2018

That Was Close! Reward Reporting of Cybersecurity "Near Misses"

Jonathan Bair
University of Colorado Law School

Steven M. Bellovin
Columbia University

Andrew Manley
University of Colorado Law School

Blake Reid
University of Colorado Law School

Adam Shostak

Citation Information

Jonathan Bair, Steven M. Bellovin, Andrew Manley, Blake Reid, and Adam Shostak, *That Was Close! Reward Reporting of Cybersecurity "Near Misses"*, 16 COLO. TECH. L.J. 327 (2018), *available at* https://scholar.law.colorado.edu/articles/1189.

THAT WAS CLOSE!
REWARD REPORTING OF CYBERSECURITY "NEAR MISSES"

JONATHAN BAIR, STEVEN M. BELLOVIN, ANDREW MANLEY, BLAKE REID, ADAM SHOSTACK*

Building, deploying, and maintaining systems with sufficient cybersecurity is challenging. Faster improvement would be valuable to society as a whole. Are we doing as much as we can to improve? We examine robust and long-standing systems for learning from near misses in aviation, and propose the creation of a Cyber Safety Reporting System (CSRS).

To support this argument, we examine the liability concerns which inhibit learning, including both civil and regulatory liability. We look to the way in which cybersecurity engineering and science is done today, and propose that a small amount of 'policy entrepreneurship' could have substantial positive impact. We close by considering how a CSRS should be organized and housed.

* Jonathan Bair and Andrew Manley are 2018 graduates of 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. Blake Reid is an Associate Clinical Professor at Colorado Law and supervised Mr. Bair's and Mr. Manley's work on this topic in the Samuelson-Glushko Technology Law & Policy Clinic. Adam Shostack is a consultant.
Author names are listed in alphabetical order.
The authors wish to thank J. Pierre De Vries and Matt Curtin for many helpful comments on drafts of this article.

INTRODUCTION 328
A. Need for Information 328
B. Mandatory Incident Reporting/Investigation has Challenges 329
C. The Aviation Sector Offers Robust Models 331
D. Our Proposal 333
I. LIABILITY CONCERNS INHIBIT LEARNING 334
A. Civil Liability 335
B. Regulatory Liability 337
C. Defining Incidents and Near Misses 341
II. IMPROVE SCIENCE TO IMPROVE OUTCOMES 343
A. What Security Practices and Outcomes are Important? 343
B. The Importance of Data 347
III. POLICY ENTREPRENEURSHIP CAN STIMULATE SCIENTIFIC EFFORTS 351
A. The First Pillar: Encouraging Experimentation and Providing Leniency 352
B. The Second Pillar: Confidentiality and Anonymity Must be Protected 356
C. Organizing a CSRS 357
D. Single Reporting Regime 359
E. Analytic Regimes 360
F. Light-Touch Cooperation 363
CONCLUSION 363
A. Industry Should Experiment With Near-Miss Reporting 364
B. Regulators Should Reward Reporting of Near Misses 364

INTRODUCTION

A. Need for Information

In aviation, medicine, nuclear power plant operation, and even mountaineering, near misses are treated as an important source of knowledge. Each field has a formalized and structured near-miss reporting and analysis system. These systems give practitioners, researchers, and regulators many of the benefits of accident investigations without the human or economic costs of those accidents. In cybersecurity, we do not have such a system, but we do have a lot of accidents. Could a near-miss program be helpful? What would it look like? What issues do we need to address to bring it about?

The proliferation of technology provides consumers immeasurable benefits, but also creates great vulnerability. In recent years, we have seen explosive growth in the number of damaging

cyber-attacks.[1] 2017 alone saw worms and malware such as WannaCry, Petya, NotPetya, Bad Rabbit, and the massive Equifax breach, among many others.[2] Uber was the target of several lawsuits within days after disclosing a breach and (apparent) ransom payment.[3] Currently, there is no mechanism in place to facilitate understanding of these threats, or their commonalities.

While information regarding the causes of major breaches may occasionally become public after the fact, what is lacking is an aggregated data set which could be analyzed for research purposes. Collecting data about such incidents is difficult because of liability concerns. Moreover, there is a linguistic quagmire in the definitions of breach, incident, and hack, all of which are intimately interconnected with reporting mandates and liability concerns. We propose here to stay outside that debate, and instead look to "near misses." We consider a near miss to be an event short of a full incident, because some controls function as intended and contain the damage.[4] For example, if a person clicks on a link in a phishing email, and the phishing site has been taken down, then that event would be a near miss.[5] Research into near misses could provide clues as to trends in attacks, the effectiveness of controls, and avoidable mistakes made on the part of operators, among other valuable data.

