The Economics of Cybersecurity — Lecture 7 Notes

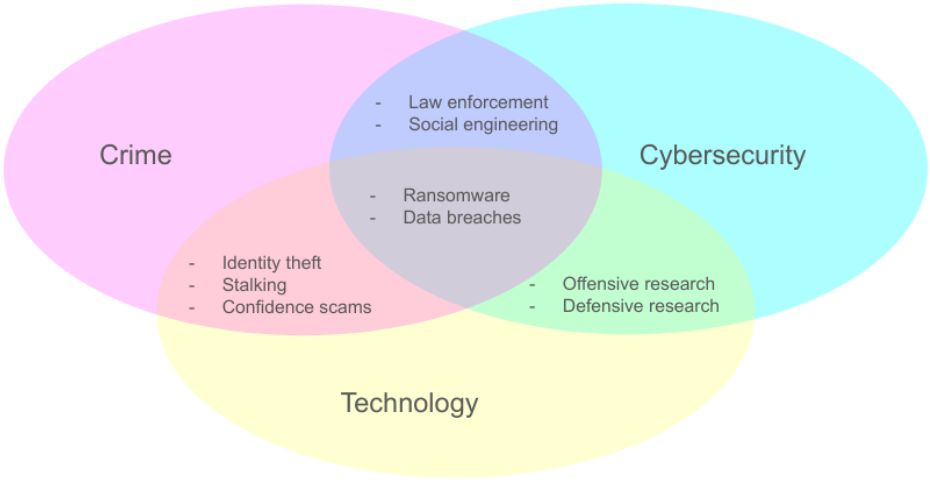
Adam Hastings

February 27, 2024

In this class we will look at three approaches towards measuring cybercrime: One from government, one from industry, and one from academia.

- What is the relationship between cybercrime and cybersecurity?
  - Are they two sides of the same coin? (Not really—Are romance scams really a question of cybersecurity?)

Show Venn Diagram of Security, Technology, and Crime:



We might think of this topic like this. But I might make a bold claim that the orange and purple sections are really just a part of the brown section. Example: Social engineering often relies on tricking a victim in some way, e.g. phishing for credentials via a false website. In many ways that is not a technology problem. The technology is not being exploited, it's social trust that's being exploited. Or is it? You could also argue that passwords are inherently weak and authentication

shouldn't rely on passwords in the first place, and should be physical-token-based authentication. So is this a security problem?

Likewise, a romance scam is not really a cybersecurity problem. But it's the same root issue of the Internet's lack of strong identification. It's hard to really know who you are talking to. So maybe this is a security problem?

(I'm going to ruffle some feathers with this one) Question: Can someone define "hacking"? (Among the hacker crowd, this usually is something close to "exploiting a technological flaw to achieve some goal"). Under this definition, how are romance scams *not* considered hacking? It is exploiting a technological flaw (namely, the lack of strong identification on the Internet) to achieve the goal of scamming people for money.

Ask: Is the lack of identity on the Internet a feature or a bug? (Probably a feature, but it still ends up being the source of many if not most of our security problems!)

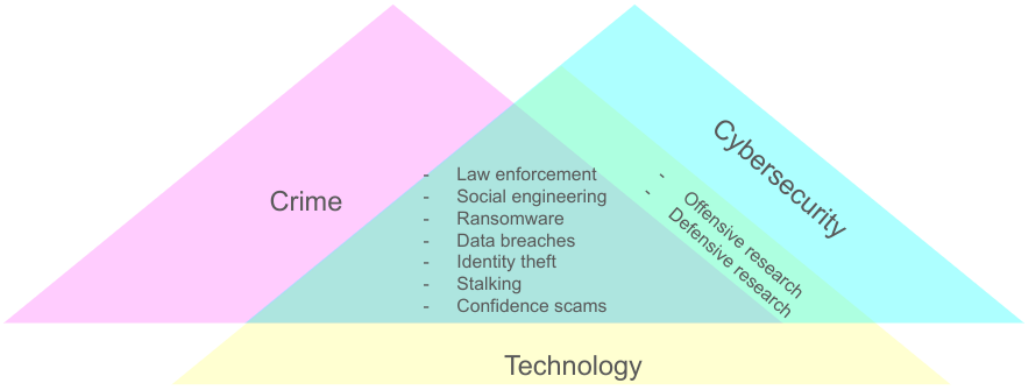


Figure 1: Maybe we should think of this topic like this

Activity: Have students list out some of the attacks mentioned in the papers. Ask students to define them. Write in form of table

Activity: For each attack, list out 1) who the attack targets (individuals, enterprises), and 2) what some reasonable defenses might be.

