Does The U.S. Need a National Cybersecurity Safety Board?

Tags: NEWS & INDUSTRY Management & Strategy

8-11 minutes

It is time, suggest two academics from Indiana University-Bloomington, for Congress to establish a National Cybersecurity Safety Board (NCSB) as an analogue of the National Transportation Safety Board (NTSB), to improve the level of cybersecurity in the U.S.

The argument is that the NTSB helped to improve the safety of air travel while still stimulating growth and innovation in the industry. "Today," they say in a paper published this week, "air travel is widely regarded as among the safest forms of mass transportation. Can the same feat be replicated in cyberspace?"

Scott J. Shackelford JD, PhD, and Austin E. Brady argue, in their paper "*Is it Time for a National Cybersecurity Safety Board?* Examining the Policy Implications and Political Pushback' that it is both time, and possible (although not immediately probable). "A NCSB is politically unlikely in the near term, but we believe that the creation of such a body is overdue... All that is needed is the political will to act, the desire to experiment with new models of cybersecurity governance, and the recognition that we should learn from history."

The paper argues that there have been many propositions for strengthening U.S. cybersecurity, "from federally sponsored cyber risk insurance programs to allowing companies to have a freer hand to engage in proactive cybersecurity measures." The former would allow the insurer to impose cybersecurity conditions, while the latter would allow 'active defense' or even the right to 'hack back' . Across most of these proposals, it suggests, "are more robust data breach investigation requirements."

This connection is not clearly established in the paper, although it precisely aligns with the transportation functions of the NTSB. The argument is that we can better prevent future cybersecurity breaches by more fully understanding past breaches, and that this process needs to be established by government.

There is an alternative model for improving cybersecurity that is not mentioned in this paper: an American Cybersecurity Association (ACA) that uses the American Medical Association (AMA) as the model. This argument argues that professionalizing the cybersecurity workforce in the same way that the AMA professionalized the medical profession would raise the standard and quality of organizations' cybersecurity.

The ACA approach has been described by Martin Zinaich, Information Security Officer at the City of Tampa, FL. In his paper, 'What does Information Security have in common with Eastern Air Lines Flight 401?', he argues, "The AMA accelerated the professionalization of medicine and the establishment of minimum standards in medical training, education and apprenticeship requirements to gain entry to the profession. The same could and should be done in the Information Security field with a similar cybersecurity national body and professional associations."

The difference between the two approaches is that one imposes regulations from outside of the profession, while the other generates standards from within the profession. Both, however, suffer from inertia, and Shackelford and Brady argue that Congress should force the issue by establishing a national safety board.

"Such a model would be an improvement on the existing reliance on Cyber Emergency Response Teams (CERTs), and aide in effective policy making at both the state and federal level given the lack of hard, verifiable data on the scope and scale of cyber attacks. The creation of a NCSB could also help law enforcement investigations, particularly local and state agencies without the resources and expertise of the FBI. Along with the ISACs, this would be a boon to academics needing reliable data to undertake scholarly analysis, as well as national security organizations, and U.S. strategic partners around the world."

Interestingly, the authors spend some time looking at the European cybersecurity model depicted by the General Data Protection Regulation (GDPR) and the Network Information Systems Directive (NISD) both coming into force in May 2018. "Although neither the GDPR nor the NIS Directive includes a version of a regional Cybersecurity Safety Board, the elements it does include moves the EU in this direction, which could make an analogous U.S. body that much more effective," they write. "Such developments would be an important step on the long journey to a positive and sustainable cyber peace."

However, GDPR is far removed from any form of a national cybersecurity safety board. The authors say, "it centralizes data protection authority in the EU into a single regulatory body, as compared with the EU Data Privacy Directive's (DPD) utilization of

national data protection authorities for each Member State." This isn't strictly true -- each member state will retain its own regulatory body, and there are many areas within the regulation where national transposition has a degree of flexibility over implementation and interpretation. While GDPR is a unifying force, its application will still vary slightly between different member states.

Such minor differences are likely to be exacerbated by the concept of national security -- which again varies between different member states. "The extent of some of these obligations, however, is still unclear, as States may see cyber threats as falling in the realm of national security, and therefore outside the scope of this strata of EU governance," note the authors.

The interplay between national security and cybersecurity is not discussed within this paper; and yet it is fundamental to the way in which any overarching regulation -- whether the EU's GDPR or a proposed U.S. NCSB -- can actually operate. In the name of national security there will always be areas where intelligence agencies, and politicians, will seek to keep the true nature of events secret. There is likely to be considerable pushback from the intelligence agencies against any national body that has the independence of the NTSB, and the independence proposed for an NCSB.

How, for example, could an NCSB handle an investigation into a breach such as the Belgacom telco hack that was revealed in 2013? According to leaked documents (Snowden) it was undertaken by GCHQ using the NSA's 'quantum insertion' technology.

Martin Zinaich certainly has his concerns over an NCSB. "I support anything that might solidify a structuring of Information Security into a normalized business risk profile," he told SecurityWeek. "However, it seems to me a National Cybersecurity Safety Board might not be the best place to start. I also do not think a NCSB could be agile enough to keep pace.

"If there is one area where Cyber Security professionals excel," he continued, "it is in the identification of cyber-attacks and breaches. Too often, the cause is not a mystery where an investigative body would expose an unknown risk that could then be shared to make the industry safer (as does the current NTSB). No, too often the cause is well-known and age old. Take the 2017 Equifax breach. The vector was an Apache Struts vulnerability that had already been patched but the patch was not applied (and there are a lot of non-technical reasons why that can be so)."

Zinaich retains his belief that the best way to improve cybersecurity is by professionalizing the practitioners. "The issue is the integration of Information Security into the business at a level where it has an impact -- be the business a manufacturer of IoT devices or a credit lending institution. I still hold that professionalizing this field is the place to start, but I predict legislation will come first."

While there are strong arguments, as outlined in this paper, for the formation of a National Cybersecurity Safety Board, it is probably not achievable in the current geopolitical climate. Similarly, while there are strong arguments in favor of an American Cybersecurity Association, existing practitioners are generally too busy firefighting cybersecurity incidents to get it started.

The greater likelihood is that the current tendency for government to impose regulations to improve cybersecurity will probably just continue and gather pace.

Related: The Increasing Effect of Geopolitics on Cybersecurity

Related: Microsoft Warns Governments Against Exploit Stockpiling

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: