

THE CYBER PROJECT

Learning from Cyber Incidents

Adapting Aviation Safety Models to Cybersecurity

Report on the Interdisciplinary Workshop on
the Development of a National Capacity for
the Investigation of Cyber Incidents

Rob Knake

Adam Shostack

Tarah Wheeler



HARVARD Kennedy School

BELFER CENTER

for Science and International Affairs

PAPER

NOVEMBER 2021



The Cyber Project

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/cyber

Statements and views expressed in this report are solely those of the author and do not imply endorsement by Harvard University, Harvard Kennedy School, the Belfer Center for Science and International Affairs, the U.S. government, or the Department of Defense.

Layout by Benn Craig

Copyright 2021, President and Fellows of Harvard College
Printed in the United States of America

Learning from Cyber Incidents

Adapting Aviation Safety Models to Cybersecurity

Report on the Interdisciplinary Workshop on
the Development of a National Capacity for
the Investigation of Cyber Incidents



Organized by

**Belfer Center for Science and International Affairs,
Harvard Kennedy School**

with support from

**The Global Resilience Institute,
Northeastern University**

March 18 - June 24, 2021

Project Team

Report Authors

Rob Knake, Harvard University

Principal Investigator

Adam Shostack, Shostack + Associates, The University of Washington

Principal Investigator

Tarah Wheeler, Harvard University

Project Advisor

Steve Bellovin, Columbia University

Research Team

Felipe Bueno, Harvard University

Ben Lefkowitz, Harvard University

Victoria Ontiveros, Harvard University

Acknowledgments

We would like to thank **Tarah Wheeler** for stepping in to assist with the drafting of this report. Her experience in the field and clear writing helped to make the final product many times better. **Felipe Bueno, Ben Lefkowitz, Victoria Ontiveros** provided superb research and organizational support. Our project advisor, **Steve Bellovin** has been an invaluable aid and supporter of this project on an idea he has long-championed. **Stephen Flynn** at Northeastern University helped us negotiate the sometimes difficult process of carrying out a National Science Foundation workshop. We would also like to thank **Sara Kiesler**, our program officer at NSF, who took a chance on two practitioners with limited academic pedigree to carry out this important work. We also would like to thank the **Hewlett Foundation** whose grant to the Belfer Center made the work there possible. Finally, we are deeply grateful to the workshop participants who enthusiastically shared their many decades of experience in a host of different fields during a series of remote sessions while a pandemic raged on.

Adam Shostack & Rob Knake

Principal Investigators

Table of Contents

| | |
|--|-----------|
| Executive Summary | 1 |
| Introduction..... | 5 |
| Workshop Organization and Format..... | 5 |
| Background..... | 7 |
| Problem Statement..... | 11 |
| Assumptions Behind A Cyber NTSB..... | 13 |
| Discovery and Incident Identification..... | 19 |
| How Can A Board Become Aware Of Incidents?..... | 19 |
| How Should a Board Select What to Investigate? | 24 |
| Investigation..... | 27 |
| How should investigations run? | 27 |
| What should a board investigate?..... | 34 |
| What investigative techniques should be used? | 36 |

| | |
|---|-----------|
| Reporting and Data Usage | 40 |
| What values can be improved by public reporting? | 40 |
| Tensions persist, including security, transparency, and blame | 44 |
| Near-Miss Reporting and Investigations..... | 47 |
| Research Agenda..... | 50 |
| Recurrent Issues and Themes..... | 50 |
| Research Questions..... | 56 |
| Recommendations for the CSRB..... | 68 |
| Recommendations for Congress..... | 73 |
| Conclusion: Failure Is Common, But Not Constant..... | 75 |
| Appendix A: Workshop Program | 76 |
| Appendix B: Participant Biographies..... | 77 |





Executive Summary

Over four months in the spring of 2021, over 70 experts participated in a (virtual) workshop on the concept of creating a “Cyber NTSB”. The workshop was funded by the National Science Foundation with additional support from the Hewlett Foundation, and organized by Harvard’s Belfer Center with support from Northeastern University’s Global Resilience Institute.

The first call for the creation of a Cyber NTSB was in 1991. Since that time, many practitioners and policymakers have invoked the analogy, but little has been done to develop the concept. This workshop was carried out with the goal of moving the concept forward.

The NTSB acts as an inspiring metaphor because it helped transform the nascent technology of aviation. It’s easy to forget how much airplanes shrunk the planet over the last century, making it possible to go anywhere in the world quickly, safely, and reliably, but that was not always the case. It’s also easy to forget how often planes crashed. The NTSB is the best known of the broad, deep, and intertwined set of aviation safety programs we learned about. While participants challenged and tested the model, the ultimate conclusion was that the information technology industry does not have strong processes for extracting lessons learned and publishing them when incidents occur. Today, cybersecurity has no authoritative, independent investigations whose focus is learning lessons, distributing them, and enabling systematic improvements.

The continuing success of attackers demands a new approach to science and policy. Lesson-learning systems — ranging from the in-depth investigations of the NTSB to studying statistics about attacks or near misses — almost certainly have a part to play. There is experimentation, the heart of science, to be done in understanding what that part may be. That experimentation includes many scientific questions, such as searching for ways to maximize the value of data to defenders and system designers while limiting how it might inform attackers. It includes policy questions such as the ability of investigators to compel participation.

(continued)

Building a strong learning system for cyber incidents will require overcoming a host of challenges, and making decisions in the face of uncertainty. We are confident that many of these issues can be usefully resolved by research, and that such research can also contribute to the success of an already established organization.

This workshop has led to the discovery of over 50 discrete research questions that we believe are worth investigating; it has generated 24 concrete findings for consideration by the technical, policy, and research community; and a series of recommendations for the Biden Administration and Congress as they work to translate the concept of a Cyber NTSB into reality. Highlights of our findings include:

Third party and in-house investigations are no substitute for objective, independent investigations.

Market forces dictate that most cyber incidents will not be revealed. When information is released, it is limited to the minimal amount that must be disclosed by law. When companies choose to share more information, they choose to do so carefully and in such a manner that they control the narrative, excluding any information that will not put them in a positive light. Thus, a Cyber NTSB is necessary to understand what contributed to an incident occurring and how other organizations can prevent a similar incident from happening to them.

Companies are unlikely to fully cooperate under a voluntary regime.

Subpoena authority will likely be necessary for a board to succeed in gaining access to the necessary data and people to reconstruct a timeline and narrative of any incident. While the nascent Cyber Safety Review Board (CSRB) may be able to gain some insights into SolarWinds given

the high profile of that incident, reviews of other incidents will likely be near impossible unless companies are required to cooperate.

Product, tool, and control failure must be identified in an objective manner.

The cybersecurity community shies away from identifying when products, controls, and the tools used to implement them fail. Without knowledge of these failures, control designers, toolmakers, and the defenders that implement them are missing critical information necessary to make good use of their security budgets and the time of security personnel.

Findings may be sensitive but should be disseminated as widely as possible.

Adversaries will doubtless pore over any reports produced by the CSRB or any other bodies stood up. This reality should not dissuade investigatory boards from producing reports; however, it may be that some reports or sections of the reports should be disseminated only over classified channels or have their dissemination limited in other ways.

Fact finding should be kept separate from fault finding.

Lawmakers must find ways to create circumstances under which the targets of cyber adversary activity can share details on their incidents without fearing that they will be penalized. Finding the right balance between providing liability protection and letting courts and regulators hold companies accountable for poor security practices will be difficult but a balance must be struck.

“Near Miss” reporting can complement incident investigations.

Many of the factors that make investigation of incidents difficult are either missing or reduced when at least one control succeeded.

A strong system of near miss reporting complemented by investigation of these near misses may yield meaningful results.

Making Progress

There is policy work to be done to enable us to learn lessons. Most importantly, Congress must work with the Administration to create and empower a set of entities to learn lessons at different scales and speeds, including the Solarium Commission's Bureau of Cyber Statistics and a system to learn from near misses.

There are many immediate opportunities to improve security that policymakers in Congress and the Administration are pursuing. Similarly, there has been an explosion of research in information security, assurance, resilience and other disciplines. These have obscured and eclipsed the need for deep lesson learning systems. Our hope is that the full report informs not only the science and policy communities, but helps the new CSRB see and meet its important goals.

Note: The findings and recommendations contained in this report were drawn from the multi-session workshop and are based on panelist and participant comments both during discussions and in follow-on email and Slack conversations. This report, however, does not represent a consensus among workshop participants. Participation in the workshop in no way serves as an endorsement of the findings and recommendations contained in this report. Similarly, mentions of specific companies or incidents, security standards, and the like are intended to provide vibrant examples, not comment on them generally. The report's authors are solely responsible for its content.

Introduction

In the spring of 2021, the Belfer Center for Science and International Affairs at Harvard University organized a multi-session virtual workshop on creating a cyber incident investigative capacity modeled on the National Transportation Safety Board (NTSB). The goal of the workshop was to develop a research agenda to further the concept. Given fast-moving events, the workshop went beyond that mandate to also address pressing policy issues given interest from Congress and the Biden Administration in standing up such an organization. This report presents the findings from the workshop. The workshop was sponsored through grants from the National Science Foundation and the Hewlett Foundation.

Workshop Organization and Format

This workshop was centered on three tracks of discussion:

1. Initial discovery of incidents
2. Investigations
3. Reporting and data sharing/publication

The workshop assembled over 70 experts in a wide variety of disciplines (See Appendix B for participant biographies). Within each track, participants identified assumptions, highlighted broad themes, and narrowed in on specific questions to inform a research agenda. While the virtual format had its deficiencies, it also had its advantages. Many participants who would not have been able to attend the previously scheduled in-person workshop in Washington were able to join virtually. The virtual format also allowed the multiple sessions to be spread out over two months to lessen the fatigue of attending long days of consecutive sessions. This format also allowed participants to engage in the development of the agenda. The first session of the workshop was an open plenary to solicit ideas and speakers for follow-on sessions. The final program is in Appendix A.

We use the terms “Cyber NTSB”, “board” and “investigations board” to refer to an independent investigatory board. When specificity aids clarity, we refer to the specific type of board, either prospectively or about the CSRB established by the executive order.

Background

Policymakers and practitioners in the cybersecurity community have long posited the need for an agency or capacity to investigate cyber incidents to identify deficiencies in security controls and better inform the defender community. Comparing this function to what the NTSB does for aviation and surface transportation incidents is a commonly used analogy because it provides both substance and form to the concept. The NTSB is an independent Federal agency charged by Congress with investigating every civil aviation accident in the United States and significant accidents in other modes of transportation – railroad, highway, marine, and pipeline. The NTSB determines the probable cause of the accidents and issues safety recommendations aimed at preventing future accidents. In addition, the NTSB carries out special studies concerning transportation safety and coordinates the resources of the Federal Government and other organizations to assist victims and their family members impacted by major transportation disasters.

The first recorded call for the creation of an entity like the NTSB that would investigate cyber incidents was made in a 1991 report by the National Research Council. That report, “Computers at Risk: Safe Computing in the Information Age,”¹ was focused on building a “repository of incident data” that could be used to support several purposes. The NTSB is mentioned, as is the then-nascent CERT operated by DARPA in the aftermath of the Morris Worm. Some of the recommendations made in the NRC report have been implemented. For example, information about vulnerabilities is managed in the Common Vulnerabilities and Exposures (CVE) and the National Vulnerability Database (NVD).² Yet the core concept of a “Cyber NTSB” has not been implemented.

1 “The committee recommends that a repository of incident information be established for use in research, to increase public awareness of successful penetrations and existing vulnerabilities, and to assist security practitioners, who often have difficulty persuading managers to invest in security. This database should categorize, report, and track pertinent instances of system security-related threats, risks, and failures. Because of the need for secrecy and confidentiality about specific system flaws and actual penetrations this information must be collected and disseminated in a controlled manner.”

2 National Research Council, *Computers at Risk* (Washington, DC: National Academies Press, 1991), <https://doi.org/10.17226/1581>

In 2006, Richard Bejtlich, then at GE Security, developed the concept further in a lengthy blog post.³ In 2008, Adam Shostack and Andrew Stewart drew attention to the importance of learning lessons from breaches in *The New School of Information Security*.⁴ Neil Robinson at the RAND Corporation made a similar call in a 2012 blog post,⁵ as did Steven M. Bellovin of Columbia University writing in IEEE Spectrum.⁶ Ben Rothke made a similar case in 2015.⁷ In 2016 Bellovin and Shostack commented that these calls were frequent, consistently not acted on, and suggested an investigation into why that was.⁸ In the same year, Rob Knake authored a piece recommending that a Cyber NTSB be included in a Federally backstopped cyber insurance program.⁹ In 2018, Paul Rosenzweig at the R Street Institute published a short paper on the topic,¹⁰ and a team at the University of Washington Henry M. Jackson School of International Studies conducted a literature review on the topic (which aided in the development of this summary).¹¹ In 2018, Tarah Wheeler argued in *Foreign Policy* that the absence of competent cybersecurity auditing is a policy issue,¹² and Scott Shackelford and Austin Brady authored a law

3 Richard Bejtlich, "National Digital Security Board," TaoSecurity Blog, entry posted August 21, 2006, <https://taosecurity.blogspot.com/2006/08/national-digital-security-board.html>

4 Adam Shostack and Andrew Stewart, *The New School of Information Security* (Addison-Wesley, 2008).

5 Neil Robinson, "The Case for a Cyber-Security Safety Board: A Global View on Risk," The Rand Blog, entry posted June 18, 2012, <https://www.rand.org/blog/2012/06/the-case-for-a-cyber-security-safety-board-a-global.html>

6 Steven M. Bellovin, "The Major Cyberincident Investigations Board," IEEE Security and Privacy 10, no. 6 (November/December 2012), <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6375729>

7 Ben Rothke, "It's Time for a National Cybersecurity Safety Board (NCSB)," CSO, February 19, 2015, <https://www.csoonline.com/article/2886326/its-time-for-a-national-cybersecurity-safety-board-ncsb.html>

8 Adam Shostack and Steven M. Bellovin, Input to the Commission on Enhancing National Cybersecurity, September 2016, https://www.cs.columbia.edu/~smb/papers/Current_and_Future_States_of_Cybersecurity-Bellovin-Shostack.pdf.

9 <https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program>

10 Paul Rosenzweig, The NTSB as a Model for Cybersecurity, R Street Shorts no. 58, May 1, 2018, <https://www.jstor.org/stable/resrep19126>

11 Jessica L. Beyer, Drake Birnbaum, and Thomas Zech, The Next Step in Federal Cybersecurity? Considering an NTSB-Style Computer Safety Board, June 2018, https://jsis.washington.edu/wordpress/wp-content/uploads/2018/08/Jackson_School-NTSB-CSB-Final.pdf

12 Tarah Wheeler, "In Cyberwar, There Are No Rules," *Foreign Policy*, September 12, 2018, <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/>

review article on the subject.¹³ In 2019, Shackelford published an opinion piece in *The Wall Street Journal* arguing for an “NTSB for Cyberattacks,”¹⁴ and Knake testified before Congress on the subject.¹⁵

While these contributions kept the concept in the discussion, furthered thinking, and promoted it to lawmakers, the most significant expansion on the concept came as part of a previous workshop in 2014. The 2014 National Science Foundation-sponsored Cybersecurity Ideas Lab produced the report “Interdisciplinary Pathways towards a More Secure Internet,”¹⁶ which included a two-page discussion and recommendation on the Cyber NTSB concept. The report noted the lack of authoritative public information, recommended a series of next steps, included a discussion of potential pitfalls, and outlined several different approaches. This effort served as a rough template for what the current workshop explored.

