Cyber NTSB

A History…

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

CS@CU

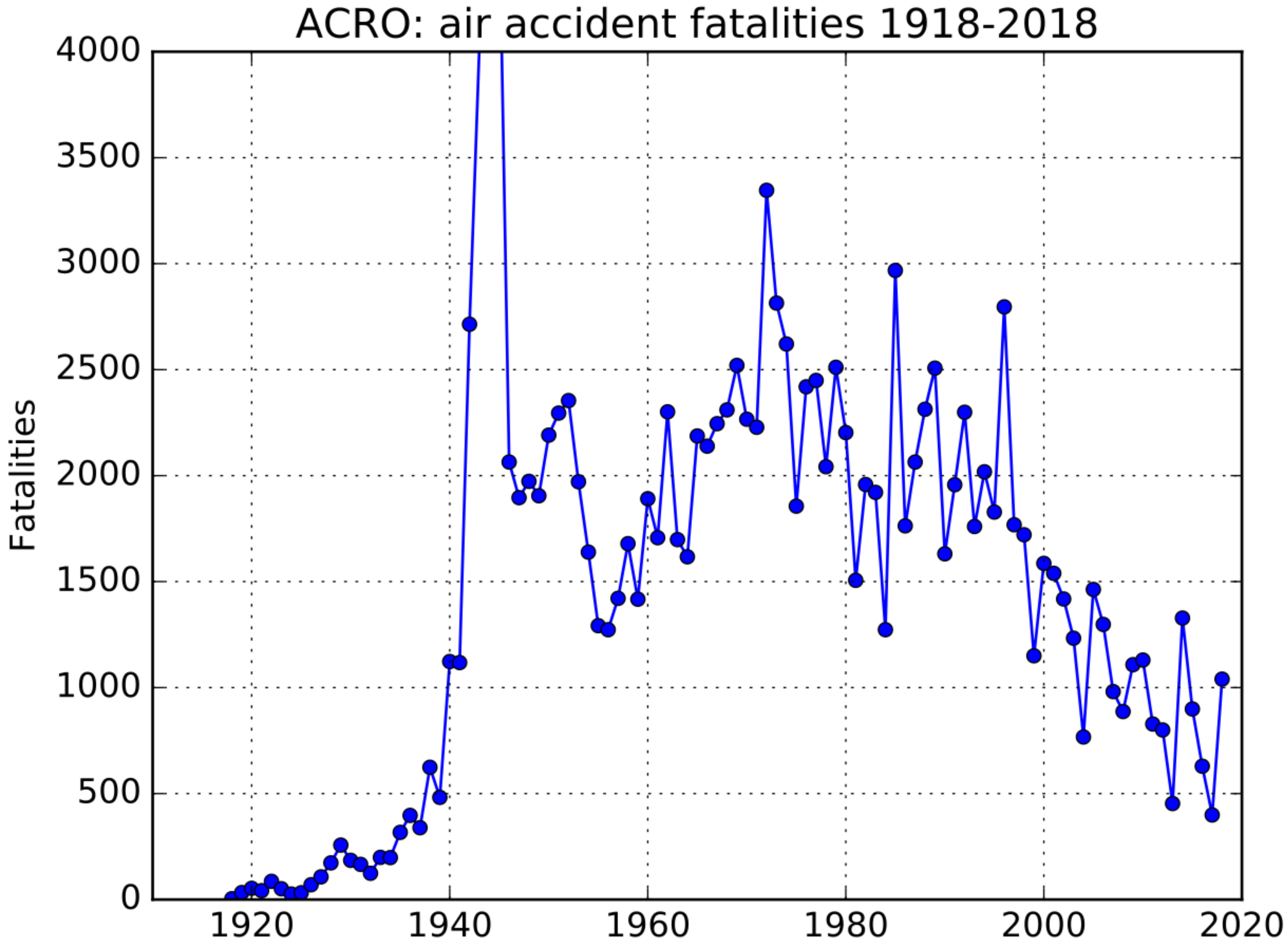
Contemplate…

Photo: Library of Congress:
https://www.loc.gov/resource/pppprs.00626

Manhattan, 29 December 2018

A Long History

- Aviation was originally very dangerous
- It’s improved a lot
- Why?



Copyright 2019, Geek3
https://en.wikipedia.org/wiki/File:ACRO_fatalities.svg

Why?

- Investigations of crashes
    - The NTSB’s ancestor was formed in 1926
- Knowledge of the root cause
    - Knowledge of contributing factors
- Changes in design, construction, process
    - Mandated by law and regulation

Why?

- Investigations of crashes
- Knowledge of the root cause
    - Knowledge of contributing factors
- Changes in design, construction, process
    - Mandated by law and regulation

Especially in recent years, plane crashes rarely have one cause. You need <u>detailed</u> knowledge of <u>all</u> of the contributing factors—and all of these <u>must</u> be dealt with.

Near Misses

- Often, if not everything goes wrong, there won’t be an accident—but there might have been

- Aviation personnel who notice these close calls are encouraged to report them

- Learn from near misses, too, and prevent future accidents

The Cyber World

- When there’s a security incident, we rarely know all of the details
- (Many penetrations are never even noticed…)
- Companies often try to hide the details and even the incident
- They rarely supply all of the important details, including where internal defenses protected parts of the enterprise
- We almost never hear about near misses, what went right and what went wrong

The Home Depot Hack

“Criminals used a third-party vendor's user name and password to enter the perimeter of Home Depot's network, the company said in a statement. These stolen credentials alone did not provide direct access to the company's point-of-sale devices, but the hackers then acquired elevated rights that allowed them to navigate portions of Home Depot's network and to deploy unique, custom-built malware on its self-checkout systems in the US and Canada.” (Infosecurity, 7 November 2014)

- Which third party? (Was it involved in other breaches?)
  - Was that password per-individual or for the company?
- How were “elevated rights” acquired?
- Were there security barriers to the self-checkout systems? If so, how did they fail?
- What “portions” of the Home Depot net were not accessible to the attacker? Why?
- What information did the attackers need to create “custom-built malware”?

Obstacles to a Cyber NTSB

- Incidents are often invisible unless self-reported
- Reluctance to disclose details
    - Proprietary data
    - Shame?
    - Inform the next attackers?
- Liability
- Airplanes of a given model are much more similar than data centers—difficult to abstract the right details

But security people need details!

Questions?

Red-tailed hawk, Great Barrington, MA, 18 September 2020