CSCI 1800 Cybersecurity and International Relations

Economics of Cybersecurity

John E. Savage

Brown University

What is Cyber Economics?

- It is the study of the economics of computer and network security.
  - Understanding incentives
  - Learning from market failures
  - Appreciating the important of externalities
  - The value of intermediaries
  - Formulating policy and remedies

Why Should CS Talk about Economics?

- Conventional CS approach failed to identify and correct all the threats

- CS needs help from economists to exercise control over vendors, markets and users
  - Economists understand use of incentives/penalties to control behavior, e.g. social media influence campaigns
- Situation is somewhat different for encryption
  - Good end-to-end encryption is contained, well defined,
  - But not exceptional access, i.e. access with warrant

Outline[1]

- Since many cybersecurity problems are economic, modest incentives can significantly improve security.
- Four areas are examined
  - Online identity theft, industrial espionage, critical infrastructure protection, and botnets.
- Three economic challenges:
  - Misaligned incentives, information asymmetries, and externalities.

1. Digest of *Introducing the Economics of Cybersecurity: Principles and Policy Options*, Tyler Moore, appearing in **Procs. Workshop on Deterring Cyberattacks**, NAS Press, 2010.

Some Cybersecurity Application Areas

- Data breaches
  - Primary way that information on individuals is lost
- Industrial cyber espionage
  - Secrets remotely stolen; undetected.
- Critical infrastructure protection (listen to talk*)
  - Industrial control systems vulnerable & not protected
- Botnets
  - Common and involved in many types of attack.

* Securing North American Electric Grid: https://www.youtube.com/watch?v=I6DBAhGx5mQ (43 mins)

Industrial Cyber Espionage

- Operation Aurora launched in 2009.
  - Google revealed attack from China and eventually stopped offering its search service there.
  - The attack targeted Perforce repository software at Google and more than 30 other companies.
  - The Google Aurora attack received a great deal of press and government attention.
  - Were files just stolen or were they modified?
- Mandiant 2013 APT1 report shows this was tip of the iceberg. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Critical Infrastructure Protection

- Example:
  - 2007 Idaho National Lab experiment (also called Aurora*) that destroyed a power generator. https://www.youtube.com/watch?v=fJyWngDco3g
- US government has identified 16 critical infrastructure sectors.
- SCADA† systems are involved in almost all sectors. They are considered poorly protected.

* https://en.wikipedia.org/wiki/Aurora_Generator_Test

† SCADA: Supervisory Control and Data Acquisition

Economic Barriers to Cybersecurity

- Misaligned incentives
  - E.g. If those responsible for protecting a system don't pay for security violations, no incentive to keep it safe.
- Information asymmetries
  - Absence of critical information can lead to poor decisions that alter markets. Example coming
- Externalities
  - Costs incurred by others not party to transactions.
  - E.g. air pollution reduces a manufacturer's cost but increases cost to society.

Misaligned Incentives

- If those who acquire systems don't pay a price for the failure of systems to meet specs, failures are more likely.
  - E.g. Electricity companies save money by replacing atomic clocks with GPS.
  - When a solar flare wipes out GPS, the public pays the price.

Misaligned Incentives

- There is a natural tension between efficiency and resiliency in design of IT systems.
  - Critical infrastructures used to be operated on separate networks. E.g. ATT network (SS7), SCADA systems
  - Efficiency drives us toward network convergence. We are now heavily dependent on Internet.
  - Who is concerned about the unintended consequences?
    - See https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2017/gridex-iv-tests-the-north-american-power-grid/
- Efficiency often trumps security
- When security fails, cost often borne by the public.

Information Asymmetries

- Incidence data is essential but hard to obtain.
  - Companies don't want to reveal vulnerabilities.
  - Reputations (and stock prices) are on the line.
  - If incident can't be ignored, such as Target POS attack, then it is reported
- Each of the 50 US states has a breach law.

Information Asymmetries

- Asymmetric information can be deleterious:
  - Ackerlof received the 2007 Nobel Prize for his explanation of the pricing of auto “lemons”
  - If market has 50 “good” used cars @ $2K and 50 lemons @$1K but customers can’t tell them apart, price drops well below $2K. Owners of good cars will not sell. Market gets filled with lemons.
  - Buyers won’t pay premium for quality that can’t be measured

Information Asymmetries

- Secure software is a market for lemons
  - Because buyers can't tell which software is more secure, they have no incentive to pay more for one product versus another
  - Wy should vendors to spend on security?
- Robust cyber incident data is missing
  - Unless required by law, breach notifications not done
  - Without good loss measurements, resources cannot be allocated properly.