Following the discovery of the SolarWinds hacking campaign, the general idea of a board to investigate cyber incidents gained renewed interest. Alex Stamos, former Chief Information Security Officer (CISO) at Yahoo, former Chief Security Officer (CSO) at Facebook, and a leader in efforts to combat disinformation and promote the integrity of the voting system in the lead up to the 2020 election, called for the creation of a Cyber NTSB in a *Washington Post* op-ed.¹⁷

¹³ Scott Shackelford and Austin E. Brady, “Is it Time for a National Cybersecurity Safety Board?,” *Albany Law Journal of Science and Technology*, nos. 18-34 (January 12, 2018), <https://ssrn.com/abstract=3100962>

¹⁴ Scott J. Shackelford, “The U.S. Needs an NTSB for Cyberattacks,” *Wall Street Journal*, June 4, 2019, <https://www.wsj.com/articles/the-u-s-needs-an-ntsb-for-cyberattacks-11559700060>

¹⁵ “Preparing for the Future: An Assessment of Emerging Cyber Threats,” Testimony Before the House of Representatives, October 22, 2021, https://cdn.cfr.org/sites/default/files/report_pdf/hhrg-116-hm08-wstate-knaker-20191022.pdf

¹⁶ National Science Foundation, *Interdisciplinary Pathways towards a More Secure Internet: A Report on the NSF-Sponsored Cybersecurity Ideas Lab Held in Arlington, Virginia on February 10-12, 2014*, https://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf

¹⁷ Alex Stamos, “Enough Is Enough. Here’s What We Should Do to Defend against the Next Russian Cyberattacks.,” *Washington Post*, December 15, 2020, <https://www.washingtonpost.com/opinions/2020/12/15/enough-is-enough-heres-what-we-should-do-defend-against-next-russian-cyberattacks/>

The uptick in interest was not only in industry and academia. Senator Mark Warner raised the issue in a February 23, 2021 hearing¹⁸ on the SolarWinds incident. Representative Yvette Clarke explicitly brought up the NTSB analogy, while Representative Kathleen Rice (and witness Kevin Mandia) brought up NASA's Aviation Safety Reporting System. Representative Bennie Thompson and others signaled interest, and several Congressional staffs began drafting legislation. Representative Michael Cloud brought up connecting the dots, and Representative John Katko brought up the challenge of learning more “with each passing day.”¹⁹ Thus, despite the ongoing pandemic, the research team was encouraged to restart efforts on this project virtually in order to inform potential administrative or Congressional action. While our workshop did not intend to produce a report on SolarWinds or mimic an investigation of that campaign, SolarWinds did serve as a useful reference point against which to consider why an investigative board might be necessary.

As the workshop was winding up, the President issued an Executive Order on Improving the Nation's Cybersecurity.²⁰ Section 5 of the order establishes the CSRB in the Department of Homeland Security (DHS). The board “shall review and assess, with respect to significant cyber incidents [...] affecting Federal Civilian Executive Branch Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses.” Given this development, the final sessions of the workshop included in-depth discussions of the content of the executive order and how it should be implemented. This report includes takeaways from that discussion and recommendations for the CSRB.

18 U.S. Senate Select Committee on Intelligence Hearing on the Hack of U.S. Networks by a Foreign Adversary, 117th Cong., 1st Sess. (2021). <https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary>

19 Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign: Hearings Before the House Homeland Security Committee and House Oversight and Reform Committee (2021). <https://oversight.house.gov/legislation/hearings/weathering-the-storm-the-role-of-private-tech-in-the-solarwinds-breach-and>.

20 Executive Order on Improving the Nation's Cybersecurity, The White House May 12, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Problem Statement

Participants began the workshop by attempting to identify the problem an investigative body would be solving. Moderators started by providing the problem statement from the 2014 NSF Report: “A critical problem in cyber security is a lack of reliable, consistently reported data about security incidents. The lack of data makes it difficult for others to learn from these attacks, and is leading to misplaced priorities.”²¹ Participants generally agreed that this problem statement, though “not wrong,” was insufficient. One participant noted that the problem was not so much “data,” something the cybersecurity industry is awash in, but rather “information, knowledge, and wisdom,” referencing the DIKW pyramid for Data, Information, Knowledge, and Wisdom.²² Raw data on cyber incidents (such as malware samples, email, IP, and web addresses used in the attack) are quite often shared, and there are already strong mechanisms for this sharing, and they continue to be improved. Transforming this data into useful “information” continues to be a challenge. The core value an incident investigation board can provide is to extract both knowledge and wisdom in understanding why an incident occurred and what to do about it. Another participant reframed this as a challenge of “data vs. narrative” – that we lack a full and complete picture of why incidents occur from which we can draw lessons learned. Another participant noted that the problem we are trying to solve is not so much the “lack of reliable, consistently reported data” but that for most incidents an investigation to understand why the incident occurred is never undertaken in the first place, let alone shared externally.

Participants also agreed that a lack of understanding of how incidents occur and what can prevent them does lead to misplaced priorities in terms of investments, but that this was also too limiting a statement. A robust lessons learned system could help organizations prioritize decisions around what products they rely on, how they operate them, what controls they implement, and should also help to identify problems with the implementation of controls. It can lead to their refinement, highlight the need for new classes of controls, identify weaknesses in regulatory

²¹ See NSF, footnote 15.

²² Jennifer Rowley, “The Wisdom Hierarchy: Representation of the DIKW Hierarchy,” *Journal of Information Science* 33, no. 2 (April 1, 2007): <https://doi.org/10.1177/0165551506070706>

mechanisms, and make the community aware of tool failures. Other participants noted that when investigations do occur, they are not always rigorous, objective, or independent. Sometimes, investigations can be politically motivated, and when conducted under the threat of litigation, there may be a desire to avoid inconveniently discovering too much. Several participants raised the point that the failure to understand how incidents occur and to share these lessons learned provides an advantage to the attacker, who can continue to use the same approaches on multiple targets without concern that their tactics will become commonly known.

Based on these and other observations, a revised problem statement was developed:

“Cybersecurity problems abound. The cause of these problems, and thus the most effective way to reduce them in future, is unclear and hotly contested within the cybersecurity community. The lack of independent, objective investigations into cyber incidents hampers the development of a virtuous cycle of ongoing improvement in cybersecurity. Without a process for understanding how incidents occur, and sharing these lessons learned, cybersecurity will continue to be more art than science.”

Assumptions Behind A Cyber NTSB

As noted above, many experts in the field of cybersecurity have concluded that an “NTSB” is necessary. Implicitly or explicitly, each of these experts has drawn this conclusion on the basis of a series of assumptions about how information on incidents is collected and shared currently and how these processes could be improved. Facilitators worked with participants to draw out and capture the following assumptions.

Assumption 1: The aviation industry models a form of risk management that the cybersecurity industry should adopt

The aviation industry improves safety based on a shared understanding of the history, nature, and causes of aviation incidents, and the cybersecurity industry can benefit from those lessons. There are, however, important differences that should be noted. First, aviation puts at risk the life of pilots, passengers, crew members, and people on the ground. Thus, the aviation industry is strongly incentivized toward safety. In most cybersecurity incidents (though this may be changing), lives are not at risk and business or operational pressures may take priority over security. Second, aviation is a heavily regulated industry that relies on the government to perform essential functions like air traffic control. The IT industry, by contrast, is largely unregulated, and use of technology within regulated industries is often not subject to cybersecurity regulations (again, this is changing). Finally, aviation lessons learning systems are primarily concerned with safety rather than security. This distinction is important because adaptive adversaries may learn just as much from an incident review as defenders. Notably, in the case of suspected intentional and criminal acts, the

NTSB cedes primary investigation authority to the Federal Bureau of Investigation.²³

Assumption 2: We do not know why major incidents happen

Underlying the need for lessons learning systems for cybersecurity is an assumption that the cybersecurity community does not understand why major incidents occur or how to prevent them. Senior and respected technology industry participants voiced the view that we do in fact “know the causes of major incidents” and “we know what we need to do to prevent them.” (One participant asked “if we know what we need to do, why do we have so many different security standards?”) Incident reports routinely find that incidents can be prevented by improving “basic cybersecurity hygiene.” Yet, public understanding of incidents may differ markedly from what those with access to privileged information conclude. One participant shared a peer-reviewed paper on the root causes of five incidents.²⁴ Another participant had worked as an expert witness in lawsuits surrounding one of those incidents and stated that the paper was incorrect, and the facts of that case were not publicly known. Disagreeing on the causes of incidents and prescribing “simple” measures that “just” fix the problem is far from uncommon in cybersecurity.

²³ As noted earlier, the aviation industry is not the only one with a robust lessons-learned system of review. We see it, as well, for example, in the healthcare industry. Our focus on aviation here is the product of two factors: it is the most commonly identified analog and it involves a government agency whose activities and effects are more readily understood than private-sector processes. This focus should not, however, be monomaniacal -- we believe that research into other lessons-learned processes can also inform the discussion.

²⁴ Hamza Saleem and Muhammad Naveed, “SoK: Anatomy of Data Breaches,” Proceedings on Privacy Enhancing Technologies 2020, no. 4 (August 16, 2020): <https://doi.org/10.2478/popets-2020-0067>

Assumption 3: Private Response and Law Enforcement Investigations are Insufficient

Law enforcement investigates many cybersecurity incidents, but not all. For example, incidents stemming from a misconfiguration of a storage system, exposing personal information, are reasonably common, but no crime has been committed. Proposals for the creation of a cybersecurity board modeled on the NTSB presuppose that existing cyber incident investigation mechanisms are insufficient. When a cyber investigation board was first proposed in 1991, law enforcement forensic capacity was nascent and heavily dependent on academic investigators.²⁵ Today, Federal, state, and even local law enforcement agencies have developed specialized cybercrime investigative capacity.

Despite these developments, the main issue raised in the National Academies report remains – we lack a mechanism for “gathering information about incidents...that makes this information available to those who need it.”²⁶ Private sector incident responders are not routinely generating lessons learned for consumption by product creators, the cybersecurity community as a whole, or the broader community of technology implementers or operators. The current market prioritizes response, generally run for the benefit of the victim, with the goal of containment and eradication, not deep investigations for understanding the causes of incidents so that similar ones can be avoided in the future. Many of these investigations are organized in ways strongly driven by expectations of lawsuits, which limits both the dissemination of findings and interest in probing failures too deeply. They are also driven by cost considerations: what is the lowest cost fix that will address the problem? That may be defined as low-cost to an insurer or victim, and may or may not reflect the likelihood of recurrence.

Assumption 4: Investigations by regulators are insufficient

Given existing regulatory regimes that require incident reporting and include broad authorities for setting cybersecurity requirements,

²⁵ Cliff Stoll, *The Cuckoo's Egg* (New York, NY: Pocket Books, 1989).

²⁶ National Research Council, *Computers at Risk: Safe Computing in the Information Age*, 1991, <https://www.nap.edu/read/1581/chapter/3#36>

investigations by regulators might, in some ways, fulfill the function of a board. Workshop attendees shared several stories about investigations that were driven by regulators, and that those investigations went deeper (and cost significantly more) than a typical incident response engagement. Regulators drew important lessons from those investigations and imparted those lessons through regulatory examinations and rule changes.²⁷ Yet these types of investigations seem to be rare and the results are not widely shared. Several attendees with years of experience working inside heavily regulated organizations could not recall any event in which a reported incident triggered a deeper investigation or mandated that one be conducted. Moreover, an important role for an independent NTSB-like entity is to evaluate the activities of regulators and make recommendations for improving their work. Such self-criticism may be difficult for a regulatory body to engage in. As a result, the NTSB performs an investigation, rather than the FAA.

Assumption 5: Investigations by insurers are insufficient

Many people express the hope the cyber insurance industry will create a positive reinforcing loop of understanding problems and disseminating recommendations in order to reduce future claims, perhaps along the model of the Insurance Institute for Highway Safety.²⁸ Yet this idea has been discussed for over two decades and has not materialized.

An investigation that determines root causes will cost more than one that only determines immediate fault or eligibility for payout. These higher costs may be more than the insurance market can bear in the near term given high payout rates and fierce competition. More work could be done on how to make the insurance industry fulfill this role, possibly in partnership with government. There are likely important scientific questions into what an insurer should measure, how to measure those

²⁷ One story was of an incident where attackers “printed money” by tampering with a database of ATM card limits, and then printing fake ATM cards to withdraw money. The regulators used discretionary powers and derived a lesson on the importance of integrity measures.

²⁸ “About Us,” Insurance Institute for Highway Safety, Highway Loss Data Institute, <https://www.iihs.org/about-us>

things in a cost-effective way, what the costs or benefits would be to a shared insurance model, and what its limitations would be.

Assumption 6: Objective third party investigations are more valuable than inside investigations

Many disagreements over the need for additional lesson-learning tools centered on perceptions of adequacy. For example, one participant wrote “root cause analysis is often best done by or close to the people who made and fixed the mistake. It doesn’t need a government agency and results can either be kept in the organization that made the mistake or shared more broadly depending on circumstances.” Others expressed a variety of concerns this strategy raises: while some organizations perform such root cause analysis, not all do. The organizations that perform root cause analysis may not be skilled at it, or they may consider it a formality, best rushed. Those who contributed to a mistake or those close to them may carry biases or be influenced by politics or even personal relationships.

Assumption 7: Legal privilege, lawsuits, and prosecutions will continue to limit the scope and dissemination of most private investigations

When organizations do request a deep investigation, they are often performed under legal privilege with investigators engaged via law firms. Even with legal privilege as a protection, victims are not incentivized to understand why the incident occurred because the “facts” of such an investigation might not be privileged and could be subject to discovery in lawsuits. Findings may become public as part of court cases but that may take a decade or more. Similarly, Federal investigators often produce detailed understandings of adversary activity inside victim systems as part of their investigation. These may also take years to be released in the form of an indictment. Indictments are written to convict criminals, not to help the defensive community learn.

It may be that these concerns could be addressed by public policy. Broad liability protection would obviously be attractive to companies, but legislators are wary of giving blanket protection, and even the more narrow questions of the interaction of state and Federal breach laws continue to fester.

Assumption 8: The Existence of an Intelligent Adversary Does Not Doom a Cyber NTSB

Except for a small number of terrorist attacks, almost all aviation incidents are the result of human or system error, weather events, or mechanical malfunction.²⁹ When aviation incidents are known or suspected to be the result of intentional action, responsibility for the investigation shifts to the FBI, with the NTSB in a supporting role. The presence of active and often determined adversaries may change the dynamic of cyber incident investigations in significant ways.

The existence of an intelligent adversary adds complexity or challenges to each part of the process of investigating cyber incidents but does not mean that such investigations should not be undertaken. Some example challenges include: the discovery of an incident may be impeded by adversaries hiding; analysis may be made more complex by deletion of evidence or by questions of ‘would defense X have stopped them, or would they have found another path?’ Publishing news of a new attacker tactic may lead adversaries to change those tactics. Top intelligence agencies are believed to study defender activities to find ways around them.

It is clear from the literature that those advocating for a cyber NTSB were using the NTSB concept as a rough analogy and that the community readily accepts and expects that a cyber incident investigative board is going to investigate incidents primarily if not exclusively caused by malicious adversaries.

²⁹ “Causes of Plane Crashes: How to Prevent Them?,” Pilot Institute Blog, entry posted June 4, 2020, <https://pilotinstitute.com/plane-crash-causes/>

Discovery and Incident Identification

This section captures findings on how a board can discover that incidents have occurred and how to determine whether they merit investigation. The workshop identified many fascinating research questions, some very broad and others quite specific. For readability, we have enumerated research questions at the end of the document.

How Can A Board Become Aware Of Incidents?

Any investigator needs mechanisms by which they become aware of incidents to investigate. Unlike in aviation or surface accidents, most cyber incidents are not kinetic in nature — there is no explosion or crash site. Therefore, in order for a board to investigate it will first need to discover that an incident took place. In aviation, the existence of pilot certificates and the ability for authorities to revoke them is a powerful incentive for pilots to comply with reporting requirements. Airlines are wary of crossing the FAA. More important, however, is that the lives of pilots, passengers, and people on the ground are at stake in any aviation accident.

In contrast, there is a culture of secrecy around cybersecurity incidents due to fear of liability on the part of companies. Given this reality, the first challenge for any cyber investigative board is going to be discovery.

FINDING: Existing Incident Reporting Mechanisms Could Inform a Board

There are many requirements to report certain cybersecurity incidents to either regulators or the public. Yet there are also broad categories of incidents that do not require reporting and judgement calls that companies can make about when to report incidents. Those judgement calls impose hard-to-measure limits on what fraction of incidents are reported. An

investigation board would likely still have more possible investigations than capacity, but self-reporting would likely have a greater impact on statistical analysis.

- Existing requirements for private firms to report incidents to regulators include the following:
- The Federal Energy Regulatory Commission (FERC) imposes requirements on the electric sector³⁰.
- The Department of Defense imposes requirements for the defense industrial base³¹.
- The FCC has mandatory confidential reporting by telecom carriers of outages that meet certain thresholds³².
- The SEC requires companies to report material risks to their shareholders (and thus the public.)³³
- The Department of Health and Human Services has requirements for notifying both victims and the department when health data is compromised³⁴.
- State laws require notices to victims and sometimes state regulators when personal data is lost. Some states publish these notices.

Whether these notifications to regulators could be shared with the CSRB or another board is an open question, and likely dependent on statutory details. In addition, there are gaps in these reporting requirements. Most intellectual property theft and financial harm never become public and very few incidents are judged to be material under current SEC guidelines.

³⁰ CIP-008-6, Fed. Reg. (June 26, 2019). <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf>.

³¹ 32 C.F.R. § 236.4 (2016). <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-M/part-236/section-236.4>.

³² “Network Outage Reporting System (NORS),” Federal Communications Commission, <https://www.fcc.gov/network-outage-reporting-system-nors>.

³³ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 C.F.R. § 229 & 249 (2018). <https://www.sec.gov/rules/interp/2018/33-10459.pdf>.

