Cyber Economic Incentives

Alessandro Acquisti

Heinz College/CyLab
Carnegie Mellon University

Toward a Federal Cybersecurity Research Agenda: Three Game-changing Themes

A problem of information, incentives, and rationality

- Research in cybersecurity economics has been growing (WEIS, FC, SOUPS, SHB, …)
- Yet, we still debate basic issues – such as whether markets can provide the solution, and what business case can be made for security. Why?
  - Asymmetric, incomplete information
  - Misaligned incentives and externalities
  - Bounded rationality and cognitive biases

Addressing incomplete information

- Insufficient data
- Disorganized metrics
- "Early stage" models

→ Incentivizing data gathering and information sharing, fostering in turn better metrics and better models

  - However: coordination costs, disincentives to share

Addressing misaligned incentives and externalities

- Do we invest too much? Not enough? Just right?

  Or, perhaps, not *well* enough?

→ Leveraging incentives, liabilities, and regulation

  - However: (not) a zero sum game
  - Holistic approach - identify roadblocks, policy will
  - Government as market maker: Cyber-insurance

Addressing bounded rationality and cognitive biases

- Information and choice are good – but not enough
- Numerous cognitive biases affect security (and privacy) decision making

→ Need to understand them, in order to anticipate them

  - Perhaps even "exploit" them, *nudging* users towards security
  - Security as the *default* setting

For more info

- http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm
- Google: economics privacy
- http://www.cl.cam.ac.uk/~rja14/econsec.html
- Google: economics information security