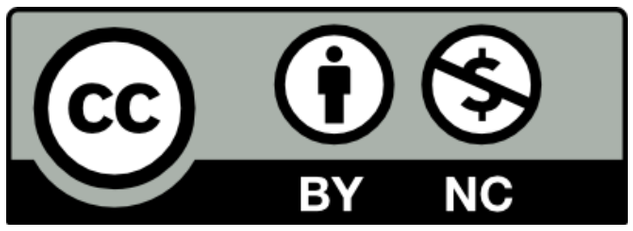
Investigating Cyber Incidents

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



“If You Can Not Measure It, You Can Not Improve It.”

“When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of *Science*, whatever the matter may be.”

—Lord Kelvin, 1883

We Can't Measure Security

- Are firewalls better or worse than antivirus?
  - Do either of them actually help?
- How about intrusion detection systems?
- If it costs *x* times more to develop (or purchase) more secure software than run-of-the mill stuff, is it worth it, compared to the cost of cleanup after an incident?

We don't know—and that's a problem.

The Market

- Hypothesis: if allowed to—e.g., if there weren't problems of restrictive EULAs, etc.—the market will solve our security problems
  - Observation: when companies face that sort of loss potential, they want to buy insurance
  - Observation: insurance works better if rates are coupled to risk
  - Observation: we don't know what's risky and what isn't
- Even without insurance, a market solution that won't simply be random requires that *someone* know how to reduce risks
- Conclusion: we don't have enough data for the market to work

Apache Struts

- Equifax was hacked, to the tune of 150 million people's personal information, due to a recently disclosed bug in Apache Struts.
- It was an annoying bug to fix—but no other major company was hit that hard.
- Why not? We don't know.

Machine Learning

- Let’s turn ML loose on the secure operations problem
- Find out what successful companies did right that hacked companies didn’t do
- But: ML requires *data*, for failures *and* for sites that fended off the attack

Airplanes

- In 2008, a plane crashed because of a combination of:
  - A design flaw
  - A failed relay, causing a heater failure
  - A failure to diagnose the problem, which led to
  - The mechanic declaring the plane safe to fly
  - A phone call to the copilot
  - An extra person in the cockpit
  - The takeoff checklist not being used
  - The slats not being set properly
  - A warning system not functioning because it relied on the same relay

But computer systems seem to be hackable if you so much as look at them sideways. What's the difference?

Data!

- *All* airplane crashes are investigated
- Pilots and other personnel can report near misses
- All of this data is used, by manufacturers, pilots, regulators, and more
- In aviation, people learn from mistakes
- In aviator, people *can* learn from mistakes, because the data is available
- In cybersecurity, it isn't—and that's a problem

What We Need

- A voluntary reporting system for near misses, akin to the Aviation Safety Reporting System
- A Federal agency that can compel cooperation in investigations of major security incidents
- *Public reports about the root causes*
- *A public database that can be queried, analyzed, etc.*

Questions?

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