³⁴ Notification to the Secretary, 45 C.F.R. § 164.408 (2011). <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.408>.

There is also a widespread belief amongst security professionals that companies actively avoid reporting incidents even when it is required by law.

Best practices for how to report incidents were raised. Two systems in the telecoms industry may be useful analogues. NORS (Network Outage Reporting System) and DIRS (Disaster Information Reporting System) respectively require mandatory confidential reporting when a network is out for more than a given threshold, or when an issue occurs in a given area designated as a disaster zone.³⁵ Design of a reporting system deserves further study.

The requirements for federal agencies to report greatly differ from those imposed on private firms. Federal civilian agencies are required to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA), while defense-related agencies report to DoD. It is likely that Federal agency notifications could be shared.

FINDING: Cybersecurity and IT Lack Incentives for (Effective) Voluntary Reporting and the Levers for Enforcing Mandatory Reporting

There are few reasons to voluntarily report an incident, and attempts to address inhibitors, increase information sharing, or add incentives have not led to significant increases in disclosures. Successive administrations and Congress have taken significant steps to address liability concerns with sharing information on cyber incidents. The Department of Justice and the Commerce Department have clarified that information sharing does not violate antitrust laws³⁶, and the Cybersecurity and Information Sharing Act of 2015, among other laws, has provided strong protections for companies sharing information with Federal agencies.

³⁵ For more information on NORS, see: <https://www.fcc.gov/network-outage-reporting-system-nors>; for more information on DIRS, see <https://www.fcc.gov/general/disaster-information-reporting-system-dirs-0>

³⁶ Federal Trade Commission and Department of Justice, “Antitrust Policy Statement on Sharing of Cybersecurity Information,” news release, April 10, 2014, <http://ftc.gov/news-events/press-releases/2014/04/ftc-doj-is-sue-antitrust-policy-statement-sharing-cybersecurity>.

More attempts to address concerns of liability protection are not likely to increase voluntary disclosure of incidents unless they are explicitly tied to reporting. Liability protection alone is unrelated to reporting and in fact may simply increase the desire for confidentiality or opacity.

FINDING: Board Awareness Could be Enhanced by Individuals Reporting/Whistleblowing

The Association for Computing Machinery Code of Ethics requires reporting of data breaches: “Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation.”³⁷ Yet, it is a truism in cybersecurity that most incidents are never publicly known. In many industrial and technical areas, public policy encourages and protects whistleblowers in various forms. Aviation near-miss reporting is done by individuals, not companies. The ASRS incident reporting form does not even ask about employment. An investigative board could have a hotline for reporting and online collection forms, as well as whistleblowing that the information it is receiving is inaccurate or incomplete. Protections for incident reporters should be clarified.³⁸

Beyond incidents, there are regularly cases where staff believe that a company is not making appropriate investments in security. These investments could be either investments in the security of products it sells, or in the operational systems it uses to deliver to customers. An example

37 Association for Computing Machinery, “ACM Code of Ethics and Professional Conduct,” 2018, <https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf>

38 Ted Knutson, “Thinking about Blowing the Whistle on Your Employer for Cybersecurity Violations? A Minefield Awaits, Warns Expert,” Forbes, May 13, 2020, accessed July 6, 2021, <https://www.forbes.com/sites/tedknutson/2020/05/13/thinking-about-blowing-the-whistle-on-your-employer-for-cybersecurity-violations-a-minefield-awaits-warns-expert/?sh=29ef6136239a> or Dallas Hammer, “Cybersecurity Whistleblowing: What Employees at Public Companies Should Know Before Reporting Information Security Concerns,” ISSA Journal, June 2016, <https://www.zuckermanlaw.com/wp-content/uploads/2014/01/Cybersecurity-Whistleblowing-What-Employees-at-Public-Companies-Should-Know-Before-Reporting-Information-Security-Concerns.pdf>

is the case of SolarWinds employee Ian Thornton-Trump.³⁹ In brief, Mr Thornton-Trump created a 23 page presentation, including the claim that “the survival of the company depends on an internal commitment to security.” There have been calls for Congress to provide whistleblower protection.⁴⁰

FINDING: Reporting forms and taxonomies involve tradeoffs

Having a form to fill out can be attractive to those who have to report because it allows for assurance that all mandatory data elements are included. Generally, there are common elements in each incident, including duration, severity, people involved, if CVEs were noted, reasonable confidence on the geography of the servers/devices and of the attackers/defenders, and so forth. Having a form filled out is attractive to statisticians, who get their data pre-coded by those near the event. Using a standardized form imposes a taxonomy and a view of events, and has consequences on the sorts of analysis that can or will be done.⁴¹ The ASRS system has a small set of checkboxes about the flight and operator, and two open-ended questions:⁴²

- Describe event/situation (“Discuss those that you think are relevant and anything else you think is important. Include what you believe really caused the problem, and what can be done to prevent a recurrence”)
- The form also encourages respondents to “keep in mind the chain of events and human performance considerations.”

39 Ryan Gallagher, “SolarWinds Adviser Warned of Lax Security Years Before Hack,” Bloomberg, December 21, 2020, <https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack>

40 Dallas Hammer, Jason Zuckerman, “SolarWinds Breach Shows Why Cybersecurity Whistleblowers Need Protection”, Bloomberg Law, Feb 2, 2021, <https://news.bloomberglaw.com/privacy-and-data-security/solarwinds-breach-shows-why-cybersecurity-whistleblowers-need-protection>

41 Geoffrey C. Bowker and Susan Leigh Star, *Sorting Things Out: A Revealing and Surprising Look at How Classification Systems Can Shape Both Worldviews and Social Interactions* (n.p.: MIT Press, 2000).

42 NASA ARC 277B, General Report Form (Download and Print version), Aviation Safety Reporting System, <https://asrs.arc.nasa.gov/docs/general.pdf>

The form drives the design of the database; changes to the form require either a process of adjusting older data or understanding that some queries cannot be run across the full historical data. Within the workshop there was substantive disagreement over the costs and benefits of forms and taxonomies. What is clear is that trend analysis, an important function of the actual NTSB and ASRS, would be greatly aided by standardizing reporting forms and taxonomies. It is also clear that such taxonomies would enable some forms of research, and inhibit others. For example, a form could say “did the attacker get in via Hacking social engineering;” or it could say “did the attacker get in via SQL injection buffer overflow phishing sophisticated methods.” The structure of a form represents the expectations of the creators of the form, and so there is a tradeoff between trend analysis and other goals.

How Should a Board Select What to Investigate?

There are a lot of cybersecurity incidents. For an indication of the scale, in the second half of 2018, 41,502 breaches were reported to European authorities under the General Data Protection Regulation.⁴³ While we are not aware of such a cross-sectoral, broad-based number for the United States, it is likely that similar reporting criteria in the United States would produce a comparable number of breaches. Even with limited awareness, there are too many incidents to investigate each one. Thus, investigative bodies will require clear criteria for selecting incidents to investigate.

FINDING: A Board will require criteria for selecting events to investigate

In the creation of the CSRB, the President established criteria for its reviews that are tied to the standup of the Unified Coordination Group

⁴³ Supreeth Shastri, Melissa Wasserman, and Vijay Chidambaram, “GDPR Anti-Patterns,” Communications of the ACM, February 2021, <https://cacm.acm.org/magazines/2021/2/250081-gdpr-anti-patterns/fulltext?mobile=false>

(UCG) under PPD-41's definition of a significant cyber incident.⁴⁴ The executive order also makes clear that the President and the Secretary of Homeland Security may direct an investigation⁴⁵. While these definitions and triggers make sense, adding more quantitative or objective measures may be appropriate.

For example, a threshold of investigation of USD 20 million would result in roughly 50 investigations over 5 years.⁴⁶ Separately, the personal information of 10 million people may be an appropriate starting point. It may also be prudent to require investigation of any incident that results in loss of life or any incident that disrupts critical infrastructure. However, these factors may not be the only ones that are sensible. For example, in 2020, Vastaamo, a Finland-based company focused on providing mental health counseling, was targeted in a ransomware attack that resulted in 40,000 psychotherapy patients having their medical records compromised. According to Vastaamo, the attackers leaked 300 patients' therapy session notes and held numerous others' for ransom, threatening to release their medical information.⁴⁷ Such an event could warrant the attention of a board.

FINDING: NTSB Investigates "Trends" and Incidents

The NTSB is well known for investigating accidents. Less well-known is that the NTSB also investigates trends. For instance, in the early 1990s, the NTSB investigated why improvements in aviation safety were plateauing. Given the growth in the industry, without continued reduction in the rate of crashes, a continual string of incidents would have scared the general

44 Memorandum by Barack Obama, "Presidential Policy Directive -- United States Cyber Incident Coordination," July 26, 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

45 Exec. Order No. 14028 Fed. Reg. (May 17, 2021), <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

46 Cyentia Institute, Iris 20/20 Information Risk Insights Study, [Page 5], 2020, <https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf>

47 Lindsey O'Donnell, "Vastaamo Breach: Hackers Blackmailing Psychotherapy Patients," Threatpost, October 26, 2020, <https://threatpost.com/vastaamo-hackers-blackmailing-therapy-patients/160536/>

public away from flying even if incidents were not occurring at a higher rate.

There is currently no entity charged with identifying common cybersecurity failures that if corrected could prevent broad, ecosystem failures as a matter of public good. A goal could be to identify what are the common failures. For instance, a board might examine data from the Verizon Data Breach Investigation Report⁴⁸ that identifies trends in attack patterns and might seek to understand what can be done to address these patterns. It could analyze claims that a particular defense is “easy” to deploy and identify and assess reasons that it was not. It might also analyze claims that a particular defense “would/could” have stopped a given attack. A board could also investigate trends in the adoption or the failure to adopt technologies with proven security benefits.

Investigation

Once a board has identified an incident worthy of review, it will need to investigate the incident in order to produce findings and recommendations for the victim, defenders, regulators, and the wider community. This

⁴⁸ Verizon, 2021 Data Breach Investigations Report, <https://www.verizon.com/business/resources/reports/dbir/>

section provides an overview of findings from the workshop on how investigations should be structured and the capabilities and authorities necessary to carry them out.

How should investigations run?

Different kinds of investigations will require different skills to conduct, including technical, investigatory, and legal skills. Some investigations will require more legal knowledge, especially as not all investigations will be necessarily cooperative or voluntary. Some will require advanced technical and forensic knowledge. Flexibility will be needed in the allocation and use of resources in these investigations.

FINDING: Subpoena Authority Will Likely Be Necessary for a Board to Succeed

While the CSRB may be able to gain participation from affected parties in the SolarWinds incident, in other, lower-profile incidents where the victims have not been as forthcoming, it is likely that an investigation for the purpose of extracting and publicizing lessons learned will require a degree of the heavy arm of the state. The NTSB has the authority to compel witnesses to testify and to subpoena documents.⁴⁹ While these authorities are a crucial backstop, the aviation community tends to work in a spirit of community interest in making flying safe and is forthcoming with materials, witnesses, etc. We can hope that with sufficient authority behind it, the CSRB or any subsequently created investigative entity could also operate in the same cooperative manner that the NTSB enjoys.

⁴⁹ National Transportation Safety Board, Aviation Investigation Manual Major Team Investigations, November 2002, at 4.8, <https://www.nts.gov/investigations/process/Documents/MajorInvestigationsManual.pdf>

FINDING: Fact-Finding Should be Collaborative but Analysis Independent

In aviation incidents, many members of the aviation community may contribute to fact-finding. This process is carried out through a “party” system in which the NTSB will designate organizations and individuals that are relevant to the investigation as “parties”. The parties help develop the timeline of the incident and provide technical expertise related to investigation. These parties, however, are excluded from the NTSB’s analysis and recommendation development and do not review or contribute to the final report, though they may submit their own recommendations for consideration.⁵⁰ It should also be noted only individuals with relevant technical expertise are allowed to represent an organization in an investigation, while attorneys and insurance investigators are prohibited.⁵¹

It is important to note that the parties should be read broadly: in a plane crash, it is not just the airline, but the airplane manufacturer and their suppliers whose parts may have been faulty, mis-installed, or poorly maintained. Each of these has a responsibility to make parts which are “fit for purpose,” and there will be nuance in bringing that to the security of software. Issues will include changing threat landscapes, discovery of new attack patterns, response to such discovery (it may be impossible to create an update which is both compatible and more secure), and the obligations of the creators of open source software.

An incident like SolarWinds illustrates a challenge to the party system. In an NTSB investigation, there may be a few parties: the airline, an airport, the pilot’s union.⁵² In SolarWinds roughly nine federal agencies and one

⁵⁰ National Transportation Safety Board, Aviation Investigation Manual Major Team Investigations, November 2002, at 4.10 and 4.12.2, <https://www.nts.gov/investigations/process/Documents/MajorInvestigationsManual.pdf>.

⁵¹ National Transportation Safety Board, Certification of Party Representative, November 2002, https://www.nts.gov/legal/Documents/NTSB_Investigation_Party_Form.pdf

⁵² FAA Office of Aviation Policy and Plans, Economic Values for FAA Investment and Regulatory Decisions, A Guide: 2021 Update, Section 8: Aviation Accident Investigation Costs [7], March 2021, https://www.faa.gov/regulations_policies/policy_guidance/benefit_cost/media/econ-value-section-8-accident-investigation-costs.pdf

hundred companies were broken into, and thousands impacted.⁵³ Even the former group might stretch the norms of the party system, or the capacity of an agency to collect and process reports on a rapid basis.

FINDING: Investigator independence produces different recommendations

For a major attack by a motivated adversary, there may be several unrelated investigations, and those investigations probably serve different interests. For example, the victim may have hired a commercial incident response firm; their insurers may have hired another, each of which will perform a direct analysis of impacted systems. Simultaneously, the FBI might be investigating the crime, and be sent a “law enforcement referral package,” and the intelligence community may be engaged in either a surreptitious attempt to discover what’s happening, or a more noticeable “sending a message” activity. All of these stakeholders in an investigation have motivations and fears, and these inevitably influence the direction, management, and resourcing for investigation, as well as the product of the investigation, including framing, findings, and recommendations, and the distribution of the investigatory products. Investigations by victims, insurers, and regulators each have a place, and their dynamics and outcomes are different from investigations that run independently of them.

Independent investigators, charged with improving public understanding or improving the safety, security, or resilience of systems will investigate differently, and produce different results. For example, they may look at contributing factors differently, and be more interested in facts than fault. Independence of analysts is crucial for the investigation of high-impact incidents. Without independence, decisions that may have contributed to the incident may never be re-examined. As an example, we talk a great deal about “vulnerabilities,” the technological issues that attackers exploit.

⁵³ Jen Psaki and Anne Neuberger, “Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021,” news release, February 17, 2021, <https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/>

But the computer industry tends to discount issues caused by human action, like clicking on a link in email, while disregarding that there is no actionable advice on how to choose what links to click that can be followed in a reasonable amount of time. An independent analysis might lead to a deeper understanding of contributing factors.

There are regular attempts by regulators to obtain factual knowledge. For example, in June 2021, the SEC sent a letter to companies that may have been impacted by SolarWinds.⁵⁴ A Reuters news story said “If the issuers and investment firms respond to the letters by disclosing details about the breaches, they would not be subject to enforcement actions related to historical failures, including internal accounting control failures, the people said.” (The article is unclear if “people” means SEC staff.) It is unlikely that an anonymous quote in a news article will result in lawyers recommending full transparency and meeting the SEC’s goals.⁵⁵

Throughout this report, we have asked questions such as “who would benefit from independent analysis” and “what are the existing mechanisms for the delivery of such information”? Implicit in that formulation is an underlying conclusion that we now make explicit – there is a value to having a neutral, independent source of analysis and a Cyber NTSB is a likely storehouse for that value.

That instinct that a “ground truth” would be useful lies behind, for example, the related suggestion for an international attribution consortium – and it is equally applicable here.⁵⁶ It seems likely that a respected, neutral, independent, and experienced source of incident analysis would provide a value-add to any number of stakeholders and that the lack of such a source is restraining policy development that may be dependent on such a source.

54 Katanga Johnson, “U.S. SEC Probing SolarWinds Clients over Cybersecurity Breach Disclosures – Sources,” Reuters, June 22, 2021, <https://www.reuters.com/technology/us-sec-official-says-agency-has-begun-probe-cyber-breach-by-solarwinds-2021-06-21/>

55 Ibid

56 Microsoft, An Attribution Organization to Strengthen Trust Online, <https://www.microsoft.com/en-us/cybersecurity/content-hub/an-attribution-organization-to-strengthen-trust-online>

FINDING: There is value in slow, careful investigations

There is also an issue of speed: the value of rapidly producing reports and sharing indicators or TTPs⁵⁷ is understood, but what possibilities could more careful analysis illuminate? For example, NTSB reports can take years to come out, while the Executive Order required a report on SolarWinds within 90 days of the standup of the board. We believe it would be to the public benefit to make such choices with a more explicit understanding of what a longer, more costly investigation might reveal.

