Free markets. Real solutions.

R STREET SHORTS NO. 58
May 2018

THE NTSB AS A MODEL FOR CYBERSECURITY

Paul Rosenzweig

INTRODUCTION

On May 12, 2015, Amtrak train 188 derailed just north of Philadelphia. Eight people were killed and 185 more were treated at nearby hospitals for injuries that ranged from minor to critical. In the immediate aftermath, there was ample speculation as to what went wrong. But a year passed before the National Transportation Safety Board (NTSB) issued its report[1] that the accident was caused by the engineer's "loss of situational awareness likely because his attention was diverted to an emergency situation with another train."[2]

Post-incident reviews such as these are common in many fields, disciplines and professions. After a baseball game, for example, players review video tape of their at-bats. After a hurricane, the Federal Emergency Management Agency (FEMA) deploys a "lessons learned" process to improve its response and learn from its mistakes. Following a battle, the military performs an "after action report" for the same purpose. In each case the goal is the same – to learn whether or not there is some systematic error or gap that can be filled in order to mitigate future risk.

Earlier this year, Rep. Denny Heck (D-Wash.) posed an interesting question: namely, whether it is time to consider creating a mechanism akin to the NTSB for the review of cyber breaches.[3] In other words, is there value in the creation of a government agency[4] that would be solely responsible for the investigation and report of how cybersecurity breaches happen and what can be done to avoid them in the future? Such an agency would, for example, provide an independent review of breaches like the one that occurred at Equifax[5] and issue reports on why the systems failed and how they could be made better. Certainly, in today's increasingly digital age, this is an idea worth exploring.[6]

THE NTSB MODEL

The NTSB is an independent agency of the federal government. It is charged with the investigation of every civil aviation accident in the United States and also investigates significant accidents that occur in other modes of transportation (such as the Amtrak train accident noted above). Its mission is to conduct objective, independent accident investigations to determine their probable causes. When the situation warrants, the agency is also responsible for issuing safety recommendations that address observed gaps in the systems, with the goal of preventing future accidents. Finally, the NTSB also carries out special studies of safety issues that arise outside the context of a particular accident or incident.

Notably, the NTSB is required by statute to focus on the cause and effect of accidents. As a consequence of such a specific mandate, the agency has no enforcement authority and thus the implementation of its recommendations (or the decision not to do so) lies with other agencies.

Some see this focus as a bit too narrow, particularly as the NTSB's remit does not include the authority to examine questions of cost, for example. For this reason, some of its safety recommendations are too expensive and do not meet a cost/benefit test. On balance, however, most observers agree that it is beneficial to have an agency tasked with the sole mission of determining the cause of an incident and then advocating for safety improvements.

TOWARD A "COMPUTER NETWORK SAFETY BOARD"

Similarly, it would be worthwhile to consider the creation of a wholly independent board to determine the probable cause of cyber intrusions and, as appropriate, to recommend network safety improvements. To this end, the proposed Computer Network Safety Board (CNSB) could be constructed along the same lines as the NTSB.

There are, of course, likely to be challenges with its operation. To begin with, the sheer volume of cyber breaches each year is daunting. Last year, for example, there were more

than 53,000 incidents and more than 2,200 breaches in the United States alone.[7] This number is far greater than the number of significant transportation accidents that occur annually in the United States.

Hence, as an initial matter, the legislation to create the CNSB would have to define some sort of threshold for review. One option is to define the significance of a breach by the number of its victims. An alternate approach would be to define significance by the scope and scale of the financial harm caused. Or, of course, some combination of these two factors could be used, along with a more qualitative assessment of harm to the overall security and economy of the nation. To be sure, any such line would be arbitrary, but having one would be essential.

Next, the CNSB would need to recognize that the forensics of cyber-breach investigations are often less determinative than those for physical events (like train accidents). Thus, while we can often identify a single point of failure (or perhaps two or more contributing causes) for a physical incident, it is likely that there will be instances in which the CNSB cannot readily discern a true cause. Perhaps more to the point, even more than is the case in physical systems, the prospect of failure in a cyber system is one of inevitability. No amount of review or improvement can ever create perfect security.