	Ransomware	**Investment**	**BEC**	**Ad fraud**	**...**
Cost (Sophos estimate)					
Cost (FBI estimate)					
Cost (Anderson et al. estimate)					
Who pays direct costs?					
Who pays indirect costs?					
Who pays defense costs?					
Other factors					

Sophos State of Ransomware 2023

- Who bothered to look up what Sophos was? Can someone explain? (Cybersecurity company. They sell network and endpoint security products like firewalls and endpoint detection. Website says they also do detection and response)
- What are some of the findings that confirmed your suspicions?
- What are some of the findings that countered your intuitions or were surprising to you?
- How was this data collected? (Survey of 13,000 cybersecurity leaders)
- What are some of the threats to the validity of this data? (Many ransomware events might go unreported)
- What are some of the issues with trusting reports from the cybersecurity industry on the state of cycbersecurity? (Incentive to oversell. Scare people into buying your product!)

Let's compare this to the other two works.

FBI Cybercrime Report 2022

- What is the IC3? *FBI's Internet Crime Complaint Center*
- What does the IC3 do? *Collect complaints, analyze threats and trends, raise public awareness, refer complainers to law enforcement agencies.*
- What are some of the findings in the FBI report that confirmed your suspicions?
- What are some of the findings the FBI report that countered your intuitions or were surprising to you?
- How was this data collected? (Complaints filed with the FBI's Internet Crime Complaint Center, or IC3)
- What are some of the threats to the validity of this data? (Underreporting)

Have Ina give an introduction of this paper. Ask her to point out the things in this paper, and the things that could be better.

Measuring the Changing Cost of Cybercrime

- What are some of the findings that confirmed your suspicions?
- What are some of the findings that countered your intuitions or were surprising to you?
- How was this data collected? (Gov reports, industry reports, victimization studies)
- What's the advantage of victimization surveys? (Statistically random sample, detect under-reported, etc.)
- What are some of the threats to victimization surveys? (Under-reporting)
- What are some of the threats to the validity of this data? (Relies on much of the same data, e.g. from the IC3. Also a bit older than the other two)

A Large-Scale Measurement of Cybercrime Against Individuals

Did anyone read this? Want to tell us what you learned?

An academic's version of the victimization surveys done by governments as cited in the Anderson et al. paper.

Concluding remarks/questions

- Question: Should the law enforcement community take a proportionate response to cybercrime based on the amount of harm done?
- Should the security community?
- Question: What do most of the attacks have in common? (social engineering)
- Question: What do most security researchers spend their time focused on? (Finding/patching vulnerabilities, researching new attack classes)
- Question: What do most of the reasonable defenses against the most common attacks have in common? (Social engineering—we can't rely on technology to save us!).
- **Security is a social problem with technical elements, not a technical problem with social elements!** No amount of research on clever attacks and defenses is going to change this fact.
- This brings up a very deep philosophical question: The lack of identification on the Internet is not a bug, it's a feature in most cases. It was a deliberate decision. How can you call it a flaw? (OK I concede, I'm motte-and-baileying this one). My point is that the difference between a technological flaw and a deliberate design decision is more or less a matter of perspective. C doesn't have memory safety. Is that a feature or a bug? Depends who you ask! DRAM cells are very tiny and can be perturbed. Feature or a bug? CPUs speculate unsafely. Feature or

a bug? Most web services still use passwords. Feature or a bug? It's a matter of perspective in many cases. The line between them is blurred in many cases.

- Problem: The feature-or-bug decision is usually decided by vendors, who may not have security as a top priority.
- How do we pick which party to be responsible for the cost? (As you can see, this really is a question of balancing costs! Doctrine papers help us here!)