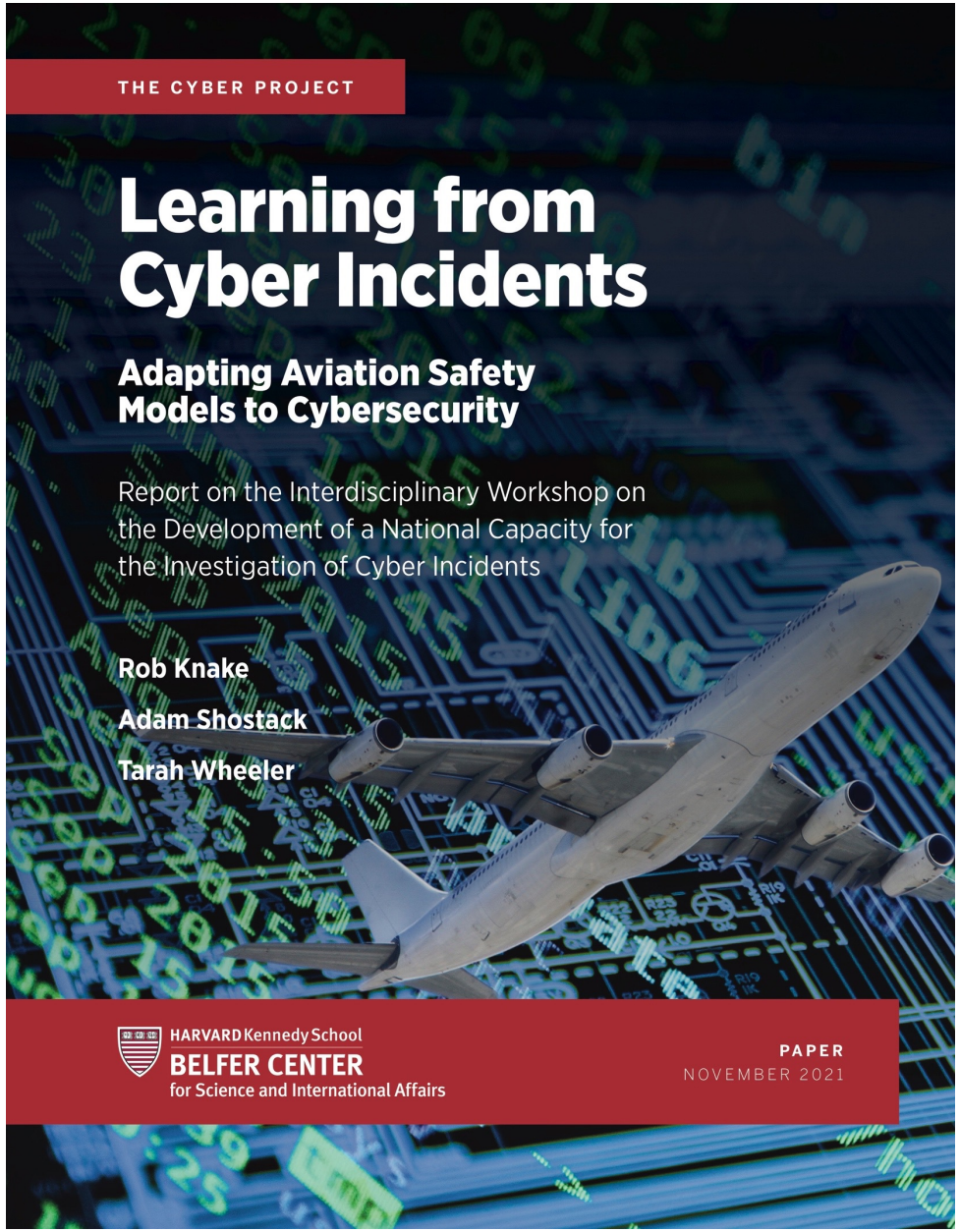
Learning from Cyber Incidents: Adapting Aviation Safety Models to Cybersecurity