B. Mandatory Incident Reporting/Investigation has Challenges

There is an important distinction to be made between reporting on vulnerabilities and reporting on incidents, and we limit our

1. Tara Seals, *Cyber-Attack Volume Doubled in First Half of 2017*, INFOSECURITY (Aug. 11, 2017), https://www.infosecurity-magazine.com/news/cyberattack-volume-doubled-2017/ [https://perma.cc/3WBK-XYSF].

2. Bill Chappell, *WannaCry Ransomware: What We Know Monday*, NPR (May 15, 2017, 2:31 PM), http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-Monday [https://perma.cc/XSS4-X8BP]; Brian Krebs, *'Petya' Ransomware Outbreak Goes Global*, KREBS ON SECURITY (June 27, 2017), https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/ [https://perma.cc/AX5R-BPZX]; Josh Fruhlinger, *Petya Ransomware and NotPetya Malware: What You Need to Know Now*, CSO (Oct. 17, 2017, 2:59 AM), https://www.csoonline.com/article/3233210/ransomware/petya-and-notpetya-the-basics.html [https://perma.cc/3MWK-9FAF]; Taylor Hatmaker, *A New Ransomware Attack Called Bad Rabbit Looks Related to NotPetya*, TECHCRUNCH (Oct. 24, 2017), https://techcrunch.com/2017/10/24/badrabbit-notpetya-russia-ukraine-ransomware-malware/ [https://perma.cc/RNS8-HX2P]; Elizabeth Weise, *A Timeline of Events Surrounding the Equifax Data Breach*, USA TODAY (Sept. 26, 2017, 12:06 PM), https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/ [https://perma.cc/9YNF-TNF8]; Zack Whittaker, *These were 2017's Biggest Hacks, Leaks, and Data Breaches*, ZDNET (Dec. 18, 2017, 5:21 AM), http://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2017/ [https://perma.cc/374G-63MD].

3. *See* Cyrus Farivar, *Uber Hit With 2 Lawsuits Over Gigantic 2016 Data Breach*, ARS TECHNICA (Nov. 23, 2017, 3:02 AM), https://arstechnica.com/tech-policy/2017/11/uber-hit-with-2-lawsuits-over-gigantic-2016-data-breach/ [https://perma.cc/P4HL-357Y].

4. *See* discussion *infra* Section I.C.

5. *See* discussion *infra* Section I.C.

discussion to the latter.[6] One possible regime for gathering such information would be to require disclosure of incidents, and to create a public investigations board which would analyze incidents and issue public reports on them.[7] Mandatory reporting and investigations would result in better data collection.[8] The regime would also cause firms to internalize, to some extent, the externalities of security.[9]

However, there are challenges that have made a mandatory reporting regime difficult to implement[10], and there are claims that such a regime would be more costly than beneficial.[11] Microsoft points out that mandatory reporting may cause firms to divert resources from more effective security measures to complying with inefficient and unnecessary reporting requirements.[12] Additionally, the lack of clearly defined terms in this area makes determining what does and doesn't qualify as a reportable event challenging.[13] Mandatory reporting regimes are often one-way, with the government requiring private actors to disclose information, but failing to reciprocate.[14] Because private actors will err on the side of compliance, they are likely to over-report, causing high-value data to become buried and less easy to identify.[15] And to ensure compliance, private actors' legal counsel may discourage disclosure to anyone other than the government

6. Vulnerabilities is a term of art in computer security, and those policy questions have been extensively explored and debated at the highest levels of government. *See* Rob Joyce, *Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do*, THE WHITE HOUSE (Nov. 15, 2017), https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/ [https://perma.cc/ZTW6-NAB3].

7. *See* NAT'L RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 179–205 (1991).

8. *See, e.g.*, Steven M. Bellovin, *The Major Cyberincident Investigations Board*, 10 IEEE SECURITY & PRIVACY 96 (Nov.-Dec. 2012).

