The Economics of Cybersecurity — Lecture 12 Notes

Adam Hastings

April 9, 2024

1 Opening Discussion

- (Note on passing of Ross Anderson)
- Format/agenda of today:
  - Brief Lecture
  - Readings review group activity
  - Open discussion (on your homework!)
- *Why are we talking about policy and regulation and standards in a cybersecurity economics class?*
- (Regulation is about getting people or organizations to behave in a certain way—in a sense imposing a *cost* onto people—with the intention of improving the greater good. This is exactly in line with mechanism design, exactly in line with thinking about how resources and costs should be distributed and allocated—all classic economics problems. Some may disagree but I think it's an essential part of this course to cover this material).
- (Likewise, standards are generally created to improve the economy, believe it or not. We'll get into this later today).
-

2 Alphabet Soup

- ONCD — Office of the National Cyber Director
  - Mission: Advise President on matters of cybersecurity.
  - Part of Executive Branch
  - Since 2021
  - Goal is to shape and coordinate federal cybersecurity policy.
  - *What's the difference between policy and regulation?*

    * Policy is generally more about high-level principles, guidelines, or objectives with the intention of being used to aid decisionmaking. Can refer to government, but many times does not (a private company can have an internal cybersecurity policy on what to during a breach, for example). Kind of a loose word in my opinion.
    * Regulation are always enacted by a government (or some organization acting on the government's behest e.g. FINRA) and implies some level of satisfying requirements. (Example: GDPR in EU). Regulations are *binding* and *enforceable*. Often implemented in pursuit of achieving some policy.
  - Published National Cybersecurity Strategy
  - In case you think this is too much talk about government instead of economics: ONCD's mission is to "advance national security, **economic prosperity**, and technological innovation through cybersecurity policy leadership."

- CISA — Cybersecurity and Infrastructure Security Agency
  - Agency within the DHS (Deparment of Homeland Security, part of Executive Branch), whose mission is public security (things like anti-terrorism, border security, disaster response (FEMA), etc.)
  - Established 2018 (replaced older program)
  - Responsible for 1) ensuring federal cybersecurity, and 2) coordinating cybersecurity and infrastructure security programs within the US.
  - *Why does cybersecurity need coordination?* Central point for information sharing
  - Focused on improving the federal government's security but also the security of US companies and citizens.

- NIST — National Institute for Standards and Technology
  - Part of Department of Commerce
  - Formed in 1901
  - Make standards. *Ask: What's a standard?*
  - Example from their website: Firehoses and firehose fittings on fire hydrants are nationally standardized (in response to Great Baltimore Fire of 1904).
  - Standardizes many things
  - Reference Peanut Butter. Costs about $2000, *Why?* For testing laboratory equipment. Guaranteed to have an exact number of calories, protein, etc. so that food manufacturers can calibrate their equipment as part of food safety testing required by the FDA (Food and Drug Administration). (Example—NIST provides standards; NIST does not enforce standards!)
  - *Where is NIST big in cybersecurity (besides the NIST CSF)?* Cryptography! AES, SHA, RSA, DSA, ECDSA are all NIST standards. *Who knew this?* The standards describe exactly how the computation should be done. Even standards for how to generate random bits!
  - Current big thing is the move to Post-Quantum cryptography (Quantum breaks RSA!). Currently in final phase (about four remaining, doing more tests and getting input from cryptographers I suppose)

