THE WALL STREET JOURNAL.

https://www.wsj.com/articles/the-u-s-needs-an-ntsb-for-cyberattacks-11559700060

BUSINESS | JOURNAL REPORTS: TECHNOLOGY

The U.S. Needs an NTSB for Cyberattacks

When there's an air crash, we call in the regulators to investigate. Let's do something similar for the biggest hacks.

A cybersecurity board would make a thorough forensic examination of large, sophisticated hacks and craft policy recommendations to guard against future breaches PHOTO: DELCAN & COMPANY

By Scott J. Shackelford

June 4, 2019 10:01 pm ET

It's time to take the worst cyberattacks as seriously as air disasters.

In many ways, cyber insecurity has never been more pronounced. Hackers have launched attacks on cities such as Atlanta, probed the U.S. power grid and even tried to compromise our democratic system. Research firm Cybersecurity Ventures projects that global losses from cyber crimes could well hit $6 trillion a year by 2021, while Gartner Inc. forecasts that world-wide spending on cybersecurity will exceed $124 billion in 2019.

The situation is dire. But we can start to bring it under control if we follow the example of another new industry that found a way to manage massive chaos.

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition

Like cybersecurity today, U.S. air travel initially wasn't regulated closely, and the industry suffered through a huge rate of fatal accidents in its early days. But after high-profile crashes killed legendary football coach Knute Rockne and Sen. Bronson Cutting of New Mexico, lawmakers set up a group—now known as the National Transportation Safety Board—to investigate crashes, figure out why they happened and let lawmakers and the industry know how to prevent them.

As a result, air travel has become one of the safest transportation methods of the 21st century. Accidents have declined for decades—despite recent tragic accidents such as those involving Boeing 737 MAX planes. From 2009 to April 2018, not a single passenger died from a crash involving a U.S. airliner.

We should learn from that history and establish a public-private body to investigate and prevent assaults on our information networks—a National Cybersecurity Safety Board.

How it would work

Currently, the closest thing we have to a safety board is the U.S. Computer Emergency Readiness Team, a division of the Department of Homeland Security designed to help a wide range of organizations inside and outside of the government respond to security breaches, assess the safety of their networks and train employees, among other things.

But this operation isn't designed to do what a cybersecurity board would do—make a thorough forensic examination of large, sophisticated hacks and craft policy recommendations to guard against future breaches.

Let's look more closely at what this theoretical board would do. By necessity, it would have to focus on a limited number of hacks. Transportation disasters thankfully are rare, while cyberattacks are all too frequent.

So, investigations would be confined to three basic categories: attacks that affect large numbers of Americans, such as the 2013 Target Corp. breach that allegedly impacted more than 40 million people; ones that cause widespread damage, such as an attack comparable to the 2012 hack on Saudi Aramco that devastated the mammoth oil company's computer systems; and ones that use novel and particularly dangerous techniques, such as Stuxnet.

Immediately after an attack was discovered, an organization would call in a National Cybersecurity Safety Board "go team," similar to those used by the NTSB, to investigate the situation. Each team member would have a specialty—such as cryptography or cyberforensics —and would work with security staffers to establish the details of the incident.

The investigation would cover a number of areas: a detailed look at the affected hardware and software, as well as interviews with organization members, and stakeholders such as suppliers and customers.

The Boeing 737 MAX saga demonstrates the effectiveness of air-accident investigation teams around the world—and a model for cybersecurity pros.

It took just 19 days in March for Ethiopian authorities to demonstrate that the antistall feature was at issue, the same problem that caused the Lion Air accident in Indonesia in November 2018. During that same time frame, countries around the world grounded the entire Boeing 737 MAX fleet, and Boeing began work on a software patch.

True, all this should have happened sooner, but it stands in marked contrast to the relatively slow response following major cyberattacks such as the one on Equifax.

Once the fact-finding was wrapped up, the cyberteam would publish its findings and make recommendations to help guide the industry and other parties toward preventing similar lapses. Like the NTSB, the board wouldn't have the power to enforce changes. But, ideally, lawmakers and industry would regularly adopt their proposals, as they do now with the NTSB.

Winning support

The political cost of establishing a National Cybersecurity Safety Board would be significant. While some industries, such as insurance, might come out in support, tech companies would likely balk at the idea—given that it would inevitably mean greater oversight by the U.S. government. Airlines and airplane manufacturers showed similar resistance back when the NTSB was being debated.

So, tech trade groups could test the waters by creating their own teams without government participation. And the government might reassure companies by giving them the same protection that the NTSB offers: Federal law bars the probable-cause findings or conclusions of NTSB aviation-accident investigations from being used in civil litigation.

But for a truly national cybersecurity board, a variety of incentives and regulatory requirements may be necessary to get companies to participate. And it may be necessary for the federal government to mandate investigations for serious breaches, such as those involving critical infrastructure.

I believe there's one incentive for establishing a cybersecurity board that will prove irresistible: access to information that isn't available right now. Currently, there aren't enough authoritative, comprehensive reports about massive cyberattacks available publicly, and their absence has caused confusion about what constitutes the gold standard for due diligence.

Comprehensive information wouldn't just help companies and other big organizations, of course. It would prove crucial to law-enforcement investigations, particularly local and state agencies that lack the resources and expertise of large government organizations that already investigate cyberattacks, such as the Federal Bureau of Investigation. It would also be a boon to academics who need reliable data to undertake scholarly analysis that would better inform policy makers and the public about the nature and scope of the cyber threats we face.

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."

Dr. Shackelford is an associate professor of business law and ethics at Indiana University's Kelley School of Business, chair of the IU-Bloomington Cybersecurity Program and director of the Ostrom Workshop Program on Cybersecurity and internet Governance. He can be reached at reports@wsj.com.

Appeared in the June 5, 2019, print edition as 'We Need an NTSB for Cyberattacks.'