SEVERAL SUPPORTERS OF CISA ADMIT ITS INADEQUACY

In recent days, there have been reports that the same (presumed Chinese) hackers who stole vast amounts of data from the Office of Personnel Management have also hacked at least United Airlines and American. (Presuming the Chinese attribution is correct — and I believe it — I would be surprised if Chinese hackers hadn't also tried to hack Delta, given that it has a huge footprint in Asia, including China; if that's right and Delta managed to withstand the attack, we should find out how and why.)

Those hacks — and the presumption that the Chinese are stealing the data to flesh out their already detailed map of the activities of US intelligence personnel — have led a bunch of Cyber Information Sharing Act supporters (Susan Collins and Barb Mikulski have already voted for it, and Bill Nelson almost surely will, because he loves surveillance) to admit its inadequacy.

> In recent months, hackers have infiltrated the U.S. air traffic control system, forced airlines to ground planes and potentially stolen detailed travel records on millions of people.
>
> Yet the industry lacks strict requirements to report these cyber incidents, or even adhere to specific cybersecurity standards.
>
> "There should be a requirement for immediate reporting to the federal government," Sen. Susan Collins (R-Maine), who chairs the Appropriations subcommittee that oversees the Federal Aviation Administration (FAA), told The Hill.
>
> "We need to address that," agreed Sen. Bill Nelson (D-Fla.), the top Democrat

> on the Senate Commerce Committee.
>
> [snip]
>
> “We need a two-way exchange of information so that when a threat is identified by the private sector, it’s shared with the government, and vice versa,” Collins added. “That’s the only way that we have any hope of stopping further breaches.”
>
> [snip]
>
> That’s why, Nelson said, the airline industry needs mandatory, immediate reporting requirements.
>
> “All the more reason for a cybersecurity bill,” he said.
>
> But for years, Congress has been unsuccessful in its efforts.
>
> Sen. Barbara Mikulski (D-Md.), the Senate Appropriations Committee’s top Democrat, tried three years ago to move a cyber bill that would have included rigid breach reporting requirements for critical infrastructure sectors, including aviation.
>
> “We were blocked,” she told The Hill recently. “So it’s time for not looking at an individual bill, but one that’s overall for critical infrastructure.”

So now we have some Senators calling for heightened cybersecurity standards for cars, and different, hawkish Senators calling for heightened cybersecurity sharing (though they don’t mention security standards) for airlines. Bank regulators are already demanding higher standards from them.

And someday soon someone will start talking about mandating response time for operating system fixes, given the problems with Android updates.

Maybe the recognition that one after another industry requires not immunity, but an approach to cybersecurity that actually requires some minimal actions from the companies in question, ought to lead Congress to halt before passing CISA and giving corporations immunity and think more seriously about what a serious approach to our cyber problems might look like.

That said, note that the hawks in this story are still adopting what is probably an approach of limited use here. Indeed, the story is notable in that it cites a cyber contractor, JAS Global Advisors Jeff Schmidt, actually raising questions whether mandated info-sharing (with the government, not the public) would be all that effective.

If OPM has finally demonstrated the real impact of cyberattacks, then maybe it’s time to have a real discussion of what might help to keep this country safe — because simply immunizing corporations is not going to do it.