- Digression:
  - There are many, many standards in technology. Examples:
  - USB standard (USB Implementers Forum); Bluetooth (Bluetooth Special Interest Group); U2F/FIDO (FIDO Alliance); POSIX (IEEE); double-width precision floating points (IEEE)
  - These are not government bodies. Made up of self-interested companies.
  - *Why are some standards like cryptography standardized by the government while others are not?*
  - Is this conversation drifting away from economics? Not really. NIST was created specifically to improve our nation's industrial competitiveness. *Why are standards a good thing, economics-wise?*
  - *Why might they be a bad thing?* (Example: USB-C charger for European iPhones (starting Augst 2024). *May* reduce overall quality. *may.*)
  - *What is the difference between a standard and a regulation?* Standards are typically very precise, regulations are often less so. Is this a feature or a bug?
- To summarize: There are a number of different organizations that shape cybersecurity policy in the US. Explaining it all might feel like reading a dictionary or a list of facts, but I think it's good for you to at least know who the players are.
- There is clear interest in Washington in taking a more active hand in security. Unclear which agency this will come from...CISA does not pass regulations, and neither does NIST...maybe someone more keyed in would know what's happening behind the scenes (Jay Healy perhaps? Plug for his class!) Cybersecurity Strategy names NIST and CISA though when mentioning regulations.
- Some non-regulatory agencies in the US:
  - USCYBERCOM — United States Cyber Command
    - **NOT** a regulatory agency. Part of the US Military, operating under the Department of Defense. Mission: cyberwarfare.
    - Founded 2010
    - Created as a defensive force; Probably better seen as an offensive force (e.g. take down ISIS servers/disrupt operations)
  - NSA — National Security Agency (1952). Purpose: Obtain intelligence, cyrptanalysis, SIGINT, data collection, Snowden Leaks, et cetera.
  - FBI, CIA do intelligence gathering as well (CIA is more focused on human intelligence though, FBI is kind of like federal police. Neither going to have an impact in national cybersecurity.)

2.1 Terminology distinctions

How would we rank the following in terms of strictness? **Policy, regulation, standard, law**

I would rank policy → law → regulation → standard. *Don't* think of this as a hierarchy though—sometimes regulations are written to clarify laws, and laws are sometimes passed to enact policy, but don't think of this as an objective of going from policy to standard.

Who writes laws? Who write policy? Who write regulation? Why aren't they the same? Is it best this way? (Maybe—probably don't want a bunch of Senators who don't know how to print a PDF deciding cybersecurity policy. Best left to experts in non-elected positions (although this is controversial among certain political factions)).

3 National Cybersecurity Strategy

- **Type** *Is this a standard, regulation, or policy?* Policy.
- **Who** *Who wrote this?* ONCD
- **When** *When?* 2023
- **Goals** *What are the goals?* "But the underlying structural dynamics of the digital ecosystem frustrate [cyber defenders'] efforts" (sound familiar?)
- **Mandatory?** *Is it mandatory? To whom?* No. High-level policy. Hint of regulations to come.
- **Cost?** *What are the costs of implementation and who pays them?* n/a
- **Beneficiaries** *Who is this designed to help?* Entire digital ecosystem.
- **Subjects** *Who does this regulation affect?* More emphasis on dismantling **threat actors**, more burden on technology providers and operators (including software vendors, IoT vendors,), less on **end users**; **NIST, CISA** likely involved at some point; **Law enforcement** (FBI/CISA Joint Ransomware Task Force), Internet standards organizations, industry leaders, international allies, academic institutions (grants/funding), nonprofits, consumer interest groups. Everything under the sun.
- **Implementation** *Is there a correct implementation? What does a successful implementation look like/How do we know when this document is being adhered to correctly?*
- **Evaluation** *How do we evaluate how effective it is?* Entire section on implementation! "Measure investments made, progress towards implementation and ultimate outcomes and effectiveness of these efforts" Perfectly vague right? Will report annually to President, Assistant to the President for National Security Affairs, and Congress.
- **Weaknesses** *What are the weaknesses/Why might this not achieve its stated goal? Can it be gamed?* I don't know. *Are there perverse incentives?* I don't know (yet).
- **Other**

