?

June 2003:

National Cyber Security Division (NCSD) created under IAIP. Headed by Amit Yoran from Symantec, the role of the NCSD is to conducting cyberspace analysis, issue alerts and warning, improve information sharing, respond to major incidents, and aid in national-level recovery efforts .

Sept. 2003:

The United States-Computer Emergency Readiness Team (US-CERT) is the United States government coordination point for bridging public and private sector institutions.

Other Gov't Actors

Congress:

Funding is major issue.

House:

- Select Committee on Homeland Security -> Subcommittee on Cybersecurity, Science, Research & Development (Putnam)
- Science Committee

Senate:

- Committee on Government Affairs (no clear winner)

Other Gov't Actors

The usual suspects:

FBI

Secret Service

Dept. of Defense

NSA

and don't forget:

DOE

Dept. Commerce / NIST

SEC

FCC

Dept. of Treasury

Office of Management And Budget (OMB)

and more…

The Big Picture

What's the Point?

Complex web of interactions. There are many different government actors with their own interests and specialties

No top down organization

Government Initiatives

Cybersecurity Initiatives

What is a cybersecurity initiative?

working definition:

A government action that attempts to work with industry or other major actors to help improve cybersecurity.

Question: How is this different from regulation?

Ex #1: National Strategy to Secure Cyberspace (2003)

Goal:

Outline U.S. strategy on cybersecurity and "empower all Americans to secure their portions of cyberspace."

What is does (highlights) :

- **Stresses importance of public/private partnerships**
- **Focus on awareness/information deficit surrounding cybersecurity**
- **Recognizes gov't role as facilitator of research and industry collaboration.**

Ex #2: Cyber Security R&D Act (2002)

Goal:

Promote research and innovation for technologies relating to cybersecurity and increase the number of experts in the field.

What is does:

Dedicated more than $900 million over five years to security research programs and creates fellowships for the study of cybersecurity related topics.

Ex #3: Critical Infrastructure Information Act of 2002

Goal:

Reduce vulnerability of current critical infrastructure systems

What is does:

Allows the DHS to receive and protect voluntarily submitted information about vulnerabilities or security attacks involving privately owned critical infrastructure. The Act protects qualifying information from disclosure under the Freedom of Information Act.

Ex #4: US-CERT (2003)

Goal:

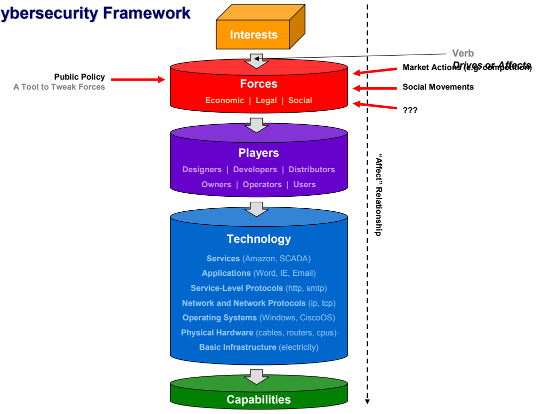
Coordinate defense against and response to cyber attacks.

What is does:

- CERT = Computer Emergency Readiness Team
- Contact point for industry into the DHS and other gov't cybersecurity offices.
- National Cyber Alert System
- Brand new, complete role not clearly defined

A Framework for Cybersecurity

Cybersecurity Framework


Interests
Verb
Drives or Affects
Public Policy
A Tool to Tweak Forces
Forces
Economic | Legal | Social
Market Actions (e.g. competition)
Social Movements
???
Players
Designers | Developers | Distributors
Owners | Operators | Users
Technology
Services (Amazon, SCADA)
Applications (Word, IE, Email)
Service-Level Protocols (http, smtp)
Network and Network Protocols (ip, tcp)
Operating Systems (Windows, CiscoOS)
Physical Hardware (cables, routers, cpus)
Basic Infrastructure (electricity)
Capabilities
"Affect" Relationship

Example: UCITA

UCITA

Broad legislation of software

Would allow companies to put "backdoors" or "time bombs" into software

Let's use the Framework to understand the impact.

Example: Software Cycle

Extend the Software Development Cycle

Theory: too rushed → security holes; release and patch

Alter the cycle by including mandatory code audit by certified reviewer before release

Let's use the Framework to understand the impact.

Example: Spam Blocking

ISPs Block Outgoing SMTP

Spam has long been a problem

Recently ISPs began blocking outbound port 25 (stops relay servers)

There has been spam regulation, but it has not required this

Let's use the Framework to understand *why* this happened.

Analyzing Policies

Test the framework in these policy analysis cases…

Nick Miyake

Would it be unreasonable to require computer owners to possess a license? Or require some kind of preliminary training course before you can sign up for an Internet connection? We require licenses in order to drive, and it works out fine -- pretty much everybody has a license and it isn't a big deal. There are obviously huge problems as far as implementation goes and privacy may also be an issue, but what do people think about the underlying idea? When cars first came out, I doubt that people needed licenses to operate them. However, as they got bigger, faster, and became a greater part of the country, the government started to regulate. Seeing that many consumer computers are at the point where supercomputers that were classified as weapons (placed under export restrictions, at least) a few years ago are, it doesn't seem unreasonable to regulate their purchase or use.

John Cieslewicz

The article by Oram suggests the role that insurance may play in securing cyberspace. Insurance companies often require certain standards to qualify for policies and actively check up on their clients' performance (I'm thinking of fire, earthquake insurance here where building improvements, etc. are often required by the insurer). Could insurance be a solution? Could it result in security practices where insured entities aim to meet the bare minimum security requirements set forth by the insurance companies, knowing that any liability or damage resulting from other security problems will be covered by the insurance company? By the same reasoning, could insurance company or any other regulations (i.e. government regulations) cause common vulnerabilities or failures among entities with computer and/or network systems?

Just A Start…

Goal: Develop a framework

This one is not likely to be it!

But it's a start to get us thinking…
…try using it and see where/how it breaks down

What do you want to get out of a framework and how would you design one that enables this?