Policy Recommendations for Cybersecurity

Tyler Moore

Harvard

tmoore@seas.harvard.edu

Regulatory Options

- Ex ante safety regulation & ex post liability
- Information disclosure
  - Toxic Release Inventory
  - Privacy breach disclosure laws
- Indirect intermediary liability
  - Liability isn't always placed on the party responsible for harm
  - If bad actors beyond reach of law, and a 3rd party is in good position to detect/prevent bad acts, then indirect intermediary liability attractive

Intermediary Liability & the Internet

- Believe it or not, Congress has a history of intervening to stop Internet wickedness
  - CDA §230 exempts ISPs from liability for defamatory content posted by users, but also offered protection for *voluntary* cleanup
  - DMCA *obliges* ISPs to remove copyrighted material posted by users, grants exemption from liability in exchange
  - UIGEA *obliges* payment processors to block payment to Internet gambling sites

Recommendation 1

- **Devise a malware remediation program**
  - ISPs *obliged* to act on notifications that its customers are infected with malware by helping to coordinate the cleanup of affected computers, exempted from liability in exchange for cooperation
  - The costs of cleanup will be shared between ISPs, government, software companies and consumers.
  - Reports of infections (including ISP, machine OS type, infection vector, time to remediation, remediation technique) must be reported to a database and made publicly available on the data.gov website.
  - Software companies and government contribute financially to a cleanup fund according to the number of reported infections affecting its software.
  - Consumer contribution to cleanup is capped, guaranteed no disconnection in exchange for cooperating with cleanup

Recommendation 2

- **Publish aggregrated online banking & payment fraud figures on data.gov**
  - Incident figures: # of incidents, total $ stolen, total $ recovered for specified # of incidents
  - Victim bank demographics: # banks affected, # customer accounts impacted per bank, $ lost per customer, bank type, precautions taken by bank
  - Victim customer demographics: Business v. consumer breakdown - #s and losses
  - Attack vector (if known): keyloggers, phishing, card skimming, payment network compromise, etc.
  - Business category: online banking, payment cards (transaction type: retail, card present, card not present), ATM fraud

Recommendations 3&4

- **Mandated disclosure of control system incidents and intrusions**
  - Conflicting reports of widespread intrusions yet little observed by industry
  - Either voluntary disclosure via ISACs has failed, or there truly has been nothing to report
- **Aggregate reports of cyber espionage and report to WTO**
- *Contact me for a draft of the paper*
  tmoore@seas.harvard.edu