A Cyber NTSB

What a National Cybersecurity Safety Review Board Can Learn from Aviation Safety

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

CS@CU

Contemplate…

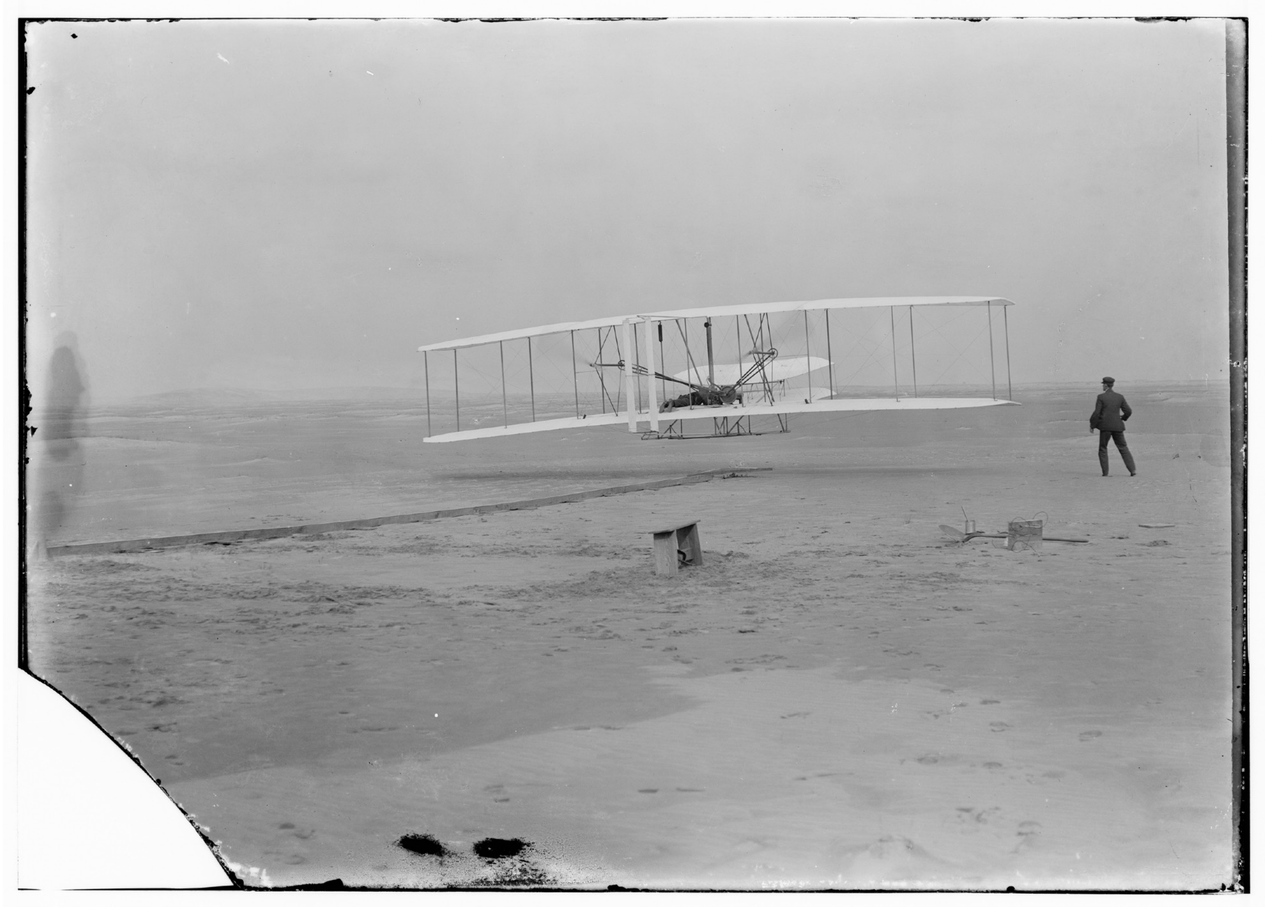
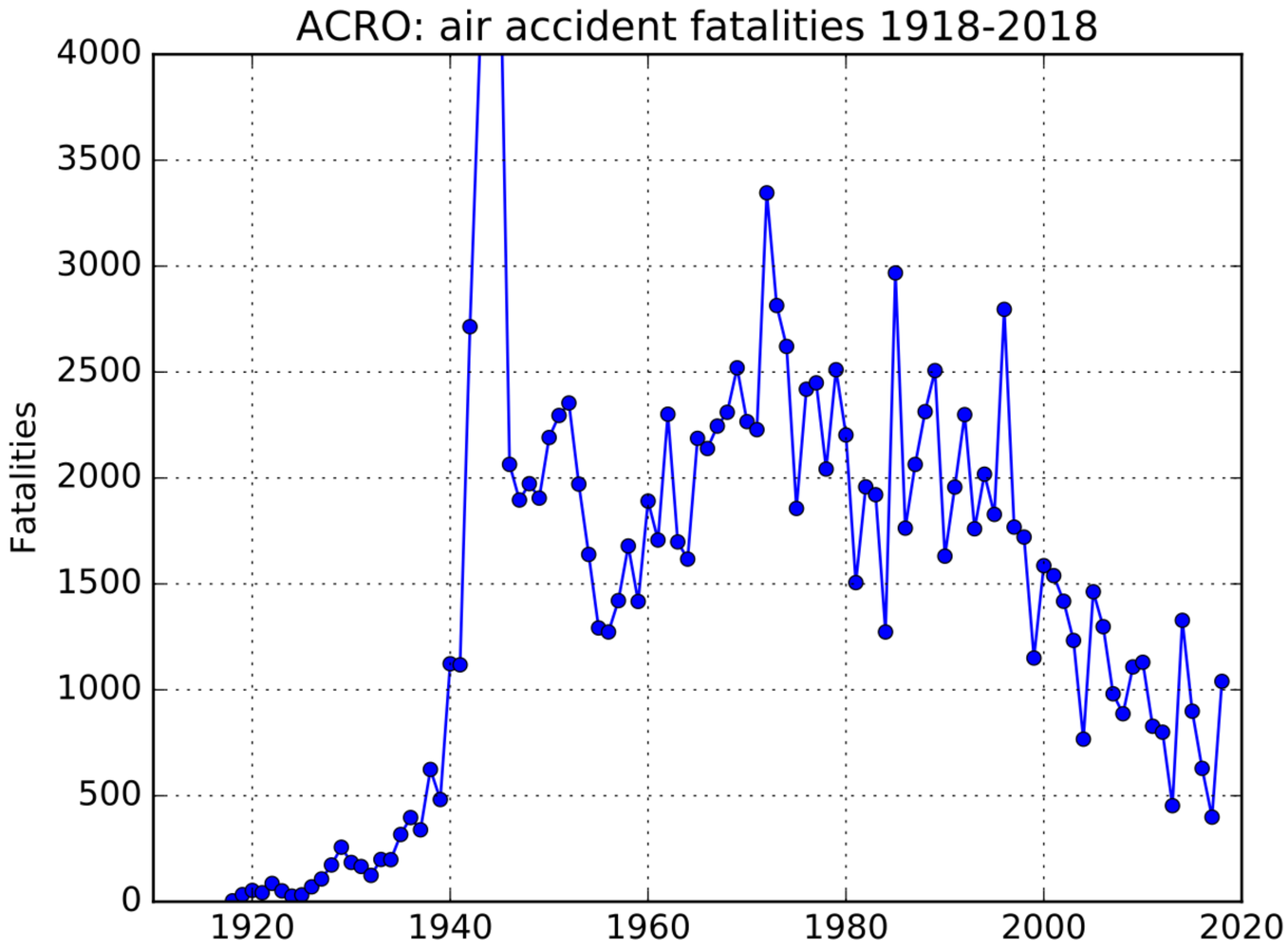


