DOI:10.1145/3475165

Article development led by acmqueue
queue.acm.org

Why we need an IT accident investigation board.

BY POUL-HENNING KAMP

What Went Wrong?

IN APRIL, 39 postmasters and sub-postmasters were cleared of wrongdoing by a court in the U.K. after being accused and sentenced for various forms of fraud and, in some cases, serving multiyear prison sentences.[a]

In total, around 700 people have been prosecuted based on the "evidence" from a single IT system installed by the U.K. Post Office, and while some of them probably did embezzle money, it looks like the majority did not. They were sentenced based on evidence from an IT system, which ... ehhh ... to be honest, we don't know what that IT system did, except we know it did it really, really badly.

a https://www.bbc.com/

Press reports have contained various mumblings and hand-waving about the shortcomings of the IT system, but nobody sat down and documented precisely what went wrong and what can be learned from it so that nobody ever makes a mistake like this again.

Had this been a ship sinking, a train derailing, or a plane crash, one of the U.K.'s official accident investigation boards would have come in and written a report everybody would be allowed to read, explaining what went wrong and how to avoid it ever happening again. But because no ships, trains, or airplanes were involved, there will be no such report.

For well over a decade, I have been arguing that governments should create IT accident investigation boards for the exact same reasons they have done so for ships, railroads, planes, and in many cases, automobiles.

Denmark got its Railroad Accident Investigation Board because too many people were maimed and killed by steam trains, and it has kept the board around because a thousand tons of steel hurtling along at 180km/h, just below a 25kV power line, can do a lot more damage than a steam locomotive with wooden wagons ever could.

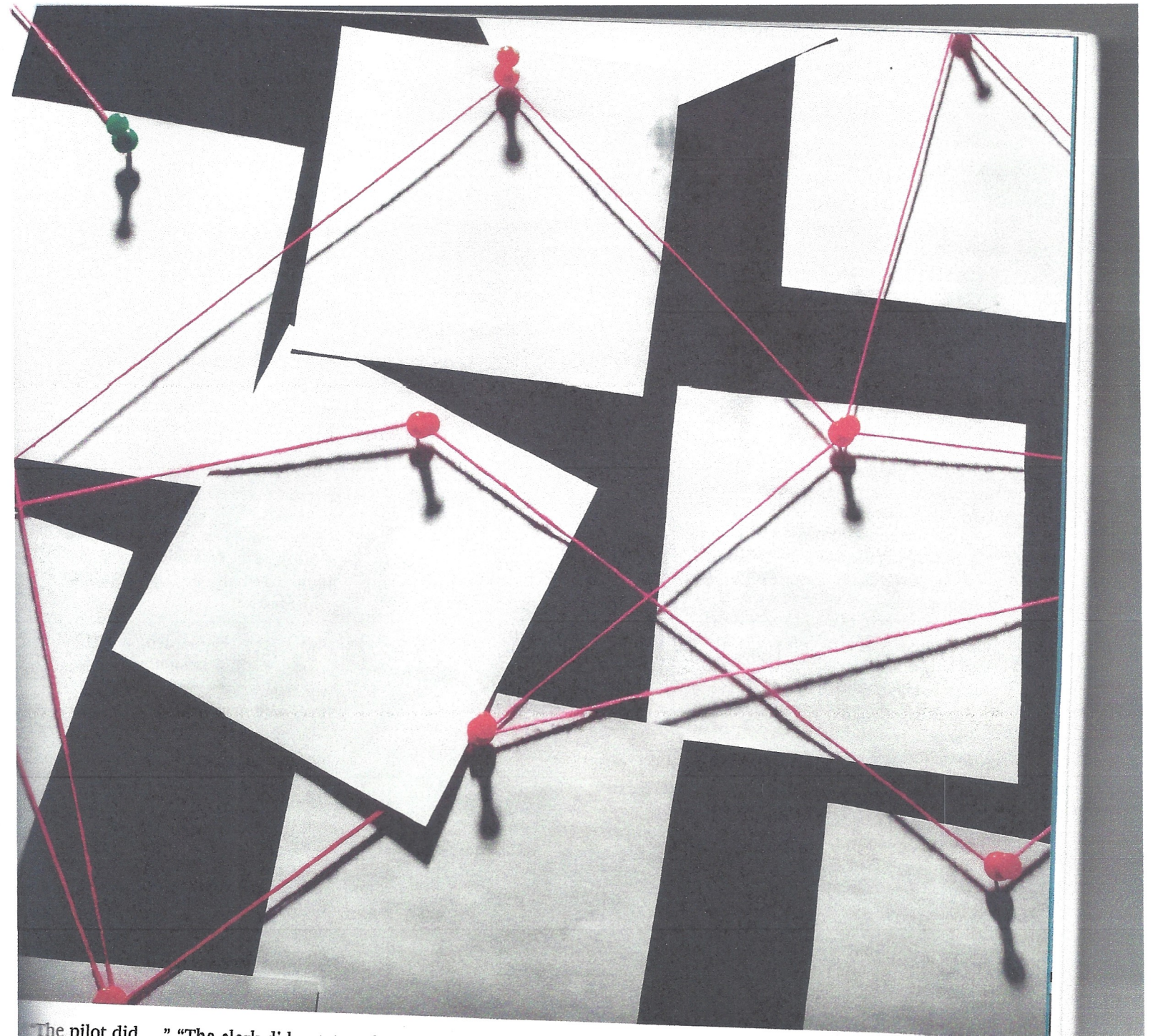
The U.K.'s Air Accidents Investigation Branch was created for pretty much the same reasons, but, specifically, because when the airlines investigated themselves, nobody was any the wiser.