9. Stefan Laube & Rainer Böhme, *The Economics of Mandatory Security Breach Reporting to Authorities*, 2 J. CYBERSECURITY 29, 29–31 (2016) (arguing that mandatory breach reporting "can incentivize firms to enhance their security levels, leading to a reduction of breach probabilities in the economy. Thus, less breaches propagate and negatively affect others.").

10. *See* Steven M. Bellovin & Adam Shostack, *Input to the Commission on Enhancing National Cybersecurity* (2016), https://www.cs.columbia.edu/~smb/papers/Current_and_Future_States_of_Cybersecurity-Bellovin-Shostack.pdf [https://perma.cc/FM4N-ZP4R].

11. *See, e.g.*, DEPARTMENT OF HOMELAND SECURITY, ENHANCING RESILIENCE THROUGH CYBER INCIDENT DATA SHARING AND ANALYSIS: OVERCOMING PERCEIVED OBSTACLES TO SHARING INTO A CYBER INCIDENT DATA REPOSITORY (2015), https://www.dhs.gov/sites/default/files/publications/Overcoming%20Perceived%20Obstacles%20White%20Paper_1.pdf [https://perma.cc/3JZY-KHWE].

12. *Cybersecurity Policy Toolkit: Mandatory Incident Disclosure Models*, MICROSOFT, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Alw (last visited Mar. 24, 2018) [https://perma.cc/QC5F-HST3].

13. *Id*.

14. *Should Companies be Required to Share Information About Cyberattacks?*, WALL STREET J. (May 22, 2016, 10:00 PM), https://www.wsj.com/articles/should-companies-be-required-to-share-information-about-cyberattacks-1463968801 [https://perma.cc/G4KR-NH9E].

15. *Id*.

authority.[16] As such, if a mandatory reporting regime is crafted incorrectly, it may result in an increase in social cost.[17]

C. The Aviation Sector Offers Robust Models

An alternative is a voluntary reporting scheme, possibly combined with an incentive scheme, whereby organizations who experience a near miss would file a report encompassing important details of the event to some neutral party. That party would encode the data and place it in a database, perform analyses, and issue reports. This database could then be used both by researchers and by the industry as a whole. People could learn what works, what does not work, and where the weak spots in security are.

The adoption of such a voluntary confidential information sharing system has proved valuable to the aviation industry. The most notable, and one of the earliest, is the Aviation Safety Reporting System (ASRS) housed within the National Aeronautics and Space Administration (NASA).[18] The ASRS is a system which collects voluntary information regarding near misses in aviation.[19] This data is then analyzed to identify weaknesses in safety systems, and possibly to identify means to prevent similar incidents occurring in the future, thus improving the safety of air travel overall.[20] The ASRS is successful for multiple reasons: First, it recognizes that to understand "why people did what they did, the best approach is to just ask [them]."[21] Adequately anonymizing the data, and ensuring confidentiality and security of the data encourages reporters to be more open and honest in their responses.[22] Additionally, NASA is a well-respected scientific agency without any enforcement interests, which reduces concerns that a reporter risks drawing unwanted attention to themselves.[23] And the FAA, for its part, treats reporting to the ASRS as "indicative of a constructive attitude" and will include that in its determination of penalties if incidents are reported in a timely manner.[24] These penalties

16. MICROSOFT, *supra* note 12.

17. Laube & Böhme, *supra* note 9 ("Interdependence between information systems allows breaches to propagate and negatively affect others . . . [causing] negative externalities in an economy." In other words, creating a social cost.).

18. *Program Briefing*, AVIATION SAFETY REPORTING SYSTEM, https://asrs.arc.nasa.gov/overview/summary.html (last visited Mar. 24, 2018) [https://perma.cc/36BG-Y8ET].

19. *Id*.

20. *Id*.

21. ASRS: THE Case for CONFIDENTIAL INCIDENT REPORTING SYSTEMS, https://asrs.arc.nasa.gov/docs/rs/60_Case_for_Confidential_Incident_Reporting.pdf (last visited Mar. 24, 2018) [https://perma.cc/W3WD-3JCB].

22. *Id*.

23. *Id*.

24. FAA, ADVISORY CIRCULAR: AVIATION SAFETY REPORTING PROGRAM (2011), https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2000-46E.pdf [https://perma.cc/T9KR-6PDZ].

can be quite severe, including revoking a license and ending a career in aviation, and so mitigating those penalties becomes quite important.