Also associated with the drive for fast investigations is a widespread belief that “cyber is fast moving,” but that belief is rarely quantified other than to describe the increasing number of devices on the web or the number of hostile attacks using specific cataloged vulnerabilities. At a less granular level, e.g. stack smashing versus heap overflows or phishing for credential theft or delivery of exploits, the change seems to be quite slow.

During the workshop, we characterized investigation speed into fast, medium, and slow, as shown in Table 1: Speed-Action. Each type of investigation has useful outputs, and the outputs serve different purposes.

⁵⁷ “Indicators” are technical details like an IP address or domain name used by an attacker. TTPs refers to “Tactics, Techniques, and Procedures” meaning the details of how a particular attacker tends to operate.

| | Quick | Medium | Slow |
|-------------------------------|---|---|--|
| Questions | What incidents are happening? | What went wrong? | Which controls worked? Which failed? Which had some effect? What product design decisions, configurations or defaults played a role? What contributing factors were involved? |
| Actions by defenders | Use indicators to find attackers. | What tactics, techniques and procedures should we look for? | How should we adjust our controls? Should we change our strategy? Should we acquire different products, or require changes from manufacturers? |
| Actions by product developers | Add indicators to intelligence, detection products. | Adjust product features, configurability, or defaults. | Develop new products, or change the design or architecture of products. |
| Actions by standards groups | None. | How do we adjust recommended policies & procedures for use? | How do we update our standards & requirements? What integration capabilities between products either limit or could enhance the security of systems? |

Table 1: Speed-Action

Longer, more thorough investigations that may require deeper systems and network forensics, more interviews, or more analysis may yield the most value. At the same time, following the model of the NTSB, boards should release preliminary findings and recommendations as soon as they can. Final reports can explicitly correct the record. We hope the Federal response to the SolarWinds incident will model this kind of effort.

The in-depth investigation that FireEye conducted into its own breach was intense and thorough but focused on understanding how the attacker gained access. By deeply investigating an apparently minor incident, FireEye found an unexpectedly substantial compromise within their organization. What apparently started as a single multi-factor authentication failure led their investigators to identify what we now call “the SolarWinds incident”, one of the most far-ranging espionage campaigns of the cyber era. Had they chosen not to investigate why there was a failed attempt to add a multi-factor device, we might still be unaware of this campaign.

As an investigations firm, they have access to tools, skills, and baseline information which make such an investigation easier and more productive. It is unclear what led to their persistence in this case, or how often such persistence pays off. It is also unclear how much the investigation would have cost if they had performed it for a third party. FireEye’s CEO has said that over a weeks-long period the company had “over 100 of our employees working virtually around the clock” on the investigation⁵⁸. What FireEye has not shared is what tools and controls failed to stop or detect the adversary. While FireEye deserves credit for the investigation, they also had a vested interest in sharing limited information with the public and other cybersecurity companies and did not share details on why their other tools failed to detect the incident, demonstrating some limits of in-house investigations. The CSRB or other investigative boards could potentially continue this investigation.

⁵⁸ “Prepared Statement of Kevin Mandia, CEO of FireEye, Inc. before the U.S. House Committee on Oversight and Reform and House Committee on Homeland Security,” House Committee on Homeland Security, last modified February 26, 2021, <https://homeland.house.gov/imo/media/doc/Testimony-Mandia.pdf/04/Testimony-Mandia.pdf>.

What should a board investigate?

A board should investigate all of the facts surrounding an incident, including at least what happened, how it happened, and how it was discovered and addressed. Some of the answers will be technical: data produced by software, and actions software took. Other answers will be decisions and actions taken by people. Both are relevant to understanding the incident.

FINDING: Product, Tool, and Control Failure Are All Important, and Rarely Investigated or Reported

The CSRB or any other board should not be shy about identifying when tools failed to detect the kind of behavior that they were designed to detect, or prevent the things they were marketed as protecting against. Some of those failures will be that products were designed to resist or detect this kind of malicious activity, and did not. Another failure may be that security was not considered in product development. Those failures may include poor design, difficulty in deployment, configuration, use or response. We know from aviation that each of these can be a contributing factor for real world incidents. There may also have been issues in integration between tools. Analysis by one cybersecurity vendor shows that many common endpoint detection and response tools were circumvented by the adversary in the SolarWinds case.⁵⁹ We can also assume that many network tools and deception tools also failed to pick up signs of the activity. Discovering and stating the facts around these tool-centered contributing factors should be a component of the final report.

Similarly, it is likely that investigations will find that standardized security controls were not properly implemented or that guidance was insufficient. Thus, investigators should pay particular attention to how the implementation of controls failed and make recommendations for clarifying or expanding controls.

⁵⁹ James Haughom, "SolarWinds SUNBURST Backdoor: Inside the APT Campaign," Sentinel Labs, last modified December 18, 2020, <https://labs.sentinelone.com/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/>

FINDING: A Board Can Discover why seemingly obvious improvements are not adopted

There are many apparently obvious solutions to commonly experienced security problems which are not in use. (These are often labeled as “hygiene” or “security 101”). There are rules-of-thumb in security which seem obvious, like ‘patch your systems.’ Applying patches can be complex or risky,⁶⁰ and it can be more time-consuming than expected. Understanding why apparently cost-effective and sensible security fixes are not immediately adopted is an extremely important function a board could address, and it may also be a research goal. Again, there is tension over when or how or if the board should consider counterfactuals, hypotheticals and what-ifs.

FINDING: NTSB Evaluates Regulators and Regulations

While the NTSB is not a regulator, it does play a crucial role in evaluating the role of regulators and regulation as a part of investigations. The NTSB evaluates both whether regulatory requirements are sufficient and clear and whether regulatory audit and enforcement functions were operating well surrounding an incident. Thus, one important reason the NTSB is independent is so that it can criticize the actions of regulators and identify gaps in their regulations. This finding is important for the development of the CSRB as its host agency, CISA, as well as other Federal regulators may come under scrutiny. A cycle whereby the CSRB is continually evaluating and helping to improve the work of Federal agencies as they support private sector organizations should be encouraged.

⁶⁰ Steve Beattie et al., “Timing the Application of Security Patches for Optimal Uptime” LISA XVI, Philadelphia, PA, November 3-8, 2002), <https://shostack.org/files/papers/time-to-patch-usenix-lisa02.pdf>

What investigative techniques should be used?

There are many styles of investigation and analysis. The NTSB uses a party system in which it formally designates organizations or individuals as parties to the investigation. Investigating failures in complex, high reliability systems is a skillset that must be developed. The absence of single points of failure is a hallmark of a high-reliability design. And so failures in such systems rarely have a single “root cause,” and investigators look at contributing factors, including human factors and control failures. They use techniques that look to delve deeper than finding a root cause or operator error.

FINDING: “Contributing Factors” is a better approach than Root Cause Analysis

Aviation and other high safety fields have eliminated single points of failure, and as such, there never is a single root cause but rather a series of “contributing factors.” The tradeoffs in investigative structures that try to understand the causes of incidents and prevent their emergence elsewhere have been studied deeply in the context of safety, reliability, and resilience. A series of “contributing factors” likely led to the ultimate bad outcome. In some cases, correction of any single contributing factor may have prevented the bad outcome.

In contrast, cybersecurity professionals often focus on understanding the “one thing” that led to an incident. For example, guidance from the Center for Internet Security and the Department of Defense both call for incident investigators to understand “root causes.”⁶¹

⁶¹ Department of Defense, Cybersecurity Maturity Model Certification (CMMC) Version 1.02, March 18, 2020, [IR 2.097], https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; Center for Internet Security, CIS Controls Version 8, [16.3], <https://www.cisecurity.org/controls/v8/>. Root cause analysis, as called for in both the CMMC and CIS Controls, is important for treating cyber incidents as isolated events rather than as a systemic issue.

IR 2.097 in NIST CMMC and CIS 19.6 are both about “root cause” vs. “contributing factors”. Root cause analysis is, as previously mentioned, often part of treating cyber incidents as isolated instead of systemic.

It is important to recall that security has adversaries that safety does not, and adversaries may adapt. A determined adversary will adapt to the barriers they encounter, with various levels of success. Some participants made arguments for considering the controls which were not implemented, or features that “should” have been built into products. Others expressed concern that that would be a license for speculation and could undercut the fact-driven nature of an investigation. The CSRB should keep this finding in mind as it investigates the SolarWinds Incident and incidents in the future.

FINDING: “5 Whys” Analysis is an important tool

One of the benefits of the NTSB style of analysis is that very few things ever trace back solely to “pilot error,” because it usually takes a chain of events and multiple inputs to create a catastrophic error in a resilient system. That is acknowledged in aviation, but somehow, in cybersecurity, there always seems to be one single person who made one single catastrophic error, and blaming/firing them solves the problem entirely. Perhaps relatedly, large company Chief Information Security Officers have a stunningly short average tenure of 26 months.⁶²

A 5 whys analysis consists of repeatedly asking why and applying some judgment to when to stop. Other than that, it’s much like being around a three-year-old. For example, there was a memory-based buffer overflow. Why?

- Because Adam wrote a bad line of code. Why?
- Because it’s hard to use `strncpy`. Why don’t we remove those? ⁶³
- Because there’s an awful lot of them. Why can’t we do it anyway?

⁶² Caitlin Cimpanu, “Average Tenure of a CISO Is Just 26 Months Due to High Stress and Burnout,” ZDNet, last modified February 12, 2020, <https://www.zdnet.com/article/average-tenure-of-a-ciso-is-just-26-months-due-to-high-stress-and-burnout/>

⁶³ The C language has a function call, `strncpy`, which copies “n” characters from one string to another, and is known to be hard to use safely. Modern systems have replacements which are better designed.

One participant suggested that the result of such a 5 whys analysis would always be “because the code was written in C, and should be re-written in a memory safe language.” Such an outcome would be about as useful as “don’t fly in snowy conditions.” In practice, the NTSB might find fault with a pilot for flying in Instrument Meteorological Conditions without an instrument rating, and ASRS has issued a good deal of guidance about effective de-icing practice. Like other analytic techniques, “5 Whys” should be treated as a guide, not a constraint.⁶⁴

FINDING: Human Factors Should Be Included but “Human Error” Should be Discounted

Overworked engineers or systems administrators — much like a pilot flying on too little rest— are likely to be important contributors to incidents. Bad system design, lack of planning, poor usability, and notification fatigue may be contributors to incidents. Systems design, management prioritization, and security culture will also be contributors. Do job requirements explain a safe route to completion? For example, if someone is processing invoices, their job involves a constant stream of opening documents from new correspondents outside the firm. Is there a documented way to do so safely, and has that person been trained in what to do if something suspicious happens? Are they rewarded for raising concerns?

It is common to see the passive voice or a deflection used when describing how incidents occur in technical cybersecurity issues or malfunctions. An example of this is found in a news story about an incident and its post mortem. The issue was a change pushed out by a single engineer – who was subsequently blamed for the resultant outage.⁶⁵ In that article, an executive is quoted “For whatever reason that we don’t understand, the employee decided to do a global deployment.” A commenter explained it as, “Someone was breathing down their neck to get the release out there NOW and we don’t want to name them.”

⁶⁴ Alan J. Card, “The Problem with ‘5 Whys,’” *BMJ Quality & Safety* 26, no. 8 (July 20, 2017), <https://qualitysafety.bmj.com/content/26/8/671>

⁶⁵ Richard Speed, “That Salesforce Outage: Global DNS Downfall Started by One Engineer Trying a Quick Fix,” *The Register*, May 19, 2021, https://www.theregister.com/2021/05/19/salesforce_root_cause/

Blaming a single engineer in a large company is not just an oversimplification. There is often pressure from above, or systemic or cultural pressure to operate according to custom that causes this kind of error. The public “root cause analysis” provided by the company above does not actually state why the change was done in the way it was done, which is an obvious next question if using a “5 whys” style of analysis that could actually help prevent future incidents of this type.⁶⁶

⁶⁶ “Multi-Instance Service Disruption on May 11-12, 2021: Knowledge Article Number 000358392,” Salesforce, last modified June 28, 2021, <https://help.salesforce.com/articleView?id=000358392&type=1&mode=1>

Reporting and Data Usage

Any investigations board will maximize the impact of its investigations by publishing its reports to the extent practicable. Independent, thoughtful and reliable investigations are rare in cybersecurity. There is a lack of reliable data about incidents that can be used to build a coherent and consistent narrative about what has actually happened in cybersecurity, much less around which to build policy and incident response plans. Often, when reliable data is produced, it can disappear as links rot on the internet. There are few sources of truth, and little incentive to build careful history.

What values can be improved by public reporting?

There is value in a shared narrative about the major events in cybersecurity. The lack of a shared set of facts of an incident in the immediate aftermath of that incident means that the defender community is often attempting to shift tactics and implement tools in response to an incident that they do not fully understand. In the case of the 2011 RSA hack, there was a great deal of contemporaneous reporting. However, a decade later when non-disclosure agreements expired, important new facts emerged about that incident. That reporting states multiple opportunities to detect and stop the attacker were missed. Many of these mistakes happened prior to the loss of the seed values for the then-heavily-relied on authentication devices sold by RSA.⁶⁷ Rapid investigation with published results would have proved valuable. In many ways, the snarky Twitter hot take can appear to be the extent of analysis that's published. Frequently, a claim is put forth that something that wasn't done was "security 101." It is unfortunately rare that those making those claims point to a list, such as an actual introductory ("101") course. The disrespect and snark that are often heaped on victims are not helpful. Respectful, thoughtful analysis is rare.

⁶⁷ Andy Greenberg, "The Full Story of the Stunning RSA Hack Can Finally Be Told," Wired, May 20, 2021, <https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/>

FINDING: Cybersecurity lacks objective, preserved records and history

One of the under-appreciated aspects of NTSB reports is that they are authoritative, concentrated, and factual history. Even though airplane crashes are heavily reported in local, national, and international news, those reports are sometimes incorrect, frequently incomplete, and their accessibility in five to ten years may be limited.

Recently, one author spent a good few days trying to track down some facts related to Stuxnet, widely considered to be one of the seminal international cybersecurity events of 2010 because of its use of several 0-day vulnerabilities. The details were in a set of blogs, tweets, and corporate reports, some of which were even still accessible via the internet archive.⁶⁸

At the moment, no one is charged with producing and maintaining authoritative reports. The technical reports that do exist are gathered in personal repositories or corporate blogs, and tend to disappear over time, while some less authoritative or more sensational reporting in traditional news venues may preserve inaccuracies far longer.

FINDING: How organizations select and prioritize controls is hampered by the lack of authoritative data, narrative, and analysis

Industry participants assured us that they know what goes wrong and what to do about it. Insurers told us that one of the values they deliver is help in getting management buy-in for those things. Stories of management refusal to fund technology maintenance or upgrades are legion.

As we were writing this report, the White House issued a memo, “What We Urge You To Do To Protect Against The Threat of Ransomware,” containing five items “*we urge you to do now*,” and four “high impact steps” that

⁶⁸ See also Jonathan Zittrain, “The Internet Is Rotting,” *The Atlantic*, June 30, 2021, <https://www.theatlantic.com/technology/archive/2021/06/the-internet-is-a-collective-hallucination/619320/>

companies should take.⁶⁹ The letter does not contextualize these controls to other advice from the US Government, such as NIST CSF, NIST 800-53, FedRAMP or CMMC guidance. The steps listed seem like fine steps to take, but prompt the question “*why are these things not already being done?*” Are corporate executives unconvinced that backing up data and testing those procedures is necessary? The mention of the step in a White House memo suggests that it may be being lost in the noise, not funded, or otherwise not prioritized and properly deployed.

It is likely that the CSRB will find that products were not designed with security in mind, that they were misconfigured, or that commonly accepted cybersecurity controls were not effectively implemented. The CSRB should not stop its analysis there. Cybersecurity controls, even at the most well-intentioned companies, are often not rigorously, completely or comprehensively implemented. They may lack precision or they may not be realistic in operational settings. The CSRB should make recommendations to all regulators on how specific controls should be revised. These recommendations should be made public and catalogued so that industry can evaluate and adopt them ahead of their formal acceptance by these bodies or by regulatory agencies.

As with the work of the actual NTSB, it is likely that much of the time investigators will conclude that existing and known controls were not in place or that these controls were improperly configured and tested and may make recommendations to the victim rather than recommendations to product developers, systems integrators, regulators, standards organizations, or the community at large; however, there will also likely be a smaller set of incidents where clarification or revision of product requirements or control sets will be merited or new controls deemed necessary.