Photo: Library of Congress:
https://www.loc.gov/resource/ppprs.00626

Manhattan, 29 December 2018

A Long History

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



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 detailed knowledge of all of the contributing factors—and all of these must 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"?

Equifax

- Personal data on ~150M compromised
- The attackers exploited a known hole
- What happened?

What Happened?

First Approximation

- There was a serious security hole in Apache Struts, a web application-building tool
- A patch was released on March 7, 2017
- Struts-based systems were under heavy attack by March 9
- Equifax sent out an internal alert on March 9, requiring patch installation within 48 hours.
- They did an internal scan on March 15—but it didn't find the vulnerable machines.

What Happened?

First Approximation

- There was a serious security hole in Apache Struts, a web application-building tool
- A patch was released on March 7, 2017
- Struts-based systems were under heavy attack by March 9
- Equifax sent out an internal alert on March 9, requiring patch installation within 48 hours. Why was the alert two days late? Why was the vulnerable server not patched within 48 hours?
- They did an internal scan on March 15—but it didn't find the vulnerable machines. Why not?

Second Approximation

- When was Equifax penetrated?
- Access to sensitive data started on May 13 but wasn't detected until July 30.
- The attackers created about 30 web shells, which remained even after the Struts problem was patched.

Second Approximation

- When was Equifax penetrated? We don’t know. How did lateral movement take place? We don’t know.
- Access to sensitive data started on May 13 but wasn’t detected until July 30. Why wasn’t it detected sooner?
- The attackers created about 30 web shells, which remained even after the Struts problem was patched. Why weren’t these noticed?

Third Approximation

- Why didn’t the security group *know* which web servers existed, and based on which software?
- Why did it have to run an internal scan?
- Why did not not track acknowledgements from each group operating a web server?

Fourth Approximation

- This was not an easy vulnerability to patch. From Ars Technica, March 9:

  > The fix here, by contrast, typically requires each Web app that was developed with a vulnerable version of Apache Struts to be recompiled using a patched version.
  >
  > "Many of those apps may be essentially abandoned," Bright wrote. "The earliest affected version of Struts was released in October 2012, and I bet that there's plenty of apps developed since then that are 'finished'. They're still used and deployed, but they're not receiving ongoing maintenance; their developers have moved on to other projects, or even other companies."
  >
  > It's an interesting explanation and one that suggests it could take weeks or months for this bug to be fully extinguished.

- *Why did an IT-intensive company like Equifax rely on such hard-to-maintain technology?*

CS@CU

We Need Details

- We need a deep dive to understand *all* of the contributing factors to an incident
- Ordinary incident investigations won't get us there, even if they're made public—and they generally are not

By Contrast

- 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, given the weather that day
  - 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

We know all of this because of an accident investigation

Near Misses

- A Cyber NTSB tells us what has failed
- Often, though, we want to know what has worked
- In other words: what defenses successfully thwarted an attack?
- We need a near-miss reporting system

The Aviation Safety Reporting System (ASRS)

- In aviation, anyone in the system—pilots, air traffic controllers, ground crews, *anyone*—can file a report about a near miss
- The ASRS is run by MITRE under contract to NASA, *not* the FAA
- Initial reports are not anonymous—the person accepting the report (a late career aviation professional) can request clarifications, details, etc.
- The eventual published reports are anonymized; not even the airline is identified

The Cyber Safety Review Board

- In May, President Biden signed executive order 14028 creating the *Cyber Safety Review Board*
- Part of DHS
- Charged with investigating significant incidents in Federal civilian and critical infrastructure systems
- Reports to the Secretary of DHS to “provide recommendations … for improving cybersecurity and incident response practices”
- A good start, but not enough

What's Needed in a CSRB

(Taken from a Lawfare essay by myself and Adam Shostack)

- As objective as possible: what happened and what conclusions can be drawn
- *Not* reverse-engineering malware; not about evidence for prosecutions
  - Leave those to the IC and the FBI
- Not about finger-pointing
  - NTSB reports cannot be used in disciplinary or civil court proceedings
- Needs in-house expertise
- Must be independent of a regulatory agency—the regulations themselves may be at fault
- *Published* reports that get at root causes, including non-technical issues

What's Needed in a Near-Miss Reporting System

- Voluntary, as in the ASRS
  - Avoid regulatory issues
- Grant forbearance to companies that do report voluntarily
  - Avoid FTC, etc., sanctions
  - Get buy-in from state attorneys-general
  - But what about civil liability?

Getting There

- We could start small, with sector-specific CSRBs and CSRSs
  - The FCC, for telcos and ISPs
  - Department of Education, for FERPA-related incidents
  - HHS, for the health sector
  - The NHTSA, for automotive security issues
  - Etc.
- The SEC could use its authority: breaches represent material risks to investors
- The FTC already has jurisdiction over some incidents—could it mandate published reports as part of a remedy?

Obstacles to a Cyber NTSB/ASRS

- 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 we need the data!

Readings

- *The major cyberincident investigations board. IEEE Security & Privacy, 10(6):96, November--December 2012.*
- *Steven M. Bellovin and Adam Shostack. Input to the Commission on Enhancing National Cybersecurity, September 2016.*
- *Jonathan Bair, Steven Bellovin, Andrew Manley, Blake Reid, and Adam Shostack. That was close! Reward reporting of cybersecurity "near misses". Colorado Technology Law Journal, 16(2), 2018.*
- *Steven Bellovin and Adam Shostack. Finally! A cybersecurity safety review board. Lawfare, June 7, 2021.*

Questions?

Great blue heron, Rock Creek Park, May 26, 2019

CS@CU