Externalities

- Positive network externality:
  - First-mover advantage results in market dominance
    - Think Facebook, Windows, etc.
- Negative network externalities:
  - Firms ignore security to achieve dominance
  - When firms dominate, individuals lose control over some issues, such as privacy.

Other Negative Externalities

- Underinvestment in security may impose burden on others:
  - Botnets proliferate
  - The power grid is less secure
  - National security is put at risk
- Free riding
  - If investment in security by others protects you, why would you invest in your own protection?
  - Consequence: security is likely to decline

Addressing Externalities

- Some solutions effective only when widely used
  - The Border Gateway Protocol (BGP), which is employed to announce new IP addresses, is insecure
  - Pakistan Telecom stole YouTube for 2 hours in '08
    - https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/
- Several methods to secure BGP introduced but are not widely used.
- New approach: ARTEMIS*, operated by an AS

* https://blog.apnic.net/2018/07/19/artemis-neutralizing-bgp-hijacking-within-a-minute/

Is Regulation the Solution?

- Topics we examine:
  - Ex Ante Safety Regulation vs Ex Post Liability
  - Information Disclosure
  - Cyber-Insurance
  - Indirect Intermediary Liability

Ex Ante Safety Regulation vs Ex Post Liability

- Ex ante goal: prevent accidents in advance.
  - 1999 Gramm-Leach-Bliley Act – repealed Glass-Steagall Act of 1933 & allowed affiliations between commercial banks and securities firms. (See Crash of 2008!)
- Ex post liability: threat of monetary damages
  - Would this push Microsoft to make code more secure?
    - Were they making progress without it? Or were aware of cost?
  - Ex post liability has a negative externality – it would reduce pace of innovation.
  - But, without changes in coding techniques, software security may not increase.

Ex Ante Safety Regulation vs Ex Post Liability

- Unfortunately, security errors are unavoidable.
- Would results be better if vendors were held to a higher standard of coding and testing?
- In some sectors, best to use both approaches.
  - However, ex ante regulation doesn't work well when regulator lacks information about harms or is uncertain about minimum standards.
  - Also, ex post liability doesn't work when firms not always held responsible or they can't pay.
- These conditions often hold in cybersecurity.

Information Disclosure

- Since information asymmetries are barriers to cybersecurity, info disclosure may be the answer.
  - "Sunlight is the best disinfectant" – Justice Brandeis
  - Community has a right to know.
- Law requires disclosure of toxic chemicals released into the environment.
  - This law has reduced the amount of such chemicals.
  - The Whitehouse-Kyl Cyber Security Public Awareness Act of 2011 might have done the same for cyber.
    See http://www.gpo.gov/fdsys/pkg/BILLS-112s813is/pdf/BILLS-112s813is.pdf

Information Disclosure

- In 2017 Ponemon Institute study
  - Average cost of a breach was $3.62 M
  - Probability of a material data breach ~ 28%
  - Average of 191 days needed to discover a breach and 66 days to contain it.
  - Breach source: Criminals (47%), Glitches (25%), Error (28%)
  - Existence of incident response team reduces cost
- Failure to publicize breaches exposes others.

Information Sharing

- Information sharing and analysis centers (ISACs) are industry groups set up by DHS to protect the critical infrastructure.
  - Data access limited to ISAC participants.
  - Financial Services ISAC (FS-ISAC) said to be effective
  - But, there is evidence suggesting that targeted threat sharing, i.e. directly affecting a company, is preferred to general threat sharing
  - Information sharing and analysis organizations (ISAOs) – sharing between org.s, not industries

How to Manage Risk?

- Accept it
  - Pay for loss through fees
- Mitigate it
  - Install better technology (increases security cost)
- Avoid it
  - Impose customer requirements (lost business?)
- Transfer it
  - Buy cyberinsurance (must pay premiums)
  - Let others absorb the loss

Cyber-Insurance

- Coverage provided for data breaches, business interruption, and network damage.
- Offers incentives to take precautions
- Rewards investment by lowering premiums
- Encourages data collection, dealing with informational asymmetries.
- Smooths out financial outcomes – small fixed present cost offsets future large losses.

Cyber-Insurance

- Cyber-insurance market been small for a long time.
- What is wrong with cyber-insurance industry?
  - On the demand side: firms not aware of their risks. Legislation clarifying liabilities might help.
  - On the supply side: Hard to measure security levels
- Needed: partnerships between forensics firms and insurance companies to better assess, reduce risk and price insurance products.
  - E.g. Arceo Analytics – combines insurance & forensics

Indirect Intermediary Liability

- Liability doesn't have to be placed on the party directly responsible for harm.
- Usually 3 players: bad actor, victim, third party.
  - E.g. Employers responsible for actions of employees
- Works when
  - Bad actor inaccessible, can't be identified, or can't pay if caught.
  - Too costly to design contracts that assign blame fairly.
  - Third party can detect or prevent harm & can internalize negative externalities by reducing number of bad actors.

Indirect Intermediary Liability

- Lichtman and Posner (2004) argue that these conditions apply to ISPs as third parties*.
  - For what types of behavior could ISPs play this role?
- ISPs exempted from liability for defamatory content of subscribers (1996 Communications Decency Act)
  - Gave license to ISPs to monitor posts by users
- DMCA exempts ISPs from copyright violations if they comply with "notice-and-takedown" requests.
- To stop online gambling, credit card companies are made 3rd parties.

* https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1235&context=law_and_economics

Indirect Intermediary Liability

- The FCC announced in 2012* that ISPs representing more than 90% of US Internet users have agreed to take voluntary action against the following cyber threats:
  - Anti-bot Code of Conduct
  - DNS Best Practices
  - IP Route Hijacking Industry Framework

http://www.techlawjournal.com/topstories/2012/20120322.asp

Indirect Intermediary Liability

- Credit card fraud makes bank the intermediary when fraud occurs at brick and mortar establishments but makes the merchant the intermediary for online transactions.
  - The reason apparently is that online transactions are considered more risky.
  - This treatment of fraud could change over time

Botnets Becoming Major Threat

- Mirai botnet became major threat in late 2016
  - ~1.2 terabit/sec against DYN
- Infected hundreds of thousands of devices:
  - Cameras, some printers and routers
- Located in
  - Vietnam (13%), Brazil (12%), US (11%), China (9%), Mexico (8%), Taiwan (5%), Russia (4%), etc.
- 2018 ~1.3 terabit/sec against Github*

* https://www.wired.com/story/github-ddos-memcached/

Recommendation #1: Infected Bots

- Tyler Moore's program for malware remediation
  - Require ISPs to act on notification of customer infection by helping to clean up customer computer. In return, ISPs exempted from liability. Else, liable.
  - Share cost of cleanup between ISPs, government, software vendors and consumers.
  - Publicize infections (report ISP, OS type, infection vector, time to remediation, and fix.)
  - Make software vendors pay for cleanup in proportion to number of reported infections of their software.
  - Cap the consumer contribution. They cannot be disconnected if they cooperate in cleanup.

Cleaning Up Infected Bots

- Situation unsatisfactory. What should be done?
  - Can encourage ISPs to help customers – very weak.
  - Can use DMCA as model. Give immunity to ISP if they help cleanup infected computers. Make them responsible if they don't.
- Must have a) fair distribution of cost of cleanup, b) transparency via mandatory disclosure of infections, and c) protection of consumer connections.

Recomm. #2: Fraud & Security Disclosure

- Regularly publish aggregated losses due to online banking and payment cards.
  - Incident figures
  - Victim demographics
  - Attack vectors
  - Business category
- Such info can help decide security measures.

Fraud & Security Disclosure

- FBI runs Internet Crime Complaint Center (IC3)
- Financial services ISAC data kept in closed circle.
  - Because ISACs have voluntary disclosure systems, financial services industry does not internalize all costs of insecurity. Businesses cover themselves.
- Users also need to know where fraud occurs.
- Disclosure would help decide if more secure credit card technologies should be used.

Recommendation #3: SCADA Incidents

- Make disclosure of control system incidents and intrusions mandatory to the relevant ISACs who then publicly disseminate them.

- Intelligence officials say that Chinese and Russians are regularly intruding into US electrical grid.

Recommendation #4: Espionage

- Aggregate and report cyber espionage and report to WTO.

- Industrial espionage is a significant problem for American companies.
- They don't report intrusions for fear of damaging their reputations.
  - Did the Google Aurora caper signal a change?

Conclusion

- Economic perspective essential to understand cybersecurity today and to improve it.
- Principal recommendations:
  - Get ISPs to take more active role in ridding malware
  - Collect and publish data on a range of security incidents
  - Raise awareness of the issues and assign responsibility for action