⁶⁹ Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, to Corporate Executives and Business Leaders, memorandum, “What We Urge You to Do to Protect against the Threat of Ransomware,” June 2, 2021, <https://s3.documentcloud.org/documents/20796933/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware17.pdf>

FINDING: There is a need for both narrative and numbers

There are many reporting systems that produce statistics, and many that produce narratives. Each serves a purpose. Few produce both. This relates to the speed of investigation: if most data is collected into a form, then statistics are easy; if data is gathered via interviews, logs, and other less structured data, that enables narrative output and different questions. Table 2: Independence and Blame was generated during the workshop by one of the organizers to help make sense of the information and tradeoffs.

| | Company control | Depth/Cost ⁷⁰ | Finding Facts or Faults? |
|-------------------------|-----------------|--------------------------|---------------------------------------|
| Post-mortem | High | Low | Either (depends on entity's practice) |
| Blameless retrospective | High | Low | Learning (facts) |
| Audit | High | Low | |
| Whistleblower hotline | Medium | Medium | |
| Courts | Low | Very high | Blame (faults) |
| NTSB investigation | Very low | High | Learning & sharing |
| 9/11 Commission | Very low | High | Learning & sharing |
| Vendor driven analysis | High | High | Learning & sharing |

Table 2: Independence and Blame

Statistical questions such as “*how many BEC (Business Email Compromise) attacks took place in 2020*” or “*how many ransomware payments took place in May, 2021*” use implicit, but important taxonomies of what attacks are; further, the frequency of expected reporting is important to designing the reporting mechanism. Forms that are expected to be handled routinely need to be smaller and require different training or support than preparation to testify under oath before investigators.

⁷⁰ As depth and cost increase, the number of investigations which are feasible decreases.

There are many questions that could be addressed by statistical analysis:

- What attacks work in 2021?
- How much is the “physics” of attacks really changing and how quickly?
- Do attackers need to win once, or must they achieve repeated wins?
- What product features are frequently attacked? Are there configuration settings which are hard to set or check? Are the defaults on those set securely?
- What products are attacked most frequently? Are those numbers related to market prevalence, and if not, what might we learn?
- What common controls don’t seem to matter (in preventing breaches or rapidly recovering from them?)
- What uncommon controls seem to help (for example, call attention to attacks more rapidly or provide unexpected benefits in remediation)?

These questions are speculative, and can be enabled by deeper research questions.

Tensions persist, including security, transparency, and blame

Cybersecurity professionals often communicate with each other, and not the general public. Communication skills are absolutely vital in conveying the gravity and long-term meaning of incidents while also protecting victims and the privacy of those involved.

FINDING: Blame and learning are in tension

Participants framed investigation in two distinct ways: blame and learning. (Also referred to as “fact-finding vs fault-finding.”) Perhaps unsurprisingly, and to simplify, lawyers were focused on blame (lawsuits, fines) and engineers were focused on learning from mistakes. No participant offered a system that does both, although in writing this report, the post-Apartheid Truth and Reconciliation Commissions was raised as a potential model. It is unclear how they might be ported to cybersecurity. It seems likely that a focus on either blame or learning is a policy choice for those designing the systems and being explicit about the choice, and its impact on the overall system will be useful.

FINDING: Knowledge and wisdom must be accessible to all audiences

Clear writing educates the reader, and clear writing about technology is rare. If reports contain knowledge that’s hidden behind jargon, it does not convey that knowledge. The NTSB may exhaustively detail mechanical failures and human failings. But they do so in accessible language. They explain what happened, why, and make recommendations on how to prevent it from happening again. The CSRB should invest in great writers, and resist the temptation to stifle them, require the passive voice of them, or otherwise produce bureaucratic pablum.

As cybersecurity grows in importance and scale, the need for a shared understanding of incidents that is communicable in standard terms to a lay audience grows as well. Sometimes the technical details of vulnerabilities are well documented, but the context is missing or obscured by a deluge of detail.

FINDING: Parts of reports may not be appropriate for public distribution

Workshop participants had widely diverging opinions on the need for public distribution of information about breaches. The default information

sharing choice for the NTSB is total public distribution, but there are exceptions made for things like pilots' last words to families. There were strong reasons given to both treat much of the analysis of given incidents as confidential by default as well as making all of it public by default and this conversation led to interesting future questions about what kinds of information should be made public and which can be kept confidential without decreasing trust in the system.

Conflict over the role of confidentiality of security information has been explicit for over 100 years.⁷¹ The CSRB or any board will need to grapple with its default policy, and the exceptions it will make. The NTSB publishes all the facts and has a shortlist of things it won't publish, such as cockpit recordings. There were certainly distinct perspectives on this approach amongst the participants, ranging from "protect the victims of crime" to "enable learning."

An example issue to be decided: If a system operator has made a difficult-to-adjust decision about security, should the board obscure that fact? For example, if a company has a "flat" network⁷², should the board avoid mentioning that? What if the design choice is replicated across an industry, perhaps because of some recommendation from an influential manufacturer? If the company doesn't use multi-factor authentication, should the board say nothing about that? In each of these instances, it seems that an attacker will quickly and easily discover those, and for the board to note the fact of the decision and its impacts seems reasonable.

Given these considerations, the CSRB should consider releasing public reports with classified appendices.

71 At least since Kerckhoffs expressed as a principle that "[a] system must not require secrecy and can be stolen by the enemy without causing trouble," as translated by Fabien Petitcolas. See Fabien Petitcolas, "Kerckhoffs' Principles from 'La Cryptographie Militaire,'" The Information Hiding Homepage, <https://www.petitcolas.net/kerckhoffs/index.html>

72 A flat network is one without internal controls, like firewalls. The systems containing things like financial information or customer data are accessible from every point in the internal network. This is usually seen as poor security, and it is common because it is easier to configure.

Near-Miss Reporting and Investigations

Throughout the workshop, the concept of near-miss reporting in aviation was continually raised as an analogy and this analogy was thoroughly explored in one session with the head of ASRS. American aviation has a successful model for learning from near misses, and that model has been adopted by both other countries and other sectors. Many of the issues with investigating incidents are simpler when at least one control has worked.

Finding: Near Miss Reporting Can Complement Incident Investigation

Many of the factors that make investigation of and reporting on incidents complex or difficult are either missing or reduced in studying “near misses”. Near misses are situations in which at least one control failed but a bad outcome was avoided. The success of a control means there is a lower likelihood of a lawsuit, and the victim can tell a positive story about controls succeeding.

Lawyers are less concerned, and attackers know there’s a chance they were caught, etc.⁷³ Companies may even seek positive press coverage from the event as one did when writing a blog post about how they stopped the SolarWinds intrusion after their security product detected the malicious behavior. While they deserve credit for stopping the intrusion, if they had shared the near miss more widely or investigated it more deeply, it is possible that the investigation and sharing of the information discovered in that investigation could have revealed the campaign sooner. While they traced the compromise back to the SolarWinds server, they did not

⁷³ Jonathan Bair et al., “That Was Close! Reward Reporting of Cybersecurity ‘Near Misses,’” Colorado Technology Law Journal 16, no. 16.2 (January 2, 2017): http://ctlj.colorado.edu/wp-content/uploads/2021/02/16.2_4-Shostack-8.7.18-FINAL.pdf

conduct the kind of in-depth investigation into how the incident occurred and thus did not uncover the enormity of the problem.⁷⁴

ASRS receives roughly 100,000 near miss reports per year for aviation safety. These reports are incentivized, and treated confidentially, including rapid anonymization to ensure that the system does not retain identifiable details that would be discoverable via subpoena. This leads to an investigation that is quantitatively and qualitatively different from those conducted by NTSB.⁷⁵

Today in cybersecurity, there are systems such as MITRE's ATT&CK which are fed by both near misses and real attacks. The addition of near-miss data aids in the anonymization and obfuscation of victim identities, and reduces concerns about "tipping off the attacker." It is worth noting that not all near misses or even incidents are caused by "attackers." For example, a journalist discovering that a cloud data store containing sensitive personal information was exposed is likely an incident under a variety of laws.

Finding: Near Miss Reporting Can Lead to Discovery of Incidents

Today's regulatory regime incorporates many requirements for near-instant reporting of problems. (For example, the US Treasury proposed requiring a report within 36 hours⁷⁶, CISA requires a report of potential issues **within one hour** [bold in original]).⁷⁷ Some of these incidents turn out to be near misses once further investigation returns results; some incidents

⁷⁴ Nimesh Arora, "Palo Alto Networks Rapid Response: Navigating the SolarStorm Attack," Palo Alto Networks Blog, December 22, 2020, <https://www.paloaltonetworks.com/blog/2020/12/solarwinds-statement-solarstorm/>

⁷⁵ Two of the report authors have done work on adapting this approach to cybersecurity. *Supra*, 64.

⁷⁶ Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, Fed. Reg. 2299 (Jan. 12, 2021) (to be codified at 12 C.F.R. pt. 53, 225, 304). <https://www.federalregister.gov/documents/2021/01/12/2020-28498/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank>

⁷⁷ U.S. Computer Emergency Readiness Team, US-CERT Federal Incident Notification Guidelines, U.S. Cybersecurity & Infrastructure Security Agency, April 1, 2017, <https://us-cert.cisa.gov/incident-notification-guidelines>

initially thought to be near misses turn out to be real incidents. Policy goals including notification, fast response, and statistical analysis may well be served by integrating reporting, support and routing for investigation and follow up into a single point of contact. Such a “desk” could pass notifications to the right places, provide coordination, and follow up with reporters to learn more. Especially if the reports are made available to all appropriate regulators, treating a single report as evidence of good faith intent to comply with reporting regulations could meet policy goals of transparency while reducing burden on incident responders.

Research Agenda

The primary goal of this workshop has been to identify research questions around adapting lesson learning systems from aviation, and we have identified a great many such questions, spanning the hard and social sciences. We are also very aware that these lesson learning systems have an opportunity to act as “platforms”, enabling further research. Doing so is, of course, not free, and in this section, we lay out a series of recurrent issues that we could not resolve within the workshop and that require further analysis and science. We then set out specific research questions tied to each section of the report.

Recurrent Issues and Themes

There were a set of recurrent issues which we grappled with through the workshop. They include:

- The intelligent adversary problem
- Complexities of the regulatory context
- Framing of safety, security, systems or resilience
- Organizational structures of boards
- Costs and benefits of investigative boards
- Access to data

Each deserves its own workshop and research agenda.

The Intelligent Adversary Problem

The NTSB investigates accidents; criminal and/or terrorist activity is outside their remit. The existence of an intelligent adversary in cyber incidents adds complexity or challenges to each part of the process.

Some examples include: the discovery of an incident may be impeded by adversaries hiding; analysis may be made more complex by deletion of evidence or by questions of ‘would defense X have stopped them, or would they have found another path?’ Publishing news of a new attacker tactic may lead adversaries to change those tactics. Top intelligence agencies are believed to study defender activities to find ways around them.

This real myriad of challenges and differences should not be overlooked (and may inspire either or both technical and socio-technical research). At the same time, every adversary is not a ninja; every attack cannot be sophisticated if that term has any meaning.⁷⁸ Many attackers continue to exploit published vulnerabilities for which patches are available,⁷⁹ and/or exploit⁸⁰ either human foibles or places where unrealistic demands are made on those people.⁸¹

Cybersecurity is not unique in having adaptive adversaries. There are other sciences where adversaries adapt, such as medicine, and even those, like finance, where they may read your papers as part of an effort to outthink you.⁸² Additionally, there are important questions about the rate of adaptation by particular adversaries, and the distribution of those rates. For example, do a few highly professional attackers change regularly, while most use the same attacks for months (or years?) What is the lifetime of an “indicator” or a “tactic”? What measures of the effectiveness or usefulness of information sharing measures can we derive, noting that there may be no observation perch outside the system?

78 Ben Buchanan, The Legend of Sophistication in Cyber Operation, January 2017, <https://www.belfercenter.org/sites/default/files/files/publication/Legend%20Sophistication%20-%20web.pdf>

79 Microsoft, Microsoft Security Intelligence Report, Vol. 11, 2011, <https://go.microsoft.com/fwlink/p/?LinkId=2036161&clid=0x409&culture=en-us&country=US>

80 Kenna Security and Cyentia Institute, Prioritization to Prediction, Vol. 7: Establishing Defender Advantage, <https://www.kennasecurity.com/resources/prioritization-to-prediction-report-volume-seven/>

81 See for example, Cormac Herley, “So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users,” in NSPW ‘09: Proceedings of the 2009 Workshop on New Security Paradigms, comp. Anil Somayaji and Richard Ford (Association for Computing Machinery, 2009), <https://dl.acm.org/doi/10.1145/1719030.1719050>

82 Stephanie Yang, “The Epic Story of How a ‘Genius’ Hedge Fund Almost Caused a Global Financial Meltdown,” Insider, last modified July 10, 2014, <https://www.businessinsider.com/the-fall-of-long-term-capital-management-2014-7>

Some of these issues will be effectively tackled by scientific research, others may make certain problems the purview of a statistical or near-miss focused agency, and yet others may simply influence the operations of a board such as the CSRB.

Regulatory Context

Aviation is a highly regulated industry. Participants from manufacturers through pilots are licensed, the facilities they use are usually purpose-built airports, and the industry's regulator, the FAA, coordinates with other national regulators to create a system where aviation is safe and cost-effective. This is in stark contrast to the “thicket” of laws concerning computerized and technological systems. These laws exist at the city,⁸³ state,^{84,85} and national level, applying different and possibly contradictory rules to different industries, as well as voluntary reporting formats and frequency differences. Additionally, the NTSB was created during an earlier period where tight regulations were more common and competition within aviation was limited. Historically, aviation looked even more different than the current IT landscape. More research is needed on how to conduct lessons learned investigations against or in the absence of a regulatory backstop.

Framing and Orientation

Workshop participants came from a wide variety of industry, academic, and government backgrounds. There was vigorous discussion of the importance of framing, including risk, systems thinking, safety thinking, and cybersecurity analysis. Many participants advocated strongly for one

⁸³ Libor Jany, “Minneapolis Passes Restrictive Ban on Facial Recognition Use by Police and Others,” Star Tribune (Minneapolis, MN), February 12, 2021, <https://www.startribune.com/minneapolis-passes-restrictive-ban-on-facial-recognition-use-by-police-others/600022551/>

⁸⁴ See for example Dmitry Shifrin and Mary Buckley Tobin, “Past, Present and Future: What’s Happening with Illinois’ and Other Biometric Privacy Laws,” JD Supra, <https://www.jdsupra.com/legalnews/past-present-and-future-what-s-5319231/>

⁸⁵ See also California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199.100 (June 28, 2018). <https://oag.ca.gov/privacy/ccpa>

of these or another.⁸⁶ There are opportunities to investigate the impact of framing on the results, and each frame has much to recommend it. We did not attempt in this workshop to resolve the differences.⁸⁷

The framing we use also impacts the language we choose. In this report, we aimed to be nuanced around a collection of closely related ideas which enable learning from problems. Each of these topics deserves further study:

- The nature of the problem: is it an accident, an incident, an attack, or a near miss?
- The nature of the analysis: are we focused on learning from many problems, perhaps statistically, or fewer, in more depth? This is a spectrum with many useful points, not a one-or-the-other choice.
- The degree of independence: Who is performing the steps of data gathering and analysis?
- The utility of the effort: How transparent, accountable, and scalable are the systems we develop?
- The cost of the inquiry: At some fundamental level all data collection, analysis, and publication impose costs. Are the costs incurred outweighed by the benefits of the effort?

Product Security vs Security Products

Products must be secure. An operating system must authenticate its users, and resist attacks. Businesses construct systems from many products. For example, one might use Salesforce to manage leads, Google Apps for documents, and Slack for conversation. Someone wanting to operate all three might need a way to aggregate and analyze logs, and so security products must augment the security of individual products, and their

⁸⁶ For a flavor of how heartfelt these debates are, one participant has a book chapter titled “Safety is Not a System Property.” Erik Hollnagel and David D. Woods, “Safety Is Not a System Property,” in *Resilience Engineering: Concepts and Precepts*, ed. Erik Hollnagel, David D. Woods, and Nancy Leveson (Boca Raton, FL: CRC Press, 2006).

⁸⁷ Algirdas Avizienis et al., “Basic Concepts and Taxonomy of Dependable and Secure Computing,” *IEEE Transactions* 1.1 (2004): 11-33 https://www.nasa.gov/pdf/636745main_day_3-algirdas_avizienis.pdf

security must be at least as secure as the products they are meant to secure. Security incidents often have contributing factors at each level of this. Incidents can result from product security flaws, human factors flaws including products that a person can't use securely, where the security impact of a choice is unclear, or where a person makes a slip or mistake in using a product. There are also flaws in the configuration of those products, their integration, or the application of supplemental controls. This complicates our understanding of "how incidents occur."