Papers We Love: JIT Winter Revival

December 14, 2021

John Benninghoff


THE CYBER PROJECT
Learning from Cyber Incidents
Adapting Aviation Safety Models to Cybersecurity
Report on the Interdisciplinary Workshop on the Development of a National Capacity for the Investigation of Cyber Incidents
Rob Knake
Adam Shostack
Tarah Wheeler
HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs
PAPER
NOVEMBER 2021

The Authors

Robert Knake

- Director, Cyber Lessons Learned
- Non-Resident Fellow, Cyber Project

Expertise: Cyber Security

Bio/Profile
Email
More by this author
@robknake
LinkedIn

Adam Shostack

- Co-Director, Cyber Lessons Learned

Expertise: Cyber Security

Bio/Profile
More by this author
LinkedIn
Website

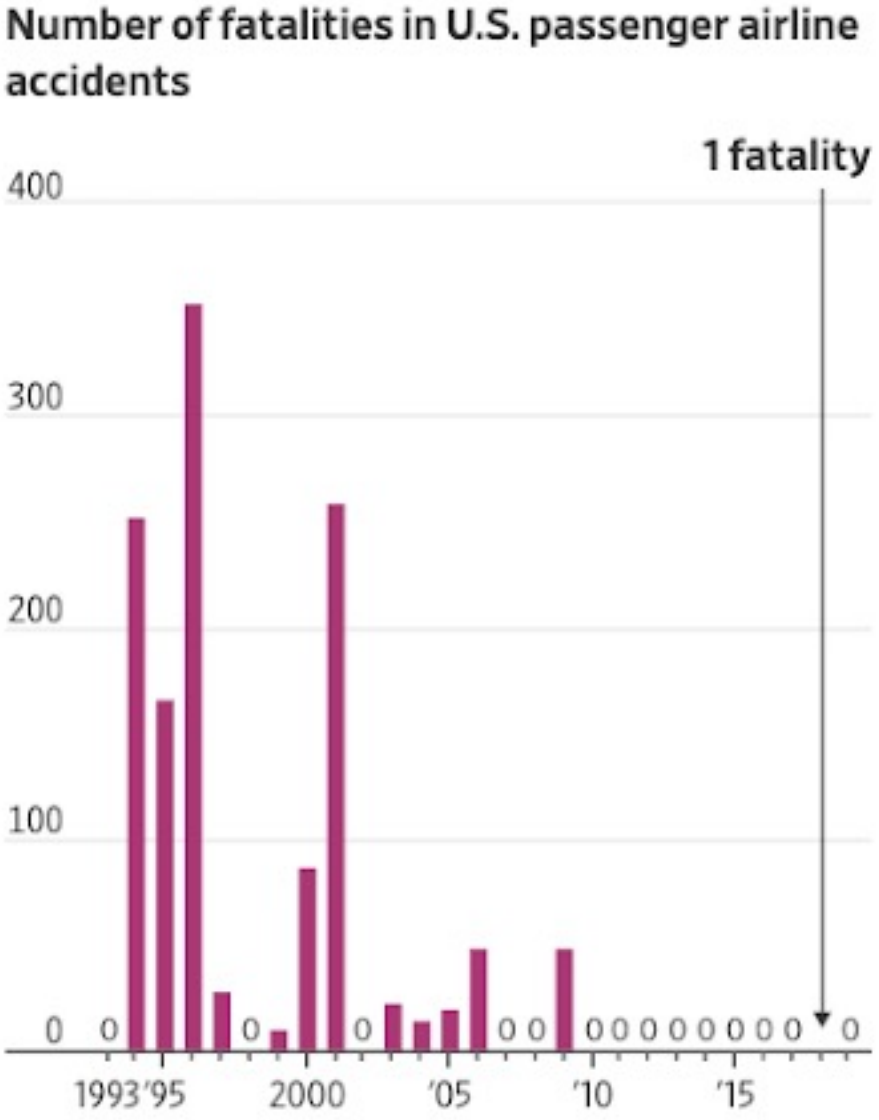
Tarah Wheeler

- Non-Resident Fellow, Cyber Project

Expertise: Conflict & Conflict Resolution, Economics & Global Affairs, Trade, International cooperation, European studies, International Relations, U.S. foreign policy, United Nations, NATO, Globalization, International Security & Defense, Security Strategy, Science & Technology, Cyber Security, Information technology, Science & Technology Policy

Bio/Profile
Media Inquiries
More by this author
@tarah
Website

Why even do this?



