PHYS.ORG

How airplane crash investigations can improve cybersecurity

February 22 2018, by Scott Shackelford

Credit: AI-generated image (disclaimer)

While some countries struggle with safety, U.S. airplane travel has lately had a remarkable safety record. In fact, from 2014 through 2017, there were no fatal commercial airline crashes in the U.S.

But those years were fraught with other kinds of trouble: Security breaches and electronic espionage affected nearly every adult in the U.S. , along with the power grid in Ukraine and the 2016 U.S. presidential campaign, to name a few. As a scholar of cybersecurity policy, I think it's time that my own industry took some lessons from one of the safest high-tech transportation methods of the 21st century.

Like today in cybersecurity, the early days of U.S. air travel weren't regulated particularly closely. And there were a huge number of accidents. Only after public tragedies struck did changes occur. In 1931, a plane crash in Kansas killed legendary Notre Dame football coach Knute Rockne. And in 1935, U.S. Sen. Bronson Cutting of New Mexico died in the Missouri crash of TWA flight 6. These events helped contribute to the 1938 creation of the first U.S. Air Safety Board. But it took until 1967 for the new Department of Transportation to be created with an independent National Transportation Safety Board.

Since then, the NTSB has rigorously investigated all airplane crashes and other transportation incidents in the U.S. Its public reports about its findings have informed changes in government regulations, corporate policies and manufacturing standards, making air travel safer in the U.S. and around the world.

As cybersecurity incidents proliferate around the country and the globe, businesses, government agencies and the public shouldn't wait for an inevitable disaster before investigating, understanding and preventing these failures. Nearly a century after the original Air Commerce Act in 1926, calls, including my own, are mounting for the information industry to take a page from aviation and create a cybersecurity safety board.

The flight plan to safer skies

The creation of the National Transportation Safety Board was the first independent agency charged with investigating the safety of various transportation systems, from highways and pipelines to railroads and airplanes. Since 1967, the NTSB has investigated more than 130,000 accidents.

These investigations are vital since they help establish "the who, what, where, when, how and [perhaps] why behind an incident." After the facts are determined, policymakers can back up, and often have backed up, NTSB recommendations with new regulations. Failing that, it is common for air carriers, for example, to voluntarily implement changes it suggests. A similar approach could help improve the internet, a new technology that, like airplanes, is tying the world closer together even as it threatens our shared security.

The case for a cybersecurity safety board

Two elements of the NTSB may be particularly useful for enhancing cybersecurity. First, it separates fact-finding proceedings from any questions of legal liability. Second, these investigations are broad, involving various stakeholders like manufacturers and airline companies. Cyberspace is similarly made up of a wide range of companies and technologies.

A cybersecurity safety board need not in fact be national. It could begin from the bottom up, with companies partnering together to protect their customers by sharing best practices.

Critics of establishing a cybersecurity safety board would likely contend that the speed at which technologies change makes it difficult for any recommendations, even if they were quickly implemented, to sufficiently protect organizations from cyber attacks. NTSB investigations can take a year or more; to ensure findings were still relevant, cybersecurity inquiries would need to be faster, such as by streamlining cyberforensics and relying on widely used tools such as the

National Institute for Standards and Technology Cybersecurity Framework.

Other challenges include standardizing terminology across the industry and identifying the right experts to look into data breaches, which might be easier said than done given the talent shortage among cybersecurity professionals. Broad-based cybersecurity educational programs, like a new partnership between the law, business and computer science schools here at Indiana University, should be encouraged to help address this shortfall.

A path forward

Additional measures would likely be required to make a cybersecurity safety board successful, such as launching investigations only for serious breaches like those involving critical infrastructure.

More nations and regions – including the European Union – are imposing stringent requirements on companies that suffer data breaches, including mandatory reporting of cyberattacks within 72 hours and more rigorous preventive measures. Businesses, governments and scholars around the world are working on how to improve data security. If they came together to support a global network of cybersecurity safety boards , their efforts could promote cyberpeace for people and institutions alike.

All that is needed is the will to act, the desire to experiment with new models of cybersecurity governance and the recognition that we should learn from history. As President Franklin D. Roosevelt famously said, "It is common sense to take a method and try it: If it fails, admit it frankly and try another. But above all, try something."

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How airplane crash investigations can improve cybersecurity (2018, February 22) retrieved 9 April 2024 from https://phys.org/news/2018-02-airplane-cybersecurity.html