The lack of a shared set of technical facts impacts many groups beyond the cybersecurity community. The broader systems engineering community, including in particular creators and operators, needs to understand what attacks must be addressed and the effectiveness of tools to address those issues. This includes the creators of both popular systems like Microsoft Windows or Linux or iOS and the operators of popular cloud systems like AWS or Google Cloud. It also includes the creators of less popular systems such as SolarWinds, XiongMai (creator of many of the cameras exploited by the Mirai botnet), specialized markets such as operational technology providers, or medical device makers, and multiple other examples.⁸⁸ Beyond the systems engineering community, every business assembles and combines systems to deliver value. These integrations can be the source of security weaknesses, and the quality of the integration tooling, the security advice available, or the discoverability of flaws may all be usefully illuminated by a board. More research is needed that focuses on product security on the one hand and failures and successes of security tools on the other.

Other Organizational Structures

There are many lesson-learning systems in aviation, and most have inspired analogies that were brought up in the workshop. We focused our efforts on an independent investigations board modeled on the NTSB. The Executive Order's Cyber Safety Review Board (CSRB) may be an instance

⁸⁸ Karl Bode, "Chinese Company Recalls Cameras, DVRs Used in Last Week's Massive DDoS Attack," Techdirt, October 24, 2016, <https://www.techdirt.com/articles/20161024/08552535872/chinese-company-recalls-cameras-dvrs-used-last-weeks-massive-ddos-attack.shtml>

of such a board but does not have all of the NTSB's legal, investigatory or organizational independence.

This workshop did not have time to deeply investigate other structures that were raised, such as a near-miss agency, modeled on NASA's Aviation Safety Reporting System (ASRS)⁸⁹ and a statistical agency, such as a proposed Bureau of Cyber Statistics (BCS), informed by the work of the Solarium Commission.⁹⁰ Additionally, participants made reference to the Commercial Aviation Safety Team (cast-safety.org) and the Chemical Safety Review Board. We did not investigate these further, but each concept deserves more research.

Costs and Benefits of Investigative Boards

The wide variety of possible investigative aims is not supported by very much theory. Investigative activity in today's cybersecurity industry is focused on protecting the victim and limited to ending the incident. If causes are probed, that investigation is generally limited to production of IOCs (Indicators of Compromise) and TTPs (Tactics, Techniques, and Procedures) — in other words, the technical explanations. The work to develop other, more comprehensive and human-readable findings is not well categorized, and there's no clear list or reference of what skillsets, time, tooling, or other input produce what sorts of outputs. There are research opportunities in creating new types of tools that reduce skill needs, or that changes the kinds of skill sets involved in investigations.

Much of cybersecurity analysis is focused on risks and risk mitigation. That framing is one of several we can use. Cost-benefit analysis is widely used for environmental or medical questions. The process of collection and analysis is not cost-free.

⁸⁹ Jonathan Bair et al., "That Was Close! Reward Reporting of Cybersecurity 'Near Misses,'" *Colorado Technology Law Journal* 16, no. 16.2 (January 2, 2017): [Page 327], http://ctlj.colorado.edu/wp-content/uploads/2021/02/16.2_4-Shostack-8.7.18-FINAL.pdf

⁹⁰ Cyberspace Solarium Commission, *Cyberspace Solarium Commission Official Report*, [Page 73], March 11, 2020, <https://www.solarium.gov>

Thus, while much of this report is moderately supportive of the idea of the concept of review boards, we must examine the implementation of a system of analysis that will necessarily come with administrative costs. We note particular ones below. But more generally, those costs will exist. To be sure, there is every reason to expect that the benefits of analysis will outweigh those costs, but open research questions exist regarding the quantification of that expectation.

Access to Data

The workshop identified many opportunities for the research community to help develop the learning process in the cybersecurity industry. For that to happen, the research community will need access to data. Given liability concerns with organizations sharing this data, the NSF could fund efforts at data extraction and anonymization.⁹¹ A focused effort to identify incidents in which concerns over liability can be addressed or minimized through anonymization could produce valuable data sets. For instance, incidents at Federal agencies could be good sources for testing investigative techniques and anonymization approaches and technologies as share price impact and lawsuits are not concerns. The authors acknowledge that we are not experts in the NSF's funding processes, and recognize that they have many priorities. Nevertheless, we believe this would be a powerful lever in improving both applied cybersecurity and the science of cybersecurity.

Research Questions

The workshop has resulted in the discovery of many questions as participants challenged one another's assumptions or experiences. Many of these questions are sparked by our findings, but so far unanswered by them, and which we suggest then could be carried forward profitably in

⁹¹ Tyler Moore et al., "Valuing Cybersecurity Research Datasets" (paper presented at Workshop on the Economics of Information Security, Cambridge, MA, June 3, 2019), [Page 13], https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_41.pdf. Moore et al. discuss the need for information sharing about cybersecurity incidents and evaluate the value created by the Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT).

future research. Given the overlap between science and policy, we include some questions which may be more suited for research by legal scholars and less suited for work by computer scientists.

Incident Discovery and Identification

Incident Reporting Requirements

RQ: Could the various reporting regimes (such as data breach reporting to state AGs, CMMC reporting to DoD, Critical infrastructure, reports to the PCI Council, complaints to insurers or the Internet Crime Complaint Center) feed into a board? Is the data submitted sufficient to make determinations or initiate investigations? Are there legal inhibitors to such data flows?

RQ: Many requirements to report to regulators have timelines on the order of hours or days. What can be done to determine if an anomaly is an incident in those timeframes? How reliable are those methods? What are the normal ranges of time to make such a determination reliably, and what can be done to drive down the timeframes? Are there important “transfer to practice” issues where useful inventions are stuck?

RQ: What would be required to increase assurance that security incidents, breaches or near misses are being reported in accordance with the law? What incentives or penalties have been applied for reporting/concealing incidents, and what has the impact of those been? Is the regulatory toolkit being used in a coherent manner to support public policy goals?

RQ: How should reporting systems be designed? What are the effects of choice on definitions, timelines, and other factors? How can the space of incentives and penalties be defined? Is there an optimal mix of incentive, protection, and penalties on individuals or what are the effects or consequences of sectoral regulation? What lessons can be learned from aviation incident and near miss reporting and from incident reporting in other fields such as telecommunications outages?

RQ: How could the ASRS anonymization system be replicated for cybersecurity? What tradeoffs does this entail? How do the differences between computer system operations and aviation result in differences in the way near miss investigations might take place, especially the duration of an investigation, and what impact does that have on anonymization? Should a threshold be set about what can be reported?

Whistleblower and Professional Obligations

RQ: Assuming that many incidents are known to staff and concealed from the public, could either whistleblowing protections or professional obligations to report crimes be leveraged to assess the scale of the problem or to learn about specific incidents? For example, lawyers may be required to report threats to harm someone; doctors are often required to report gunshot wounds. These requirements span from professional obligations to legal ones.

RQ: What are the rights or obligations of a person who becomes aware of a crime against their employer, or who believes their employer is unreasonably concealing a breach? What other industries use whistleblower hotlines, and where do they fail or succeed? When are incentives important versus other values, such as saving a life? Can contracts ensure that whistleblowing is viable, or is legal protection required? What can cybersecurity learn from the professional obligations imposed in other fields? How do such obligations interact with duties and obligations?

RQ: Individuals have an ethical responsibility to “Design and implement systems that are robustly and useably secure.”⁹² But what should they do when either their organization is not providing that appropriate support, or when they believe that to be the case is harder to address? Several participants suggested the extension of whistleblower protection to product design or implementation. This raises complex questions including what responsibilities an organization has to incorporate security (or privacy) into product design or how those responsibilities change as they

⁹² ACM Code of Ethics, *supra*.

go from making installable software to operating it in a software-as-a-service business; who should respond to the blown-whistle; how to address the intricacy of legitimate business tradeoffs between security and other properties; how to address the natural tendency of staff to believe their area is important⁹³, and more.

Reporting Forms and Taxonomies

RQ: What exists today in terms of reporting forms and standards? What are the commonalities and differences? What research questions are enabled or blocked by the forms? What engineering questions are enabled or not by the forms? (For example, a form that asks about ‘phishing’ vs ‘credential phishing’ and ‘attachment phishing’ enable different product engineering.) Who is responsible for filling and checking forms? Is it technical staff, lawyers, or someone else?

RQ: Do forms ask open-ended questions? How frequently? What fraction of information is “listening” vs “box checking?” Would a collection of stories about having to “pick the box” be a helpful tool for those designing future forms? What strengths and limitations apply to AI (such as natural language processing) analysis of unstructured contributions? How does that relate to qualitative coding as practiced in social science. How does all of this relate to the questions that researchers can ask?

RQ: Much of our attention today is focused on enterprise incidents. Individuals may find reporting difficult: do they report a problem to local police? The FTC? The ICC? What could we learn if we improved police or insurance practice for individuals reporting local incidents of harassment or hacking? Could we discover, for example, that victims of certain breaches are reporting identity theft at greater rates? What threats to validity would impede such a system, and how could they be overcome?

⁹³ Adam Shostack, “Employees Say Company Left Data Vulnerable”, October 7, 2014 <https://adam.shostack.org/blog/2014/10/employees-say-company-left-data-vulnerable/>

Criteria for Investigating Incidents

RQ: How can a board rapidly select issues whose investigation will bear fruit? Are there indicators that can be inexpensively detected?

RQ: What tradeoffs between investigation depth and number of investigations yield what benefits? For example, if a board is budgeted in a way that allows a person-year of investigation, how can it judge if it should perform four investigations lasting 3 months each, or 1 lasting a year?

RQ: What data exists that could be used to develop thresholds for investigation? What characteristics of that data might influence its use? What should be included in the calculation of a loss? Direct thefts? Costs of technical response? Total costs of response including legal fees and penalties? (The answer clearly isn't some average cost multiplied by a number of records)⁹⁴. How predictable are losses? How long does it take to determine the factors that lead to accurate prediction of losses?

RQ: An investigation clearly uses resources not only of the board and parties, but potentially also other parties. What are the costs and benefits of board discretion to investigate incidents which do not clearly meet thresholds (either because aspects are unclear, or because the incident doesn't meet the established thresholds, but it does have interesting facets to it)?

Performing Investigations

Investigator Skills and Methodologies

RQ: What NICE categories and skill sets should an investigative team include? How important is the initial set of skills and experience brought to bear? Is there a strong path dependency on those initial skills, and

⁹⁴ Jay Jacobs, "Analyzing Ponemon Cost of Data Breach," Data Driven Security (blog), entry posted December 11, 2014, <https://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/>

what exercises, techniques, or facilitation can help a nascent organization understand, assess, and correct if needed? Does the balance of human skills needed from investigators change as the investigation progresses from identifying technical issues to creating a systemic picture of what went wrong?

RQ: What is the relationship between a cyber incident investigation and other investigations? What is the relationship between tools designed for legal discovery or other high volume data analysis and the needs of an investigative board? Are tools such as emotion detection useful at discovering debates between staff, and if so are such debates informative in a way that informs contributing factors?

RQ: To what extent can skills be augmented by playbooks? What is the interplay between playbooks (or other tools) and adaptive engagement with the details of the incident? How can we characterize the tradeoff between creativity, speed and deep learning?

RQ: How do the skillsets of NTSB investigators differ from the skillsets of operators? How would those differences manifest for the CSRB? What are the investigative skills that are required in terms of building and testing ideas? How do those relate to law enforcement investigators, investigations by Inspectors General, and other related investigations?

RQ: To what extent are counterfactuals, hypotheticals, or similar techniques used in investigations in other fields, what pros and cons have been identified, and what is the operational outcome in those fields?

Investigations by Interested Parties

RQ: What incident information does the legal system expose at the stages of indictments, pleadings, trials and decisions? What can scientists extract from these for use in producing timelines, and how to think about the work involved? How should we characterize the completeness of such analysis, or the impact of the adversarial system on the scientific or engineering uses of the information? Are the exposures in civil and

criminal trials meaningfully different for these purposes? For criminal cases, are there case summaries or other analyses that could be released after a trial? Prosecutors are, nominally, required to release such information to defendants under “Brady” and other rules.⁹⁵

RQ: What are the benefits and tradeoffs involved in insurance investigation of cyber incidents?

There are likely important scientific questions into what an insurer should measure, how to measure those things in a cost-effective way, what the costs or benefits would be to a shared insurance model, and what its limitations would be.

RQ: Internal investigations & retrospectives were brought up. Can we measure the frequency or impact of practitioner driven investigations in cybersecurity? (Obviously, a large amount of work has been done by safety professionals.) There is a policy question: should such documents be protected in some way to encourage more candor, or required by regulators because of the social benefit? What would be the pros and cons of mandating them and mandating their release?

Products and Controls

RQ: There is a relationship between security as a property of products and add-on security products. To what extent do attacks take advantage of insecurity of products in the form of technical vulnerabilities?

RQ: What is the variation in control sets? There are many control sets, such as NIST CSF, 800-53, CMMC, FedRAMP, COBIT and CIS. How much do they vary, and what is the impact of the differences? How do these line up against self-regulation guidance? Do the additional rules make organizations more secure, or distract from key advice that’s common?

⁹⁵ Marc Allen, Non-Brady Legal and Ethical Obligations on Prosecutors to Disclose Exculpatory Evidence. National Registry of Exonerations, University of Michigan, July 2018, <https://www.law.umich.edu/special/exoneration/Pages/Official-Misconduct.aspx>

Can a statistical agency make use of the variation as a form of natural experiment where outcome variation might trace to control variances?

RQ: What cybersecurity advice is commonly given but not followed? What are the reasons for that? Can we use techniques such as Emotion Detection to discover what leads to expressions of exasperation? Is exasperation a useful predictor of control failure?

RQ: How quickly do attacks change? How can we quantify attacker's skills or resources, and what's the relationship between those and the rate of change in attacks, the indicators they leave behind, and the tactics, techniques and procedures they use?

Reporting and Dissemination

Statistical Data

RQ: What decisions could be enabled by faster, more frequent statistics? What can the history of statistical tools like the CDC's weekly morbidity reports⁹⁶ teach those making tradeoffs about cybersecurity reporting?

RQ: What is the connection between taxonomies and use of statistics for decision making? Are there decisions where business, technology, or product leaders express a desire for data to inform their decisions? Which data would inform the most decisions, or the most impactful decisions? Do some taxonomies enable more decisions than others? What is the usability cost of such taxonomies?

RQ: What assumptions are being made about the causes of incidents? How do those beliefs contribute to defensive strategies, and would alternate beliefs result in different strategies?

⁹⁶ "Morbidity and Mortality Weekly Report," Centers for Disease Control and Prevention, <https://www.cdc.gov/mmwr/index.html>. We do not mean to ignore that the MMWR also includes case studies.

RQ: Are there non-incident sources of trend information that should inform a board?

RQ: What is the impact if investigators cannot both understand the technical issues involved and also generate human-readable explanations of systemic problems?

Transparency and Anonymization

RQ: How does published information inform attackers, which attackers does it inform, and what can they do with the information? Do we have evidence that specific types of attackers respond, or how quickly they respond? Is it “in campaign”, “next month” or next year?

RQ: What principles or guidance can be used to either assuage concerns about transparency, or to guide a board in making decisions?

RQ: Are there incidents that could be investigated with findings published anonymously to protect the victim? Such publication carries a host of complications. When does it get invoked/provided? Who can decide? If a board publishes anonymous findings, what happens if the incident becomes public? Does the report get re-identified? What if the vendor makes claims that are contradicted by the report?

RQ: Are there ways of reporting that help attackers and defenders differently? What can we learn from the full disclosure movement about the value of publishing vulns, which, over time, led to new forms of memory safety at a high temporary cost? Over what time scales, if any, was that a good tradeoff?

Near Misses

RQ: How could liability protection be used to incentivize near-miss reporting? What lessons can be drawn from ASRS in this regard? Would

model language, draft operating manuals, or other blueprints, prototypes, or exemplars aid in transition to practice?

RQ: How can companies clearly differentiate between a cybersecurity incident and a near-miss in the context of a report? Do current reporting forms account for the possibility that a reported incident is a near-miss, or that a near-miss that was reported (perhaps because it exposed interesting indicators or TTPs) was really an incident? Do current processes treat such as evidence of constructive engagement?

RQ: To what extent might near miss reporting be deterred by the risk that a near miss is actually an as yet unidentified incident? Would the goals of immediate reporting of incidents be well-served by some design for incremental reporting? Are there models for such, and how can they be adapted to cybersecurity?

RQ: What is the impact of fast reporting timelines on the ability to determine whether an incident has occurred versus a near miss?

RQ: What are normal incident timelines? What fraction of anomalies are fully tracked down? How do those differ across sectors or other communities? Are “not resolved” issues characterized in some way? What leads to those leads being “abandoned?”