4 NIST Cybersecurity Framework

- **Type** *Is this a standard, regulation, or policy?* "Framework" technically, I would list is as a policy. But a desired policy for *end organizations*, **not** the federal government.
- **Who** *Who wrote this?* NIST, obviously.
- **When** *When?* Version 1.0 in 2014. Version 2.0 in February 2024!
- **Goals** *What are the goals?* Guidance to industry, government agencies, and other organizations to manage cybersecurity risks. Identify and manage risk. *Describes* outcomes without specifying how to achieve them. (Do we see how this is different from a regulation or a standard?)
- **Mandatory?** *Is it mandatory? To whom?* To government agencies and contractors as well, I believe.
- **Cost?** *What are the costs of implementation and who pays them?* Paid by organization itself. Will (hopefully) produce positive externalities though. Costs are the cost to "Identify, Protect, Detect, Respond, Recover, and Govern" cybersecurity risk. Each of these are taxonomized into categories and subcategories.
- **Beneficiaries** *Who is this designed to help?* The organization itself that is implementing it.
- **Subjects** *Who does this regulation affect?*
- **Implementation** *What does a successful implementation look like/How do we know when this document is being adhered to correctly?* Some of the subcategories are pretty clear, e.g. "ID.AM-01: Inventories of hardware managed by the organization are maintained" or "PR.AA-03: Users, services, and hardware are authenticated". Les clear is "DE.CM-01: Networks and network services are monitored to find potentially adverse events". Doesn't specify "how much" or how much you ought to spend. When is enough enough?
- **Evaluation** *How can we evaluate the efficacy of this? Is that even possible?*
- **Weaknesses** *What are the weaknesses/Why might this not achieve its stated goal? Can it be gamed?* No reason to game it if it's for your own benefit. *Are there perverse incentives?* Perhaps, if it becomes more mandatory. Companies could spend time and money on "security theatre"—making a visible effort to make the auditors happy without actually improving anything (and wasting money in the end).
- **Other** *Other:*

5 ENISA Cyber Resilience Act

- *Is this a standard, regulation, or policy?* A regulation.
- *Who wrote this?* European Union Agency for Cybersecurity (ENISA) (How that acronym works—I don't know...). Maybe best thought of as analogous to CISA in the US. Also included input from various member state cybersecurity agencies, hardware and software manufacturers, importers, trade associations, citizens, academics via a series of workshops.

- *When?* Proposed in 2022. Amends 2019 regulation I think. Still being approved. Last I checked it was approved by the Eurpoean Parliament in March 2024 and now requires adoption by the Council of the European Union before it's enforced. I don't know what these organizations are or what they do but from what I can tell it sounds like this is going to be European law.

- *What are the goals?* (1) create conditions for the development of secure products with digital elements, by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and (2) create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. (*What's the economics name for #2?* Reducing information asymmetry)

- *Is it mandatory? To whom?* "All products with digital elements whose intended and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network" — super broad!!

- *What are the costs of implementation and who pays them?* Listed out in the Articles of the regulation, which I only made you skim. Easy to identify where the costs are; hard to tally them up. Example: Cost of including technical documentation with a product (Article 23); others harder to know a priori ("be delivered in a secure default confirguration" — how to verify?)

- *Who is this designed to help?* End users mostly.

- *Who does this regulation affect?* Software and hardware vendors.

- *What does a successful implementation look like/How do we know when this document is being adhered to correctly?* Should adhere to Annex I (perhaps look through). Specific yet vague! E.g. "be designed to limit the attack surfaces, including external interfaces"

- *How can we evaluate the efficacy of this? Is that even possible?* Did a public consultation to rank measures; There is a EU Guideline for determining effectiveness, efficiency, relavance, (didn't read it); Commission will "monitor" and issue public report (misaligned incentives perhaps?)

- *What are the weaknesses/Why might this not achieve its stated goal? Can it be gamed?* Security theatre, perhaps. *Are there perverse incentives?* Security theatre, perhaps.

- *Other:*

  - "the standardisation process that will follow would take into account the technical specificities of the products". Thoughts on this? Scary?