To prevent cyberattacks, paper suggests agency similar to National Transportation Safety Board

February 13 2018

After arguably the worst year ever for cyberattacks and data breaches, Indiana University research suggests it may be time to create an independent cybersecurity agency board comparable in approach to the National Transportation Safety Board that investigates airplane crashes and train derailments.

"In the wake of a series of destabilizing and damaging cyberattacks ranging from Equifax to Yahoo, there has been a growing call for the U.S. government to establish an analogue of the National Transportation Safety Board to investigate cyberattacks," the researchers write in the *Albany Law Journal of Science and Technology*.

The safety board model "separates fact-finding proceedings from any questions of liability, allowing attribution to be established, for example, without parties initiating litigation."

The paper's authors are Scott Shackelford, associate professor of business law and ethics in the IU Kelley School of Business, chair of the Cybersecurity Program and director of the Ostrom Workshop Program on Cybersecurity and Internet Governance at IU Bloomington; and Austin Brady, a degree candidate in the IU Maurer School of Law and IU's Master of Science in Cybersecurity Risk Management.

This approach has been floated in recommendations to the Trump

administration by the Center for Strategic and International Studies. But until now, the idea has never received in-depth academic treatment. In their paper, Shackelford and Brady review what led to the passage of the NTSB and evaluate proposals to establish a "National Cybersecurity Safety Board."

"Propositions for strengthening U.S. cybersecurity range widely, from federally sponsored cyber risk insurance programs—akin to flood insurance—to allowing companies to have a freer hand to engage in proactive cybersecurity measures," they wrote.

"A common refrain across many of these proposals ... (is a call for) more robust data breach investigations, which could include on-site gathering of data on why the attack occurred so as to help other companies prevent similar attacks. This evokes one of the core functions of the NTSB, that is, to investigate and establish the facts behind an incident, and to make recommendations to help ensure that similar events do not occur in the future."

Enhancing cybersecurity in the emerging Internet of Everything is technologically complex and legally challenging, especially when organizational cultures can be so different. Microsoft has estimated that the number of Internet-enabled devices could increase from 11 billion to 50 billion between 2013 and 2020. Another estimate from Morgan Stanley places the number at 75 billion by 2020.

Shackelford and Brady think a cybersecurity safety board could be a public-private partnership, potentially run by coalitions of companies.

"Funding could come from interested stakeholders, such as insurance companies," they said, "because such secondary markets would benefit from greater clarity surrounding the attribution of claims, as well as more information about the utility of various cybersecurity best

practices."

They also acknowledge the limitations and criticisms of a safety board model. Some critics say firms may use it for settling litigation and reputation management than for preventing future attacks. Another concern is that any cyber safety board's conclusions could be out of date by the time they are released, due to the dynamic cyberthreat environment and rapidly changing technologies.

"Such a model would be an improvement on the existing reliance on Cyber Emergency Response Teams and aid in effective policymaking at both the state and federal level, given the lack of hard, verifiable data on the scope of cyberattacks," the authors said.

"The creation of a National Cybersecurity Safety Board could also help law enforcement investigations, particularly local and state agencies without the resources and expertise of the FBI," they added. "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."

Provided by Indiana University