Cybersecurity Economics

CYBR 4400/5400: Principles of Internet Policy, Lecture 6-3

Dr. David Reed, Technology, Cybersecurity, and Policy Program, CU Boulder

Class Announcements

- New lecture format for this week!
  - will record lectures and post recordings and lecture slides to module 6 on Canvas under official class meeting dates
    - you can view at your convenience, but strongly urge keeping up!
- Opening ”Lecture Questions and Discussion” thread on Canvas
  - post any questions you have while viewing lectures, and I will respond in timely fashion (goal: 24 hours)
- Final exam: essay format
  - Available from 5 a.m., Saturday, May 2 — 10 pm, Tuesday, May 5 on Canvas

Today's Lecture

- Current Events
  - German Wins 'Right to Be Forgotten' Case
- Cybersecurity Economics Lecture

Cybersecurity Economics

Cybercrime Economics

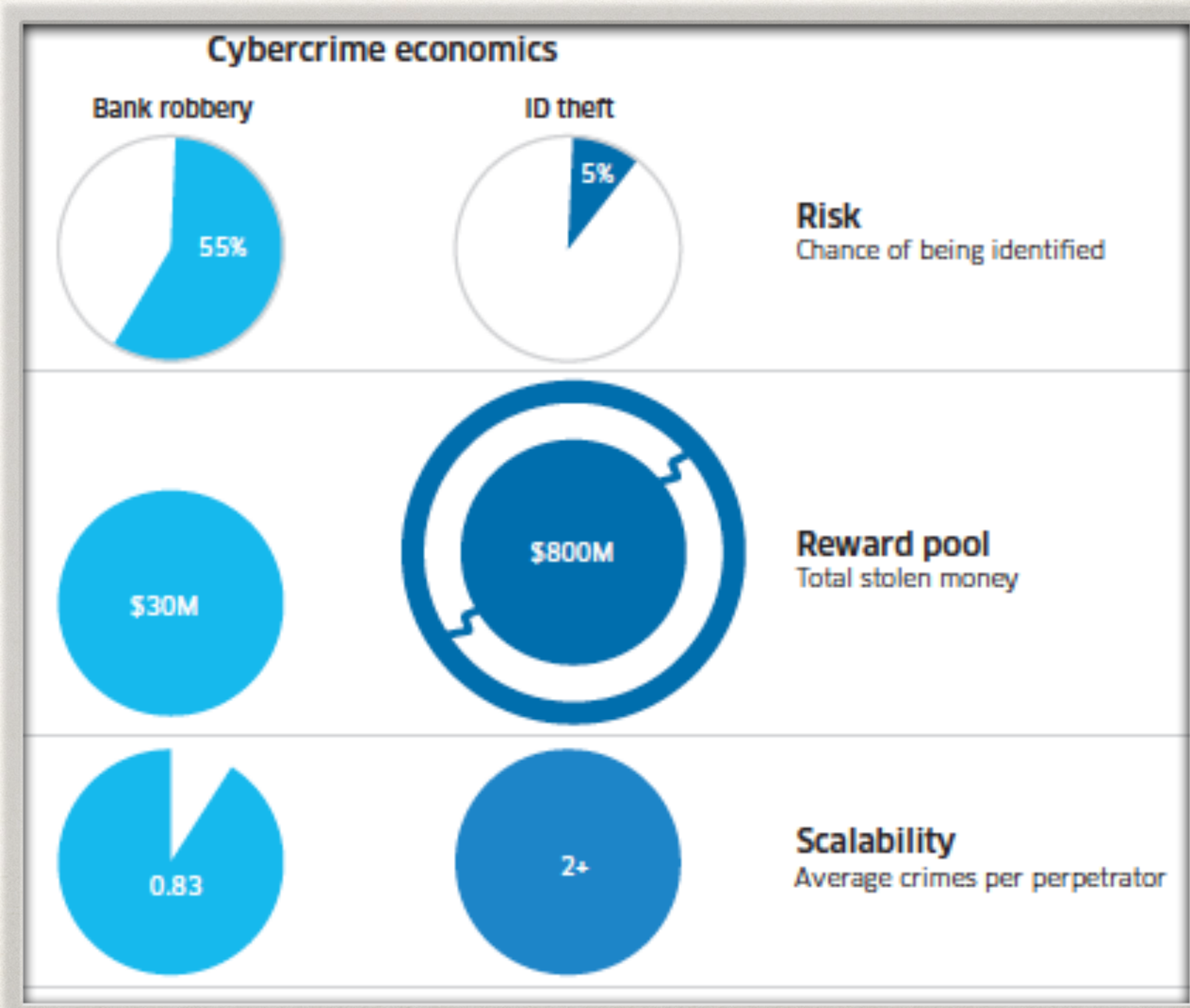
- "Information is secure when it costs more to get it than it's worth."

- Kevin Poulsen (aka "Dark Dante, now Wired contributing editor)

What are the trends in today's world?