RQ: What fraction of anomalies are determined to be real intrusions within one hour (or 36), and what skills and tools are involved in those determinations?

RQ: What is the impact of shrinking reporting timelines on the systems receiving these reports, the staff following up on the reports, etc?

RQ: To what extent does the reporting of a near miss assist attackers in further potential intrusions versus assist companies in defending against attacks?

RQ: How could contracts require counterparties to investigate or share near misses? Doing so would be easier if there were sample contractual language including definitions, a set of penalties or incentives. There is an opportunity here for applied, socio-technical, or legal research into meeting these needs.

Legal Issues

RQ: If a board has subpoena authority, and both legal and technical protection for its data, what impact, if any, would there be on how companies investigate and memorialize incident information? The range and nuances of protection granted to data given to the government is wide across not only cybersecurity, but medical data given to the FDA, tax data given to the IRS, and more. A review and analysis such as the one performed by Sedenberg for health data could be helpful.⁹⁷

RQ: What is the impact of conflict, crime, espionage and other elements of adversarial action on our ability to derive truth? Are there goals which would be usefully served by revising policies around information submitted to court under seal?

RQ: What is the interaction between legal privileges (attorney-client advice, attorney directed work product), to what they apply, and what a board can request? What is the impact of the basis under which material is provided to a board (eg, voluntary vs subpoena), and what legal protections are provided for material shared with other boards?

RQ: Beyond the focus of a board, the thicket of issues surrounding the risks and benefits of investigations may be worth investigation by legal or policy scholars. Thorough investigations have demonstrated benefits in a great many areas. If legal risks are preventing organizations or society from those benefits, are there tools which could reliably be brought to bear, or experiments that might be worth doing?

⁹⁷ Sedenberg, E., & Mulligan, D. (2016). Public Health as a Model for Cybersecurity Information Sharing. *Berkeley Technology Law Journal*, 30(3), 1687–1740. <https://doi.org/http://dx.doi.org/10.15779/Z38PZ61>

Other Research Questions

RQ: Current technical systems for forensics are limited by the limits on the reliability of tools. What would the impact of fully immutable logging, globally accurate timing, or other tools be on investigations?

RQ: How frequent are follow-up investigations, and at what depth? What system should we use to characterize that depth?

RQ: Inspired by the DIKW frame, what systems do we have for generating knowledge or wisdom? What basis can we use to judge sufficiency within the field? Should policy-makers use the same tests? If not, what is the relationship between the various frameworks or tests?

RQ: Do attackers adapt to defenses, or just move to another target? How frequent is each strategy? What are the scale or scope of those adaptations? At one end might be the authors of Stuxnet crafting an offensive delivery system and payload to jump the air gaps at the Natanz nuclear facility. At the other could be attackers running bulk malware campaigns who do no adaptation, or attackers who adapt their ransom demands to the victim against whom their attacks happen to succeed. How could these adaptations be characterized, measured, including for intensity or frequency?

Recommendations for the CSRB

We expect the newly formed CSRB will be grappling with many of the issues raised in this report, and in this section, we collect and present perspectives on how the board should operate. The CSRB has a rare opportunity to shape something new, and potentially to influence the course of cybersecurity for quite some time. If successful, the CSRB may be copied in other jurisdictions or sectors, and so this section includes both recommendations for the CSRB specifically, and where we have identified reasons that the CSRB cannot take such actions, additional suggestions for future lesson-learning entities on the Cyber NTSB model. We are not making recommendations targeted to either a near-miss entity or a statistical bureau only to allow us to focus; that lack should not be read as a lack of enthusiasm for either concept. We believe that this “startup phase” is crucially important and that lessons learned from the initial review can be used to shape the future of the CSRB or any other bodies created by Congress or executive action.

Focus the initial investigation on Federal agency actions and failures:

While the executive order that establishes the CSRB gives the board a large scope to investigate cyber incidents of national significance, it does not grant the board the authorities necessary to conduct what are likely to be adversarial reviews with private sector parties. Because cyber incidents can have significant impacts on customer and market confidence, companies in the United States have tended to tightly control what (if anything) they share with the public about such incidents.

While the CSRB was established in the spirit of voluntary cooperation, we hope but do not expect that most companies impacted by the SolarWinds incident will share more details with the Board than have been shared already. Yet, the President, through the National Security Advisor and Deputy National Security Advisor for Cybersecurity and Emerging Technologies, the Secretary of Homeland Security, and the Director of the Office of Management and Budget, the Director of National Intelligence,

and the Attorney General, can cajole or compel Federal agencies into cooperating with the CSRB. A transparent and thoughtfully critical review of Federal government failings would go a long way toward establishing the credibility of the Board. In addition, recommendations from that review are likely to be more actionable than recommendations made to the private sector.

Thus, while attempting to engage private parties impacted by the campaign, a successful report would be one that is mostly focused on gaps in the Federal government's ability to detect the campaign within its own networks, the failure by the intelligence community to detect the campaign or recognize the importance of it, any failures to adequately fuse intelligence and network defense data, and weaknesses in the Federal response. From this vantage, the review should seek to answer the following questions:

1. Did the intelligence community detect the campaign? If not, why? If so, why was this information not provided in a timely manner to network defenders, or why did those defenders not act?
2. What Federal agencies were targeted by the campaign? Which of these agencies detected the activity prior to the announcement by FireEye? Which of these agencies had information exfiltrated from their networks? What tools were in place that were meant to detect this type of activity but failed? Why did those failures occur?
3. What processes did Federal agencies have in place for evaluating the security of critical software installed on agency systems? Why did these processes fail?
4. Did the government have in place appropriate channels to receive early warning from private companies that detected aspects of the campaign? If not, have policies and processes been put in place to create these channels?
5. If implemented, would required security controls have prevented or detected the campaign at Federal agencies? If these controls were not implemented, why not?

Work with Federal regulators to establish processes for CSRB to investigate private sector incidents:

While clear authorities for the CSRB or any other cyber investigation board are highly desirable and likely necessary to fully investigate many incidents, existing authorities can be used in creative ways to empower CSRB investigations. Recent actions by the Transportation Security Administration (TSA) to regulate the pipeline industry and to do so in partnership with CISA may provide a good example of how such a partnership could work. The Department of Homeland Security should review TSA's authority for pipelines and other sectors under its remit and determine if it has the authority to mandate cooperation with investigations. A similar authorities review should be undertaken by other regulators.

Staff and resource the CSRB adequately:

Given the notional membership of the CSRB, board members should not be expected to carry out the review process. The board will need members with deep and broad experience and credibility in technology. A useful outcome requires that the board contain at least several members with the technical competence to credibly question the opinions of both board staff and the staff of technology companies whose work is being reviewed. There is a small set of people who have given consideration to how a board could operate and the pros and cons of choices it could make. The board will need an investigation team that is both expert and dedicated. The composition of the investigation team will depend on the scope of the investigation. For instance, the sector the incident occurred in, whether the incident impacts OT or IT, and whether the review will engage in its own technical analysis will impact the necessary skill set of the team. Operational knowledge as well as analytical, critical thinking skills are both necessary for the review to succeed. The skills necessary to carry out an investigation may be different than those necessary for real time incident response. One of the easiest requirements, and easily overlooked or undervalued, staffing

should include excellent writers. The impact of the CSRB will depend in part on its ability to deliver compelling and accessible reports.

The review team could be composed of Federal employees, contractors, Special Government Employees (SGEs), Intergovernmental Personnel Act (IPA) transfers, Federally Funded Research and Development Corporations (FFRDCs) and other individuals with requisite technical expertise and operational experience. CSRB members should provide scope and direction, provide advice and support, serve as liaisons to the private sector, review, revise, and approve the final report, and take into consideration any viewpoints provided directly to them by parties to the incident under review. Such a model will allow the CSRB to manage multiple reviews at any given time.

An initial team to review the SolarWinds incident might require expertise in:

- Investigatory skills
 - Experienced investigators from organizations like the GAO or IGs
 - Incident Response
 - Digital Forensics

- Technical skills
 - Hardware
 - Software
 - Data Security
 - Networks (Local and Wide-Area)
 - Cryptographic Systems
 - Cloud
 - Governance, Risk, and Compliance
 - Malware analysis and reverse engineering

- Legal

- Organizational Dynamics

- Information sharing mechanisms
- Intelligence liaison functions
- Systems thinking

If the review board takes on deeper investigations similar to what the NTSB engages in for an airline crash, it would need to have the capacity to conduct its own in depth investigations that could involve both network and system forensics activity. For a major incident confined to a single enterprise-level network, the team might require as many as a dozen forensics experts that might need to carry out the investigation over several months.

Develop a Manual for Conducting Cyber Incident Investigations:

The investigations into aviation incidents by the NTSB is guided by the Aviation Investigation Manual — Major Team Investigations.⁹⁸ This publicly available manual outlines how investigations are conducted and can be referenced by all parties to an investigation. The CSRB should develop, use and evolve a similar manual. The manual could draw on existing guidance from NIST, CIS and other standards bodies that provide guidance on incident response and incident review. The manual should specifically address what facts should be published, and which may need to be in a classified or controlled appendix. Consideration should also be given to asking NIST to develop the guide and to make it a special publication on conducting post incident reviews with an appendix for aspects of the CSRB's work that are particular to that body.

⁹⁸ <https://www.nts.gov/investigations/process/Documents/MajorInvestigationsManual.pdf>

Recommendations for Congress

Multiple committees are considering legislation to authorize investigations of cyber incidents. This legislation is often being developed in conjunction with legislation to require the reporting of cyber incidents. In developing this legislation, Congress should consider the following:

Grant authorities on a sector-by-sector basis:

As with the actual NTSB, Congress should grant specific authorities for each sector to whatever investigation board is being created or empowered. Investigations in different sectors, on different platforms, and with different consequences may require different capabilities on the investigation team and take place in different regulatory contexts.

Avoid making regulators responsible for conducting investigations:

A critical component of cyber incident investigations is to evaluate the failings of both regulations and regulators; thus, Congress should not make regulators responsible for conducting these reviews. Regulators should be treated as parties to the investigation and the investigating body should make recommendations for both how regulations can be strengthened and the work of regulators improved.

Stand up a diverse set of organizations charged with learning and improvement:

These efforts should include near miss analysis, a Bureau of Cyber Statistics, and other dedicated efforts. We are not at risk of having too much knowledge or wisdom brought into the area.

Look for opportunities to strengthen disclosure and encourage cooperation with investigators:

As discussed in Section 9, there may be opportunities to provide incentives including liability protection in exchange for candor on cyber incidents and near misses. The near miss systems active within the aviation industry provide limited forms of liability protection to encourage individuals to come forward. Incentives for both individuals and organizations in these systems should be considered. Individual incentives could include whistleblower protection, incentives, or rewards. The board must be able to protect information provided to it. The board may need to be able to compel disclosure or testimony. The board should have discretion in when to reveal information for the public good.

Provide legal and technical protection for investigators:

The board and its investigators may be the target of technical attacks designed to break into their systems and extract information of value to attackers. Investigators may be targeted on their personal systems, and their friends and families may be targeted as stepping stones. Investigators may also be subjected to online abuse, libel, misinformation, or conspiracy theories to either distract them or discredit their work via *ad hominem* attacks.

Conclusion: Failure Is Common, But Not Constant

In 2021, there has been a drumbeat of significant incidents including Accellion, SolarWinds, and Colonial Pipeline. Despite these, the internet and society at large mostly continue to function. Yet, there are also many organizations that seemingly are targeted by adversaries but manage to keep these adversaries from fulfilling their objections. We must create systems that can learn both from mistakes that are being made and the successes that are happening. Yet, at present, neither successes nor failures are shared with cyber defenders in any systematic way.

Secret knowledge is mysticism, not science or engineering. We heard a great deal in our workshop about how various groups have access to useful data which drives decisions that they believe are good. Yet the decisions they come to are different, which has a cost both to those trying to comply with the advice and in the credibility of the advice. Subjecting one's reasoning to criticism is scary. Such criticism and review is also a constant in fields with high rates of engineering success, ranging from bridge building to medical device manufacture. The consequences for leaving the field of cybersecurity in a prolonged adolescence are now too great; it's time for us to grow up.

Appendix A: Workshop Program

| Date | Time | Session |
|----------------|---------|---|
| March 18, 2021 | 3:00 pm | Session 1: Opening Session |
| March 25, 2021 | 3:00 pm | Session 2: What Does the NTSB Actually Do? Chris Hart, Former Chair, NTSB |
| April 1, 2021 | 3:00 pm | Session 3: Plenary Discussion |
| April 8, 2021 | 3:00 pm | Session 4: Learning from Other Domains David Woods, Ohio State University |
| April 15, 2021 | 3:00 pm | Session 5: Plenary Discussion |
| April 22, 2021 | 3:00 pm | Session 6: ASRS and Near Misses Becky Hooey, ASRS |
| April 29, 2021 | 3:00 pm | Session 7: The Role of Insurance Tom Finan, Marsh Erin Kenneally, Guidewire Bryan Hurd, Aon |
| May 6, 2021 | 3:00 pm | Session 8: Legal Issues Evan Wolff, Crowell & Moring John Woods, Baker McKenzie |
| June 24, 2021 | 3:00 pm | Session 9: Report Review |

Appendix B: Participant Biographies

Jonathan Bair is a student at the University of Colorado Law School.

Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University and affiliate faculty at Columbia Law School.

Moira Bergin serves as Subcommittee Director for the Subcommittee Cybersecurity and Infrastructure Protection at the House Committee on Homeland Security. Moira advises Members on policies related to cybersecurity, critical infrastructure protection, cyber threat information-sharing, supply chain risk management, and election security.

Felipe Bueno is currently a Master in Public Policy Candidate at the Harvard Kennedy School, where he is a researcher for the Belfer Center's Cyber Project. Felipe will join the United States Foreign Service as a diplomat upon completing his graduate studies.

L. Jean Camp is a Professor at the School of Informatics and Computing at Indiana University. She is a Fellow of the Institute of Electrical and Electronic Engineers and a Fellow of the American Association for the Advancement of Science.

Jennifer Chermoshnyuk is a Senior Manager for Customer Security and Trust and GitHub.

Richard Clayton is a security researcher in the Computer Laboratory of the University of Cambridge and the Director of the Cambridge Cloud Cybercrime Center.

John Costello is an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security. His research focuses on information and communications technology

supply-chain security, cyber strategy, emerging technology, and Chinese military strategy.

Ed Covert brings over twenty-five years of intelligence, cyber security, and risk management experience. His personal mission is to improve security postures by translating “cyber speak” to mission need and working to ensure cyber security supports the objectives of the business. Currently, he is the Director of Security Assessments and Infrastructure Engineering for WarnerMedia. Previously, he was the Global Head of Security Architecture for Deutsche Bank. He holds numerous industry cybersecurity and project management certifications and has is an author of multiple articles on security.

Frank Domizio is the Deputy Chief Information Security Officer for the Centers for Medicare and Medicaid Services (CMS). CMS Information Security Team provides full-spectrum cybersecurity services to protect the second largest information system network in the federal government servicing Healthcare.gov as well as Medicare and Medicaid. Frank is a proud Drexel University alum, holding a Bachelor of Science in Computing and Security Technology. He also holds a Master of Science in Cyber and Information Security from Capitol College as well as many industry certifications such as CISSP, GCIH and GCFE. He is also an Adjunct Professor of Cybersecurity with University of Maryland.

Ryan Ellis is an Associate Professor of Communication Studies at Northeastern University. Ryan’s research and teaching focuses on topics related to communication law and policy, infrastructure politics, and cybersecurity. He is the author of *Letters, Power Lines, and Other Dangerous Things: The Politics of Infrastructure Security* (MIT Press: 2020) and the co-editor of *Rewired: Cybersecurity Governance* (Wiley: 2019).

Jeremy Epstein is a Lead Program Officer at the National Science Foundation.

Connor Fairman is an analytic systems engineer at the MITRE Corporation. He was previously a research associate in the Digital and

Cyberspace Policy program at the Council on Foreign Relations where he researched cyber policy, U.S.-China technology competition, and digital trade. Connor speaks Chinese and Spanish and studied at the University of Pennsylvania.

Alyssa Feola is a Cybersecurity Advisor for the Technology Portfolio in the Technology Transformation Services within the General Services Administration (GSA). Since 2020, she has supported the Director in the Technology Portfolio in rationalizing, modernizing, and hardening the infrastructure and software that the workforce needs to do their jobs. She is currently working on software assurance activities and frequently collaborates with GSA OCISO's office to manage security authorizations, running TTS' Bug Bounty program, or working through various supply chain management activities.