This suggests that the mission of the CNSB must be carefully defined as risk *reduction* rather than risk *elimination*. After all, any board that were created on the premise of altogether eliminating cyber risks or intrusions would be founded on a false premise.

Third, unlike train wrecks or hurricanes (but akin to baseball games and battles) network breaches will typically be the result of adaptive adversarial action; or, a circumstance that limits—to a significant degree—our ability to close vulnerability gaps definitively. Even if the CNSB identifies a network flaw and recommends a security improvement, for example, these recommendations would not be capable of fully resolving any risk. Indeed, since the recommendations necessarily would be public, their publication would simply set a new target for malicious actors.

Fourth, the cybersecurity board would need be structured to avoid the creation of incentives for non-cooperation and would have to be carefully cabined with rules that avoid an increase in the liability of cooperating entities. In general, regulations prohibit, for example, the admissibility of NTSB final reports in court cases. But, over time, that doctrine has eroded.[8] It is likely that computer security investigations would require even greater cooperation from those concerned than physical accident investigations do. Accordingly, the protection against liability for cooperation would have to be commensurately stronger.

Especially in a complex area like cybersecurity, which is rife with ambiguity, it will be hard enough to identify causes without then filtering those conclusions through an economic-benefit filter. For this reason, although the cost/benefit issue merits careful consideration, we should lean toward a model that replicates the current structure of the NTSB; that is, one focused on cause and effect, without any enforcement authority and without any mandate to address cost/benefit questions. Other agencies will have that job.

Perhaps most saliently, the CNSB would need to be structured so that it examines both the human and technical factors behind breaches. All too often, the cause of a cybersecurity breach is inattention or lack of care by individuals rather than technical flaws in cyber systems. The board will need both technical expertise to identify gaps in intrusion detection and prevention systems, as well as human factors expertise to assess the control systems in place within a failed organization.

Thus, the board will need a good dose of humility, both in the assessment of human frailty and in the recognition that while human error is reducible, it cannot be eliminated. Thus we must be careful not to conflate the creation of a new network safety board with the false promise of perfect security.

None of these is a fatal objection. Indeed, quite to the contrary, an assessment of cyber failures is an essential component of cybersecurity success and an independent board tasked with such a systematic role would be of value. In the long run, if we are to enhance security, we need a way to measure it, or to "rate the risk" from cyber threats. To this end, having good data about how they occur is fundamentally a valuable exercise that would advance that prospect.

ABOUT THE AUTHOR

Paul Rosenzweig is a senior fellow of with the R Street Institute, where he works on legal and policy issues relating to cybersecurity, national security and tech policy, including the intersection of privacy and security.

ENDNOTES

1. "Derailment of Amtrak Train 188 Philadelphia Pennsylvania May 12, 2015," National Transportation Safety Board, May 17, 2016. https://www.ntsb.gov/investigations/AccidentReports/Reports/RAR1602.pdf.

2. "Safety Recommendation R-16-041," National Transportation Safety Board, June 9, 2016. https://www.ntsb.gov/safety/safety-recs/_layouts/ntsb.recsearch/Recommendation.aspx?Rec=R-16-041.

3. "Examining the Current Data Security And Breach Notification Regulatory Regime," House Finance Committee, Subcommittee on Financial Institutions and Consumer Credit, Feb. 14, 2018. https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402988.

4. Representative Heck notionally referred to the proposed agency as the "Computer Network Safety Board."

5. For a good summary, see "The Equifax Data Breach," U.S. Federal Trade Commission, 2018. https://www.ftc.gov/equifax-data-breach.

6. A similar idea to the concept of an Internet NTSB has been proposed previously. See, e.g., Michael Barrett et al., "Combatting Cyber Crime: Policies, Principles and Proposals," PayPal, April 2011.

7. "Verizon 2018 Data Breach Investigations Report," Verizon, 2018. https://www.verizonenterprise.com/verizon-insights-lab/dbir.

8. Alice Chan, "Trend towards the inadmissibility of NTSB final reports," Aircraft Builders Council, 2000. http://www.aircraftbuilders.com/files/2716/File/lr2000d.pdf.