Economic Incentives & Metrics of Cybersecurity

US National Cybersecurity

Kevin Soo Hoo

kjsoohoo@gmail.com

November 2, 2006

What’s an Economic Incentive?

- Economics
  - Buzzword: Rational Actor
  - Utility Theory: What People Value
  - Allocation of Resources
  - Descriptive vs. Prescriptive
- Incentive
  - Webster’s Dictionary: *something that incites*

Why People Spend Money They Way They Do?

Why Are Incentives Relevant to Cybersecurity?

- Descriptive
  - Who owns a computer?
  - How many consciously updated OS?
  - How many have Anti-Virus SW? Last update?
  - How about a personal firewall? Configured?
  - What about your friends?
  - Anyone hack for fun? Rip DVDs or CDs?

Who Bears the Risk?

Should Incentives Be Changed?

- Prescriptive
  - What would it take to change your behavior?
  - Should you be responsible?
  - Are others better equipped to do security?
  - Who will solve the security problem?
  - What will it take to get them to solve it?

National Policy Assumes a lot of Answers.

Who Bears Responsibility?

- Should software vendors be liable for damage caused by security flaws?
- Should individual consumers be liable if their computer participates in a DDOS?
- Should ISPs be responsible if attacks flow through their wires?
- Should Government intervene to ensure national infrastructure protection?

Will the Market Solve the Problem?

Why the Market Isn't Enough

- "Pure" Public Good
  - Non-Rivalous: not scarce, no competition
  - Non-Excludable: cannot deny consumption
  - Free-Rider Problem: tragedy of the commons
- Externalities
  - Costs & Benefits accrue to non-participants
  - Network Effect

Is Cybersecurity a public good? Does it exhibit externalities?

Perverse Incentives Abound

- Network Effect: Internet’s value derives from the extensive connections.
- Incentive Disconnect: Security of individual affects the security of others.
- Moral Hazard: Engaging in risky behavior thinking that you are covered -- Mac Users?

Does Government Have a Role?

Government is Already Involved

- Product Liability and Software EULA
- Criminal Laws for Hacking
- Digital Millennium Copyright Act
- Taxation (Sales Tax)
- Governance Laws
  (SB1386, HIPAA, SOX, GLBA)
- FCC and Telecom Regulation
- FTC and Anti-Trust Division of DoJ