Note: Excludes terrorist acts and fatalities on the ground

Source: Based on industry and U.S. government data

Methodology

- Conducted a virtual workshop in nine sessions over four months in spring 2021
- Included presentations by NTSB and other experts from government, law, academia, and security practitioners
- David Woods led a session on ‘Learning from Other Domains’

Appendix A: Workshop Program

Date	Time	Session
March 18, 2021	3:00 pm	**Session 1: Opening Session**
March 25, 2021	3:00 pm	**Session 2: What Does the NTSB Actually Do?** Chris Hart, Former Chair, NTSB
April 1, 2021	3:00 pm	**Session 3: Plenary Discussion**
April 8, 2021	3:00 pm	**Session 4: Learning from Other Domains** David Woods, Ohio State University
April 15, 2021	3:00 pm	**Session 5: Plenary Discussion**
April 22, 2021	3:00 pm	**Session 6: ASRS and Near Misses** Becky Hooey, ASRS
April 29, 2021	3:00 pm	**Session 7: The Role of Insurance** Tom Finan, Marsh Erin Kenneally, Guidewire Bryan Hurd, Aon
May 6, 2021	3:00 pm	**Session 8: Legal Issues** Evan Wolff, Crowell & Moring John Woods, Baker McEnzie
June 24, 2021	3:00 pm	**Session 9: Report Review**

Findings

1. Third party and in-house investigations are no substitute for objective, independent investigations
2. Companies are unlikely to fully cooperate under a voluntary regime
3. Product, tool, and control failure must be identified in an objective manner
4. Findings may be sensitive but should be disseminated as widely as possible
5. Fact finding should be kept separate from fault finding
6. “Near Miss” reporting can complement incident investigations

Practical Takeaways

- A recurring theme is discussion of blame, and how NTSB specifically avoids assigning liability in accident investigations; adopt the ‘blameless post-mortem’ approach and ‘Just Culture’
- There are domain-specific challenges unique to Security; don’t blindly copy what works in aviation safety
- Near Miss reporting is an important complement to incident investigation; share stories of the close calls

Conclusion

“Secret knowledge is mysticism, not science or engineering. We heard a great deal in our workshop about how various groups have access to useful data which drives decisions that they believe are good. Yet the decisions they come to are different, which has a cost both to those trying to comply with the advice, and in the credibility of the advice. There are certainly challenges: informing opponents, ranging from threat actors to lawyers, of what you know can be worrisome. Subjecting one’s reasoning to criticism is scary. It is also a constant in fields with high rates of engineering success, ranging from bridge building to medical device manufacture. The consequences for leaving the field of cybersecurity in a prolonged adolescence are now too great; it’s time for us to grow up.”

Questions and Discussion

References

- Paper: https://www.belfercenter.org/publication/learning-cyber-incidents-adapting-aviation-safety-models-cybersecurity
- Safety of Work, https://safetyofwork.com
- Verica VOID: https://www.verica.io/blog/announcing-the-void/
- Adaptive Capacity Labs: https://www.adaptivecapacitylabs.com
- Dekker (2017), “Rasmussen's legacy and the long arm of rational choice” https://sidneydekker.com/wp-content/uploads/2017/09/RasmussenLongArm.pdf
- LFI: https://www.learningfromincidents.io
- Etsy ‘blameless postmortems’: https://extfiles.etsy.com/DebriefingFacilitationGuide.pdf
- Adam Shostack Blog post: https://shostack.org/blog/cyber-lessons-learned/
- Just Culture: https://flightsafety.org/files/just_culture.pdf