How to Get a Cyber NTSB

Steven M. Bellovin
https://www.cs.columbia.edu/~smb

Why?

- We need to know what practices or defenses have failed
- We need to know what has worked
- Defenders need it, insurance companies need it, regulators need it

Goals

- As much information on major breaches as possible
- As much information on near misses as possible
- Sooner rather than later
- But some information now may be better than more information later

An NTSB Analog

- Difficult—this is a deregulatory era
- But: it has worked extremely well for aviation
- Are lives at stake? With the Internet of Things, increasingly so.
  - What happens if self-driving cars are hacked?
  - What about the power grid during the winter?
  - What about air traffic control networks
- The best solution, if we can get it
- And if we can't?

Sector-Specifc Regulators

- Health and Human Services, for the health sector
- Department of Education, when enforcing FERPA
- FCC, for telcos and ISPs

The FTC

- The FTC has authority over deceptive or unfair trade practices that harm consumers
- It has frequently used this for privacy harms—but what about other harms, e.g., via cyberphysical system hacks?
- FTC consent decrees often require things like 20 years of auditing—perhaps full disclosure is a more important remedy

The SEC

- The SEC has strong regulatory authority over the financial sector
- It has been paying more attention to internal cyber practices
- In event of an avoidable breach, where Boards did not exercise due diligence, could it mandate disclosure in lieu of other penalties?

Voluntary Cyber Safety Reporting System

- A voluntary system, analogous to the aviation scheme
- Avoids regulatory issues
- Grant forbearance to companies that do report voluntarily
    - FTC sanctions
    - State attorney-general actions
    - But what about civil liability?

Possible Strategy

- Try for an NTSB analog—it's what we really need
- Unless and until it happens, ask existing regulatory bodies to do their part
- In parallel, set up a voluntary scheme and try to get buy-in on forbearance

Questions?

(these slides at https://www.cs.columbia.edu/~smb/talks/why-ipsec.pdf)