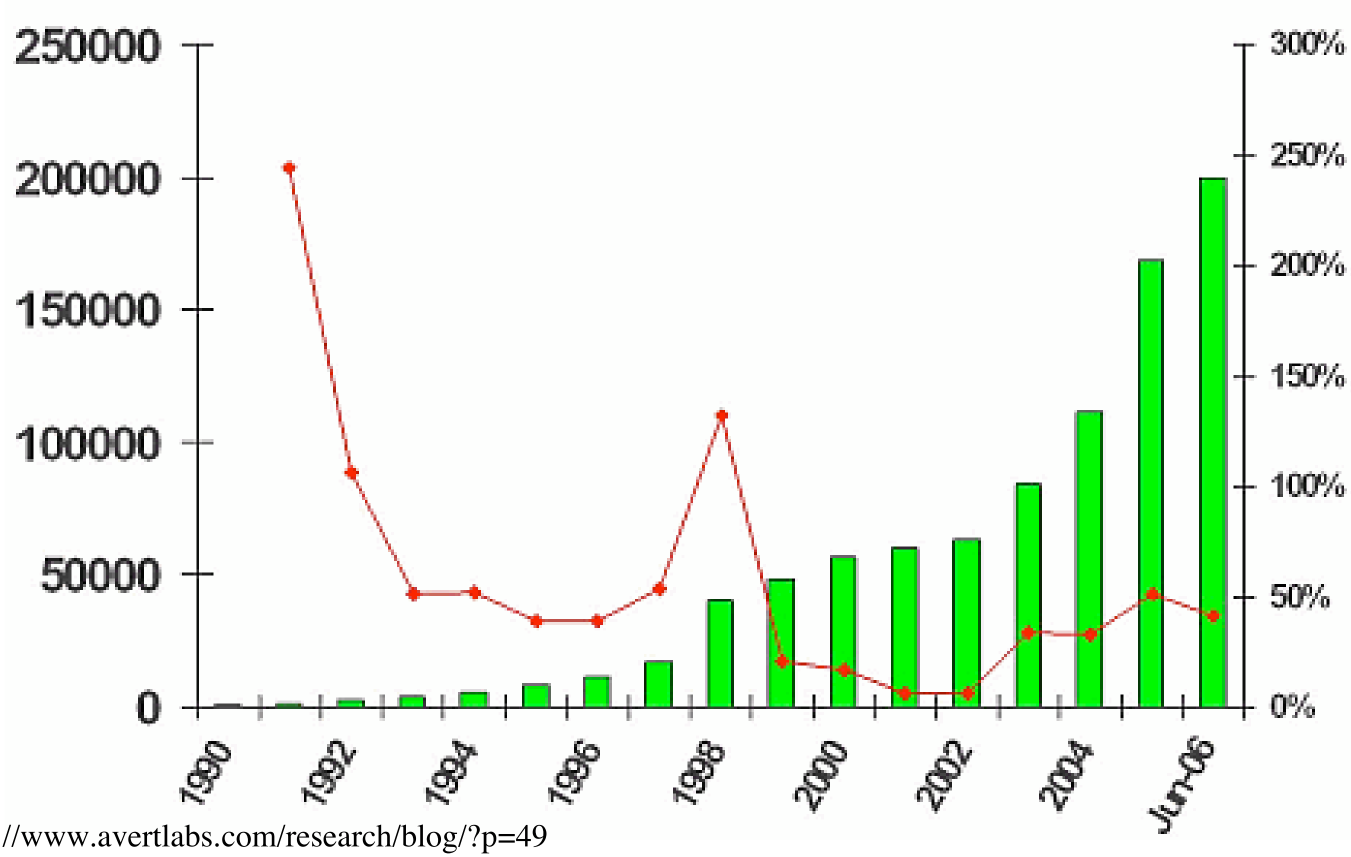
Policy Efforts in Security

- Done So Far
  - Lead by Example
  - Fund Research
  - Establish Standards
  - Encourage Information Sharing
  - Evangelize
- Avoided So Far
  - Regulation
  - Product Liability

Should government do more or less?

Is the Problem Getting Worse?

Malware Count and Growth Rate from McAfee



http://www.avertlabs.com/research/blog/?p=49

What About Damage? Is the Risk Growing?

Security Is Indirectly Measurable

- Other Security Metrics for Known Attacks
  - Troop counts
  - Fence height
  - Lock strength
- Strategies
  - Security Penetration Testing (Red Teaming)
  - Security Vulnerability Assessment (Vuln Scan)

Today, we count what’s easily counted, not what counts.

Challenge of Security Metrics

- Structural Problems
  - Poorly understood adversaries
  - Fast pace of technological change
- Fear of Sharing
  - Reputation loss
  - Liability exposure
- Lies, Damn Lies, & Statistics
  - Sampling errors in voluntary reporting
  - Poor definitions
  - Inconsistent methodologies

What Should We Measure?

- Question of Scale
  - National
  - Organizational
  - Individual
- Definition of Security and Asset
  - Confidentiality, Integrity, Availability, etc.
  - Network, system, hard drive, process
- Question of Lifecycle
  - Asset creation
  - Asset transportation
  - Asset utilization

Vendors Start Counting Everything

- Measure Code Quality
  - Attack surfaces
  - Security flaws
- Measure Threats
  - Viruses and other malware
  - Phishing, SPAM, Adware & Spyware
- Measure Policy Compliance
  - Patch application, latency
  - Policy violations, incidents

Auditors Stake Their Claim

- Regulations
  - Sarbanes-Oxley: public company governance
  - GLBA: financial records
  - HIPAA: health care privacy
  - FISMA: Federal agency security requirments
  - SB 1386: CA notification requirement
- Standards
  - ISO 17799 / BS 7799
  - CoBIT
  - Common Criteria
  - COSO
  - GASSP

Auditors Look for Controls

- Process-oriented security requirements
  - Monitor interface of humans with machines
  - Paper-based policies & procedures
- Controls
  - "Points in a process where the company's best interests are ensured"
  - Examples:
    - expense reports, travel authorization, time cards, etc.
    - active directory, firewalls, password policy, etc.