Does that sound slightly familiar in any way?

The crucial feature of any accident investigation board is that it focuses only on what went wrong and how to avoid it happening again, and not on whom to blame.

Sometimes the board may find out that somebody failed to do something crucial, did something illogical, or even did something stupid, but that information is published only if it is necessary to prevent the same type of accident from happening again.

As far as I have seen, the information is relayed in impersonal terms



The pilot did ...," "The clerk did not ..."), because it is not important who that person was; what is important is that no other person exacts that consequence again.

There are three kinds of incidents an IT accident investigation board should look into:

- when an IT system is involved in loss of life, limb, or liberty;
- when development of an IT system fails spectacularly; and
- when an IT system leaks personal information.

The first point is a matter of consistency. Two Boeing 737 MAX airplanes crashed because of IT systems, and because those IT systems happened to be installed in airplanes, we get reports, whereas we get no reports about the U.K. Post Office's IT problem because its system was bolted into 19-inch racks.

That makes no sense: The human toll caused by both IT accidents is way beyond anything any civilized society can just let pass.

The second point is a matter of sound fiscal policy. Denmark, like all other countries, has an abysmal track record with development of governmental IT systems. Millions, and in some cases billions, in tax money pour into projects that almost invariably run late, over budget, fail to deliver, and so on.

But nobody is being paid to—or given sufficient access to—write a technical report detailing the crucial mistakes and how to avoid and prevent them in future projects. If an IT accident investigation board were to write a report when such a project failed, and if the contracts for all future projects stipulated that recommendations from the board must be followed, then at least taxpayers would not have to pay to repeat the same mistakes.

The third point should barely need mentioning: Personal information is the helium of IT systems—it leaks out of every crack or imperfection faster than seems possible. This is obviously a subclass of "loss of liberty," but it is

so dominating that it deserves its own category.

While pretty much everybody agrees that something must be done, nobody wants to give an official IT accident investigation board the authority to find out what that "something" should be. Software houses hem and haw about how their trade secrets and intellectual property will be violated. What they really mean to say is they don't want anybody to stop their gravy train.

Individual developers fear they will be made scapegoats, even though this is precisely *not* what accident investigation boards do. And politicians and management in private companies are nothing if not unified in their desire to avoid accountability for cutting corners and best-case management.

One particularly bogus argument is that it is not possible to write IT accident reports in the first place. I don't know where that idea comes from, but surely not from reading accident reports. For example:

In 2017, the motor of an airplane exploded over the southern part of the Greenland icecap. Part of the engine landed on the ice while the plane continued to the first suitable airport way up north in Canada.

Nobody got hurt.

Two years later the accident investigation board located and dug up the missing parts a couple of meters under the surface of Greenland's ice.

If you think that sounds easy, I highly recommend the 69-page report about how they did it.

A year later, the board issued the final report, revealing that a failure mode called "cold dwell/cold creep" had caused the fan blades to disintegrate. That came as a surprise to everybody, because nobody, not even a mad scientist in a secret lab, had ever imagined that as a failure mode for the Ti-6-4 titanium alloy.[b]

So, yes, surely an IT accident investigation board would find it "impossible" to figure out what went wrong with the U.K. Post IT system. Not!

Another bogus argument is that people would refuse to talk and would destroy and hide evidence. This vastly underestimates lawmakers: It is a crime to do that for all other accident investigation boards, and even small infractions lead to jail time. And no, it is not "self-incrimination" unless you did something criminal.

Software houses hem and haw about how their trade secrets and intellectual property will be violated. What they really mean to say is they don't want anybody to stop their gravy train.

Finally, and most perplexing to me, people claim an IT accident investigation board will cost too much money.

Compared to what?

Compared to destroying the lives of almost 700 people with bogus criminal records and years in jail, separated from their family and kids?

Compared to the 100 million euros Denmark spent on a new IT system for the police, a project that never delivered anything? That amount of money could easily have paid for the first 20 years of a Danish IT accident investigation board.

There really are no valid arguments against IT accident investigation boards, and all the bogus arguments proffered are the same ones that people put forth to counter all the other very successful accident investigation boards now in operation.

These boards work. We need one for IT, and we need it now.

Note: Shortly after this article was written, the U.S. announced the establishment of a new Cybersecurity Safety Review Board, similar to what is described here.[c]

"The Executive Order establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity. Too often organizations repeat the mistakes of the past and do not learn lessons from significant cyber incidents. When something goes wrong, the Administration and private sector need to ask the hard questions and make the necessary improvements. This board is modeled after the National Transportation Safety Board, which is used after airplane crashes and other incidents."

b https://bit.ly/3ijweWw

c https://www.whitehouse.gov/

Poul-Henning Kamp (phk@FreeBSD.org) spent more than a decade as one of the primary developers of the FreeBSD operating system before creating the Varnish HTTP Cache software, which around one-fifth of all Web-traffic goes through. He is an independent contractor; one of his most recent projects was a super-computer cluster, to stop the stars twinkling in the mirrors of ESO's new ELT telescope.

Copyright held by author/owner.
Publication rights licensed to ACM.