Cybercrime Economics

- Cybercrime more lucrative than traditional crime
- Online markets for tools



Source: The Future X Network, A Bell Labs Perspective, Chapter 3, 2016

Key Economic Concepts in Cybersecurity

- Misaligned incentives
- Information asymmetries
- Market externalities

Misaligned Incentives

- Parties making security-efficiency tradeoff are not who incur costs when attacks occur — between those responsible for security and those who benefit from protection
  - Medical records in hospitals
  - Electric utilities control systems
  - Online banking
- Tradeoff between short-term efficiency and long-term vulnerability of system resilience
- All can lead to suboptimal choices due to misalignment

Information Asymmetries

- Lack of available data needed to guide security investment
- Who knows the costs of cyber threats?
  - Banks do not disclose online fraud losses
  - Business want to protect reputation, not draw attention to vulnerabilities
- Is security software a “market for lemons”?
- Decision making under uncertainty
  - Asymmetry means level of investment likely inefficient

Externalities

- Entities actions have side effects on others
- Race for network effects often involves insecure software pushed to market; and slow adoption of secure upgrades (DNSSEC/S-BGP)
  - SSH/IPSec provide immediate internal benefits
- Negative externalities in attacks lead to under-investment to prevent societal risk
  - Cyber security a public good?
- Free riding likely when security depends on the weakest link in the chain (why invest if others don't?)

Solutions for Market Failures

- *Ex ante* safety regulation
  - Firms adopt best practices and test compliance (Financial Services Modernization Act, Health Insurance Portability and Accountability Act, etc.)
- *Ex post* liability
  - Section 5 of Federal Trade Commission Act grants FTC authority to take action against *unfair or deceptive acts* that affect commerce

Solutions (cont'd)

- Information disclosure
  - Establish Information Sharing and Analysis Centers (ISACs)
    - Nonprofit organizations gathering info on cyber threats to critical infrastructure and providing two-way sharing of info between private and public sectors
    - Check out the Auto-ISAC website for a good example

National Council of ISACs (NCI Directorate) members:

- Automotive (Auto-ISAC)
- Aviation (A-ISAC)
- Defense Industrial Base (DIB-ISAC)
- Emergency Services (EMR-ISAC)
- Electricity (E-ISAC)
- Financial Services (FS-ISAC)
- Information Technology (IT-ISAC)
- Maritime Security ISAC
- Multi-State ISAC (MS-ISAC)
- Communications ISAC (NCC)
- National Health (NH-ISAC)
- Nuclear (NEI)
- Oil and Gas (ONG-ISAC)
- Public Transit (PT-ISAC)
- Real Estate (RE-ISAC)
- Research & Education (REN-ISAC)
- Retail (R-CISC)
- Supply Chain (SC-ISAC)
- Surface Transportation (ST-ISAC)
- Water ISAC (Water-ISAC)

Solutions (cont'd)

- Information disclosure

https://www.wsj.com/articles/nsa-to-issue-updated-cloud-security-guidance-11575409110?mod=hp_minor_pos4

NSA to Issue Updated Cloud Security Guidance

Intelligence agency to detail methods that nation-state hackers use to compromise companies

By James Rundle and Catherine Stupp

Dec. 3, 2019 4:38 pm ET

The National Security Agency plans to issue updated guidance to companies on cybersecurity in the cloud, a senior official said, amid a series of attacks that have targeted service providers in recent months.

Anne Neuberger, director of the NSA's Cybersecurity Directorate, said that one of her division's goals is to produce advisories for businesses and other organizations. The advisories will describe attack methods used by nation-state and advanced hackers and will lay out methods to counter them.

Solutions (cont'd)

- Cyber insurance
  - Mechanism to manage risk (insurance companies can offer incentives for precautions/collect data on incidents/smooth costs)
  - Global market projecting strong annual growth of 25% through 2025 (from $4.6B in 2017)
    - Standalone cyber insurance rate approaching 40%
    - Cyber insurance purchases grew most among hospitality and gaming (67%) and education (34%) organizations
    - Average limits purchased grew 11% to $20.9M
    - Among companies with revenues above $1B, average limits increased by 25% to $62.4M

Source: "Cyber Insurance Demand, Supply, Awareness Continue to Grow, Insurance Journal, April 17, 2019

What Does Cyber Insurance Cover?

- Also known as Cyber Risk or Cyber Liability Insurance
- Covers costs associated with an actual data breach where customers' PII exposed or stolen from firm's data network
- Forensic investigation to determine what occurred, how to repair damage, how to prevent similar breach in future
- Business losses due to network downtime, business interruption, data loss recovery, costs involved managing crisis, and repairing reputation damage
- Data breach notifications to customers and other affected parties
- Legal expenses associated with release of PII and IP, legal settlements, regulatory fines (may include costs of cyber extortion)

Economic Approaches to Enhancing Cybersecurity

- Use existing market mechanisms but with improved flow of info (e.g., better info about threats and vulnerabilities)
- Insurance (incentives for lower premiums)
- Liability accountability
- Direct regulation (e.g., adoption of best practices)

Other Policy Concerns

- Innovation
  - Reducing time to market vs. security by design
  - Ease of use, interoperability, and backward compatibility vs. security
- Standards setting and certification
  - Good practices codified in standards, public recognition of conformance can improve competitive position
- Civil liberties
  - Privacy/free expression/due process