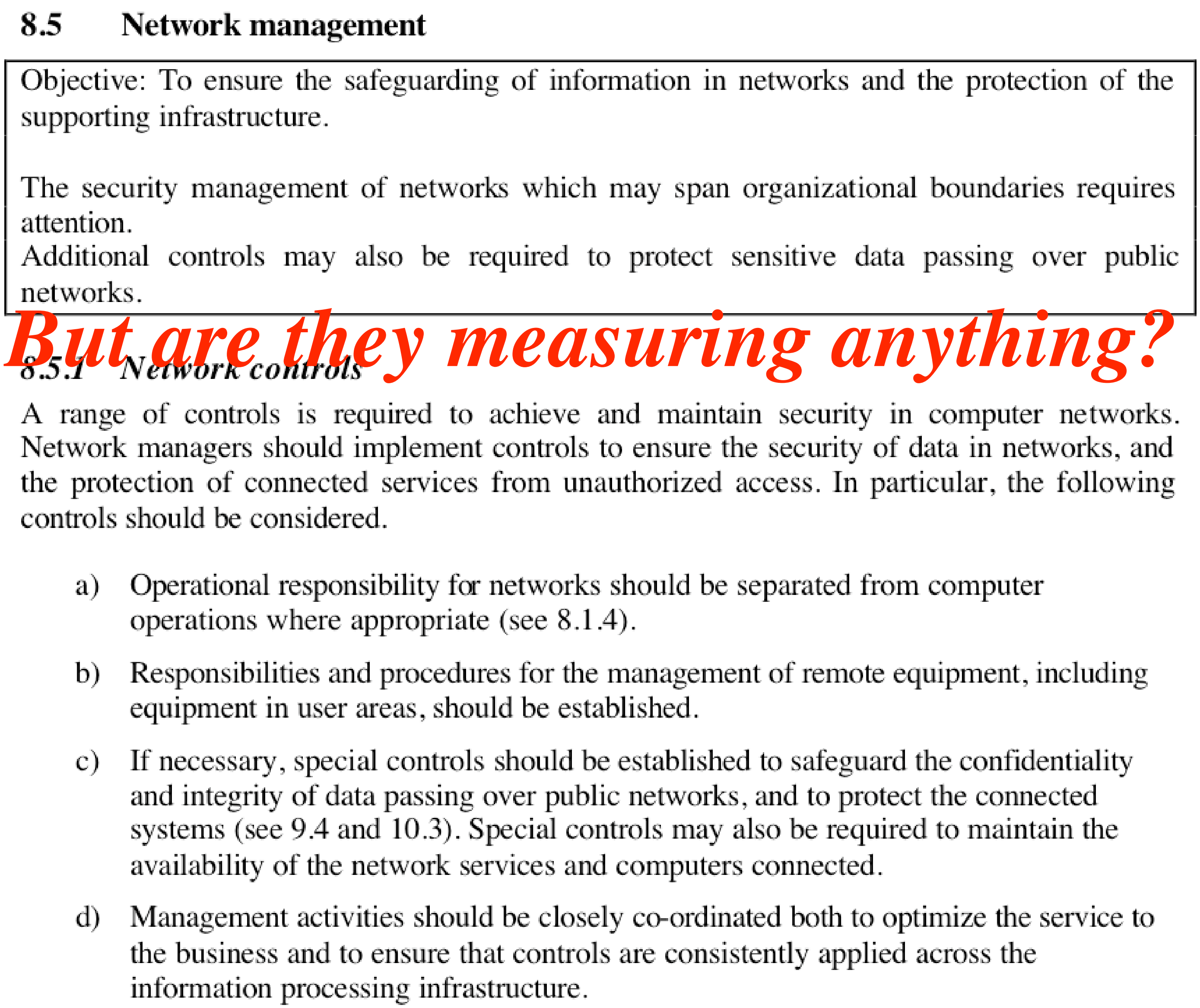
Elusive Bigfoot: Best Practices

- Best Practice vs. Common Practice
- Liability
  - “Reasonable person” standard
  - Industry custom defense
  - Risk assessment trump
- Standards-based Audits Fall Short
  - comprehensive in breadth, shallow in depth
  - inconsistent emphasis and practice

Standards' Depth/Breadth Trade-off

- Requirements
  - Comprehensive
  - Broadly applicable across industries/orgs
  - Limited specialized knowledge/technology
  - Clearly worded and defined
- Example: ISO17799
  - Security Policy
  - Organizational Security
  - Asset Classification
  - Personnel Security
  - Physical and Environmental Security
  - Communications and Operations Management
  - Access Control
  - Systems Development and Maintenance
  - Business Continuity Planning
  - Compliance

ISO17799 Detail



8.5 Network management

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

The security management of networks which may span organizational boundaries requires attention.
Additional controls may also be required to protect sensitive data passing over public networks.