Tom Finan is a Cyber Growth Leader within Willis Towers Watson's FINEX Cyber/E&O Practice. His work includes regular engagement with clients to discover their cybersecurity needs and the development and placement of responsive consulting and insurance solutions. Tom spearheaded the development of the company's Cyber Risk Solutions in North America and has actively led teams delivering the company's enterprise risk management, cyber risk culture, and cyber workforce readiness solutions. He previously served as Senior Cybersecurity Strategist and Counsel with the Department of Homeland Security's National Protection and Programs Directorate (NPPD) where he initiated and led DHS' Cybersecurity Insurance Initiative and its offshoot, the Cyber Incident Data and Analysis Working Group (CIDAWG).

Chris Folk is director of the HS SEDI FFRDC's National Protection Division. In this role, Folk oversees work program development and delivery. Mr. Folk brings more than 18 years of experience supporting the national and homeland security communities, working in operations, intelligence, infrastructure protection, and cybersecurity programs for the DoD, IC, and DHS.

Trey Ford is a strategic advisor to enterprise leaders and corporate directors. Today Trey serves as Executive Director of Cyber Security in

Vista Equity Partners' Consulting Group. With twenty years focused on the offensive, defensive, and programmatic leadership aspects of security, he is well grounded in public cloud, abuse, application, network, and platform security. Previously Trey was CISO of the Heroku platform at Salesforce, General Manager of Black Hat, held strategic advisory and global consulting roles, and still apologizes for time served as an auditor.

Allan Friedman is the Director of Cybersecurity Initiatives at National Telecommunications and Information Administration in the US Department of Commerce.

Emily Frye is the director for cyber integration for homeland security and the civilian enterprise at MITRE.

Davis Hake is an adjunct fellow (non-resident), at the strategic technologies program at the Center for Strategic and International Studies. He is the Co-Founder of a new cybersecurity startup, Arceo, and was the Director for Cybersecurity Strategy at Palo Alto Networks. Previously, Davis served nearly a decade in the US government, coordinating Federal interagency cyber incident response and policy at the National Security Council, the Department of Homeland Security, and on Capitol Hill where he drafted the first comprehensive cybersecurity legislation, culminating in the passage of the Cybersecurity Act of 2015 into law.

Malcolm Harkins is Chief Security & Trust Officer at Cymatic Security Inc.

Christopher A. Hart is the founder of Hart Solutions LLP, which specializes in improving safety in a variety of contexts, including the safety of automation in motor vehicles, workplace safety, and process safety in potentially hazardous industries. Mr. Hart is also Chairman of the Washington Metrorail Safety Commission, a three-jurisdictional agency (MD, VA, DC) that was created to oversee the safety of the Washington area mass transit subway system. Until February 2018 he was a Member of the National Transportation Safety Board (NTSB). In March, 2015, he was nominated by President Obama and confirmed by the Senate to be Chairman, which he was until March, 2017. Prior to that he was Vice

Chairman of the NTSB, after being nominated by President Obama and confirmed by the Senate in 2009 and 2013.

Jason Healey is a Senior Research Scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict, competition and cooperation.

Becky Hooey is the Director of the NASA Aviation Safety Reporting System (ASRS) which is a voluntary, confidential, non-punitive reporting system managed and operated by NASA for the FAA. She is also the director of the Confidential Close Call Reporting System (C3RS), a similar reporting system for the rail industry. Becky is a member of the International Confidential Aviation Safety Systems (ICASS) Group that promotes confidential safety reporting systems as an effective method of enhancing flight safety in commercial air transport and general aviation operations.

Bryan Hurd is a senior leader in the Stroz Friedberg (now Aon Cyber Solutions) of the international insurance brokerage company Aon where he leads global teams advising companies on solutions to assess their programs, improve security, reduce risk, prepare for emergencies, and respond to breaches.

Yurie Ito is a Founder and Executive Director of The CyberGreen Institute, a global non-profit organization focused on improving the cyber ecosystem's health by providing reliable metrics, measurement, and mitigation best practices to national CERTs, network operators, and policy makers.

Erin Kenneally is Director of Cyber Risk Analytics for Guidewire Software. In this capacity Kenneally provides cyber risk strategic thought leadership and domain expertise and also leads data-driven research innovation for novel risk analytics and modeling technology solutions.

Sara Kiesler is the Hillman Professor Emerita of Computer Science and Human Computer Interaction in the Human-Computer Interaction Institute at Carnegie Mellon University. She is also a program director

in the Directorate for Social, Behavioral & Economic Sciences at the US National Science Foundation, where her responsibilities include programs on Future of Work at the Human-Technology Frontier, Training-based Workforce Development for Advanced Cyberinfrastructure, and Smart and Connected Communities.

Rob Knake is a non-resident fellow at the Belfer Center and a Senior Fellow at the Council on Foreign Relations.

Amélie E. Koran is currently the Senior Technology Advocate for Splunk and recently served as the Deputy Chief Information Officer and most recently as Chief Technology Officer for the U.S. Department of Health and Human Services, Office of the Inspector General.

Paul Kurtz is an internationally recognized expert on cybersecurity and the Co-Founder and Chairman of TruSTAR.

Carl Landwehr is a Visiting Professor at the University of Michigan, a Visiting Scholar at George Washington University, a Life Fellow of the IEEE and a member of the National Cybersecurity Hall of Fame.

Ben Lefkowitz graduated Wesleyan University's College of Social Studies in 2020, and the Harvard Kennedy School in 2022 with a Masters in Public Policy. He's worked with the ADL, Abraham Initiatives, Blue and White party, and Haredi Institute for Public Affairs. He is a board member of Kulanu.

Steven B. Lipner is the executive director of SAFECode, a non-profit organization dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. Lipner is a pioneer in cybersecurity with over forty years' experience as a general manager, engineering manager, and researcher. He retired in 2015 from Microsoft where he was the creator and long-time leader of Microsoft's Security Development Lifecycle (SDL) team.

Bob Lord most recently served as the first Chief Security Officer at the Democratic National Committee. In that role he worked to secure the Committee, as well as helping state parties and campaigns. Previous roles include CISO at Yahoo, CISO in Residence at Rapid 7, and before that he headed up Twitter's information security program as its first security hire.

Art Manion is a senior member of the Vulnerability Analysis team in the CERT Program at the Software Engineering Institute (SEI), Carnegie Mellon University. Since joining CERT in 2001, Manion has studied vulnerabilities, coordinated disclosure efforts, and published advisories, alerts, and vulnerability notes for CERT/CC and US-CERT.

Haroon Meer is the founder of Thinkst, an applied research company with a deep focus on information security. Haroon has contributed to several books on information security and has published a number of papers on various topics related to the field.

Tyler Moore is the Tandy Professor of Cyber Security and Information Assurance in the Tandy School of Computer Science at the University of Tulsa. His research focuses on the economics of information security, the study of electronic crime, and the development of policy for strengthening security.

Jonathan Murphy is the Director of Cyber Policy at the U.S. Department of Homeland Security.

Dr. David Mussington serves as the Executive Assistant Director for Infrastructure Security at the Cybersecurity and Infrastructure Security Agency (CISA) as of February 2021. As Executive Assistant Director, he helps lead CISA's efforts to secure the nation's critical infrastructure in coordination with government and the private sector. Key areas of focus include vulnerability and risk assessments; securing soft targets and crowded places; training and exercises; and securing high-risk chemical facilities. Prior to joining CISA, Dr. Mussington was Professor of the Practice and Director for the Center for Public Policy and Private Enterprise at the School of Public Policy for the University of Maryland. His research and teaching activities focused on cyber physical system risk

management, election cybersecurity, and critical infrastructure security risk management.

Peter G. Neumann has been a computer professional since 1953. He has doctorates from Harvard and Darmstadt. After 10 years at Bell Labs in Murray Hill, New Jersey, in the 1960s, during which he was heavily involved in the Multics development jointly with MIT and Honeywell, he has been in SRI's Computer Science Lab since September 1971 -- where he is now Senior Principal Scientist. He is concerned with computer systems and networks, trustworthiness/dependability, high assurance, security, reliability, survivability, safety, and many risks-related issues such as election-system integrity, cryptographic applications and policies, health care, social implications, and human needs -- especially those including privacy. He is the PI of an ongoing DARPA project for the CRASH program (Clean-slate trustworthy hosts), jointly with the University of Cambridge (UK). Initially a four-year project, it is now in its seventh of eight years, with various ongoing technology transfer of a hardware-software trustworthy total-system co-design.

Jake Olcott is Vice President at BitSight Technologies, where he helps organizations benchmark their cybersecurity programs using quantitative metrics.

Victoria Ontiveros is an MPP candidate at Harvard Kennedy School, concentrating in International and Global Affairs. Originally from Boston, she graduated in 2020 from Johns Hopkins University, where she majored in International Studies, East Asian Studies, and Economics. Victoria has studied Mandarin Chinese for eight years and spent a year studying abroad in Shanghai, China with support from the Boren Scholarship. She is a research assistant on the Cyber Project at the Belfer Center.

Emilian Papadopoulos is president of Good Harbor Security Risk Management, a premiere cyber security risk management advisory firm.

Philip Reitingger has served as the President and CEO of the Global Cyber Alliance since December 2015. GCA is a nonprofit organization focused on eradicating systemic cybersecurity risks. He also serves on the advisory

boards of companies, mentors startups, and is a Senior Associate (non-resident) at the CSIS.

Aaron Rinehart is CTO and Co-Founder of Verica, a chaos engineering startup, and is a frequent author, consultant, and speaker in the space.

Clifton Robinson is a Ph.D. student in Cybersecurity at the Institute for the Wireless Internet of Things at Northeastern University, under Professor Tommaso Melodia. He received his B.S. in Computer Science and Mathematics magna cum laude at Bridgewater State University in 2018. He then received his M.S. in Cybersecurity in 2020 while working on his Ph.D. at Northeastern University. His research interests focus on network security, the Internet of Things, and cyberlaw.

Chris Rohlf is a Research Fellow at Georgetown's Center for Security and Emerging Technology (CSET), where he works on the CyberAI Project. Chris has worked in cybersecurity since 2003 in technical roles that include vulnerability research, exploitation and software engineering.

Sasha Romanosky is a senior policy researcher at the RAND Corporation, and former cyber policy advisor at the Pentagon in the Office of the Secretary of Defense for Policy (OSDP).

Casey Rosenthal is CEO and cofounder of Verica; formerly the Engineering Manager of the Chaos Engineering Team at Netflix.

Paul Rosenzweig is a Principal at Red Branch Consulting and a Professorial Lecturer in Law at George Washington University.

Ben Rothke is a Senior Information Security Manager at Tapad. He frequently writes about security, privacy, risk management, and social media.

Tony Sager is a Senior Vice President and Chief Evangelist for CIS® (The Center for Internet Security, Inc.). He leads the development of the CIS Controls™, a worldwide consensus project to find and support technical best practices in cybersecurity. Sager champions of use of CIS Controls

and other solutions gleaned from previous cyber-attacks to improve global cyber defense. He also nurtures CIS' independent worldwide community of volunteers, encouraging them to make their enterprise, and the connected world, a safer place. Sager retired from the National Security Agency (NSA) after 34 years as an Information Assurance professional.

Stefan Savage is a professor at UC San Diego's Department of Computer Science and Engineering and an affiliated faculty member at the School. Savage's research interests lie at the intersection of distributed systems, networking, and computer security, with a current focus on embedded security and the economics of cybercrime.

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by *The Economist*. He is the author of 14 books — including the New York Times best-seller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* — as well as hundreds of articles, essays, and academic papers. His influential newsletter *Crypto-Gram* and blog *Schneier on Security* are read by over 250,000 people. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard University and a board member of the Electronic Frontier Foundation. He is also a special advisor to IBM Security and the Chief Technology Officer of Resilient.

Scott J. Shackelford serves on the faculty of Indiana University where he is Cybersecurity Program Chair along with being Director of the Ostrom Workshop Program on Cybersecurity and Internet Governance. He is also an Affiliated Scholar at both the Harvard Kennedy School's Belfer Center for Science and International Affairs and Stanford's Center for Internet and Society, as well as a Senior Fellow at the Center for Applied Cybersecurity Research, and a Term Member at the Council on Foreign Relations.

Adam Shostack is the founder of Shostack + Associates, an affiliate Professor at the Paul G. Allen School of Computer Science & Engineering at the University of Washington and a member of the BlackHat Review Board. He is the author of *Threat Modeling: Designing for Security*, and the co-author of *The New School of Information Security*.

Alicia Smith is a Counsel in the U.S. House of Representatives committee on Homeland Security.

Jonathan Spring is a senior member of the technical staff with the CERT division of the Software Engineering Institute at Carnegie Mellon University. He began working at CERT in 2009. Prior posts include adjunct professor at the University of Pittsburgh's School of Information Sciences and as research fellow for the ICANN SSAC. His work's unifying theme is how we produce reliable evidence for various levels of cybersecurity policies. His work is some combination of leading by example and reflecting on study design and other philosophical issues.

Alex Stamos is a cybersecurity expert, business leader and entrepreneur working to improve the security and safety of the Internet through his teaching and research at Stanford University. Stamos is an Adjunct Professor at Stanford's Freeman-Spogli Institute and a visiting scholar at the Hoover Institution.

Robert Stratton is a principal at Polymathics, where he advises large enterprises on cybersecurity strategy and enterprise architecture.

David Turetsky is a Professor of Practice at the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany.

Bridgette Walsh is the Chief of Partnerships and Engagement at the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

Tarah Wheeler is a Cyber Project Fellow at the Belfer Center for Science and International Affairs at Harvard University's Kennedy School of Government. She is an International Security Fellow at New America leading a new international cybersecurity capacity building project with the Hewlett Foundation's Cyber Initiative and a US/UK Fulbright Scholar in Cyber Security. She is an Electronic Frontier Foundation advisory board member, an inaugural contributing cybersecurity expert for the

Washington Post, the Brookings Institution's contributing cybersecurity editor, and a Foreign Policy contributor on cyber warfare.

Evan D. Wolff is a partner in Crowell & Moring's Washington, D.C. office, where he is co-chair of the firm's Chambers USA-ranked Privacy & Cybersecurity Group and a member of the Government Contracts Group.

Robert Wood is the Chief Information Security Officer (CISO) for the Centers for Medicare and Medicaid Services (CMS). He leads enterprise cyber security, compliance, privacy, and counter intelligence functions at CMS and ensures the Agency complies with secure IT requirements while encouraging innovation. Prior to CMS, Robert built several security programs in the technology sector for organizations like Simon Data, SourceClear, and Nuna Health. He was also formerly a Principal Consultant for Cigital where he advised enterprises about their software security initiatives.

John Woods serves as co-head of the Global Cybersecurity practice group and is a partner based in Washington, DC. Over the past decade he has received recognition or ranking in the Legal 500, Chambers Global and USA Guides, Washingtonian Magazine, Corporate Counsel Magazine and BTI Consulting Group.

David Woods (PhD, Purdue University) has worked to improve systems safety in high risk complex settings for 40 years. These include studies of human coordination with automated and intelligent systems and accident investigations in aviation, nuclear power, critical care medicine, crisis response, military operations, and space operations. Beginning in 2000-2003 he developed Resilience Engineering on the dangers of brittle systems and the need to invest in sustaining sources of resilience as part of the response to several NASA accidents. His results on proactive safety and resilience are in the book Resilience Engineering (2006). He developed the first comprehensive theory on how systems can build the potential for resilient performance despite complexity. Recently, he started the SNAFU Catchers Consortium an industry-university partnership to build resilience in critical digital services (see stella.report or <http://bit.ly/StellaReportVelocity2017>).

Chris Wysopal is Co-Founder and Chief Technology Officer at Veracode, which pioneered the concept of using automated static binary analysis to discover vulnerabilities in software. He is a member of the executive team. Prior to Veracode, Chris was vice president of research and development at security consultancy @stake, which was acquired by Symantec.

Sounil Yu is the creator of the Cyber Defense Matrix and the DIE Resiliency Framework, serves on the board of SCVX Corp and the FAIR Institute, teaches security as an Adjunct Professor, co-chairs Art into Science: A Conference on Defense, and advises many startups. He is currently the CISO at JupiterOne and previously served as the CISO-in-Residence at YL Ventures and Chief Security Scientist at Bank of America.

Lauren Zabierek is the Executive Director of the Cyber Project at Harvard Kennedy School's Belfer Center. She comes to this role as a 2019 graduate of the Kennedy School's mid-career MPA program. Lauren served as an intelligence officer in the United States Air Force at the beginning of her career. Later, as a civilian intelligence analyst with the National Geospatial Intelligence Agency (NGA) assigned to the Office of Counterterrorism, she completed three war zone deployments. Throughout her six years at NGA, she became a subject matter expert on Activity Based Intelligence (ABI) and served as an adjunct professor in ABI at the NGA college.



National Security Fellows Program

Belfer Center for Science and International Affairs

Harvard Kennedy School

79 JFK Street

Cambridge, MA 02138

www.belfercenter.org/NSF