But are they measuring anything?

8.5.1 Network controls

A range of controls is required to achieve and maintain security in computer networks. Network managers should implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access. In particular, the following controls should be considered.

a) Operational responsibility for networks should be separated from computer operations where appropriate (see 8.1.4).

b) Responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established.

c) If necessary, special controls should be established to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems (see 9.4 and 10.3). Special controls may also be required to maintain the availability of the network services and computers connected.

d) Management activities should be closely co-ordinated both to optimize the service to the business and to ensure that controls are consistently applied across the information processing infrastructure.

Measurements vs. Metrics

- Measurements are observations
- Metrics give context to measurements
- Good Metrics have a Goal and are:
  - Specific
  - Measurable
  - Attainable
  - Repeatable
  - Time-dependent

What’s the Goal of Cybersecurity?

- Goals:
  - National Security: Service Availability
  - Protect Identity: Preserve Privacy
  - Economic Security: Ensure Integrity
- Network Integrity:

  A state in which the network performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

How do we link top-level goals to real metrics?

Metrics Depend Upon Actions

- Powers of the Metric Audience
  - Government: Regulation, Liability, Markets
  - Security Executive: Allocate Resources
  - IT Operations: Hardware & Software Service
  - Security Team: Security Policy & Technology
- What Audience Cares About
  - Government: Availability, Privacy, Integrity
  - Security Executive: Money
  - IT Operations: HW/SW & Service Availability
  - Security Team: Data Protection & Service Availability

Metrics for Security Team

- Questions:
    - Were compromised computer policy compliant?
    - What changes should be made to policies?
    - What technologies/processes will prevent future compromises?
    - What was the impact of the compromise?
- Metrics:
    - Vulnerability Counts
    - Detailed Compliance Reports
    - Incident Forensics
    - Impact of Compromise (users, services, costs)
    - Remediation Time

Metrics for IT Operations

- Questions:
  - What computer(s) are compromised? Where? How?
  - How is the compromise taking place? Worsening?
  - How serious is the impact of the compromise?
  - What measures can be taken to isolate/remediate?
- Metrics:
  - Count of Policy-Compliant Devices
  - Counts of Managed Devices vs. Unmanaged
  - Total Devices & Users on Network
  - Network Utilization, Performance, & Wait Times
  - Impact of Compromise

Metrics for Executive Officers

- Questions:
  - How does network integrity compare to peers?
  - How does network integrity compare to last year?
  - Am I spending the right amount on security?
  - What are the cost/benefit trade-offs of investments?
  - What are the costs & consequences of not acting?
- Metrics:
  - Network Service Level
  - Numbers of System Compromises
  - Organizational Impact of Compromises
  - Costs/Benefits of Investments
  - Peer performance on these Metrics

Metrics for Government

- Questions:
  - Can the infrastructure be taken down? How easily?
  - What's the impact of an outage?
  - What can be done to limit damage/prevent outage?
- Metrics:
  - Frequency and Propagation Speed of Worms
  - Time/Effort to Attack Single Points of Failure
  - Risk Assessment of Infrastructure Outage
  - Costs/Benefits/Impact of Policy Options to Address

Where Are We Going?

- Economic Incentives:
  - National Plan Assigns No Responsibility
  - Nobody Owns the Risk
  - ISPs Are Getting into Content Filtering
  - Class-Action Lawsuits Against MS
- Metrics
  - Patch to Exploit Window Shrinking
  - Rudimentary Metrics, Little Sharing, No Analysis
  - Standards: TechNet, CoBIT, CCC, ISO17799, . . .

Threat Environment: Money changes everything.