A clear definition of what constitutes an accident allows the FAA to investigate accidents, while rewarding the reporting of near-miss events to NASA. Moreover, "Title 14 of the Code of Federal Regulations (14 C.F.R.) part 91, section 91.25 prohibits the use of any reports submitted to NASA under the ASRS (or information derived therefrom) in any disciplinary action, except information concerning criminal offenses or accidents that are covered under paragraphs 7a(1) and 7a(2)."[25]

These features have led to a successful program. ASRS' intake of reports, which averaged 400 reports per month in its inaugural year, has now grown to an average of over 7,600 reports per month.[26] These reports are also used to generate safety alerts, with the underlying problem being addressed in 56% of instances where an alert was issued, and action taken as a direct result of the alert in 22% of instances.[27] The database of de-identified reports is also searchable and open, handling over 1,500 queries per month.[28] And lastly, the ASRS publishes a monthly newsletter, *Callback*, aiming to provide educational safety information to the aviation community.[29] They are sufficiently valued that the U.S. ASRS program has been emulated in the aviation regulations of many other countries.[30]

In addition to ASRS, airlines tend to operate internal "aviation safety programs," some of which feed into other cross-organizational safety programs, such as the FAA's Aviation Safety Information Analysis and Sharing (ASIAS) System.[31]

Voluntary information sharing regimes are also frequently employed in other industries. The Federal Railroad Administration operates a Confidential Close Call Reporting System (C^3RS).[32] As with ASRS, the C^3RS allows for confidential reporting of unsafe conditions

25. *Id*.

26. AVIATION SAFETY REPORTING SYSTEM, ASRS 2016 PROGRAM BRIEFING (2016), https://asrs.arc.nasa.gov/docs/ASRS_ProgramBriefing2016.pdf [https://perma.cc/N6XT-2C5E].

27. *Id*. at 26.

28. *Id*. at 33.

29. *Id*. at 37.

30. *Id*. at 48.

31. ASIAS performs analysis between organizations, learning from telemetry data that one airline or another experiences meaningfully more issues flying into a given airfield. *About ASIAS*, FAA, https://www.asias.faa.gov/apex/f?p=100:1:::::: (last visited Mar. 24, 2018) [https://perma.cc/QQ9R-JTAB]; *Performance Success Stories How the FAA and Airlines Sleuth for Safety*, FAA (Aug. 2016), https://www.faa.gov/nextgen/snapshots/stories/?slide=36 [https://perma.cc/5K9H-JGT7]. We focus on ASRS in this article in part because the technology sector has more diverse equipment, operated in more diverse ways and with less rigor than the aviation sector. The obvious rejoinder of "standardize more" would likely have an impact on the amount of innovation in the sector.

32. *Confidential Close Call Reporting System – C^3RS*, FED. RAILROAD ADMIN., https://www.fra.dot.gov/c3rs (last visited Mar. 24, 2018) [https://perma.cc/Y68X-U7CN].

by stake holders, which in turn allows for changes in rail transportation which make the system safer.[33] A similar system can be found for medical devices with the Food and Drug Administration, and for nuclear power plants in the IAEA.[34] Some, but not all, of these schemes involve explicit incentive structures.[35] Similar programs for near-miss reporting exist in other fields, ranging from medicine[36] to mountaineering.[37]

D. Our Proposal

We propose the creation of a similar system for cybersecurity near misses. When there is a near miss, companies and their employees would be encouraged to file a report with some organization. As is done for aviation, this organization would review the report for completeness (and solicit additional data if necessary), anonymize it, publish it in a database, and analyze the reports and data for actionable results. We call this system a Cyber Security Reporting System, CSRS, in homage to the ASRS.

There are some obvious challenges. The first, of course, is the reluctance of corporate executives to disclose details of an event, be it incident or near miss. They may be afraid of liability,[38] of personal

33. *Id*.

34. *Adverse Event Reporting Data Files*, FDA, https://www.fda.gov/MedicalDevices/Safety/ReportaProblem/ucm124064.htm (last visited March 24, 2018) [https://perma.cc/EZA3-SAYQ]; INTERNATIONAL ATOMIC ENERGY AGENCY, GUIDE ON INCIDENT REPORTING SYSTEM FOR RESEARCH REACTORS (2000), https://www-ns.iaea.org/downloads/ni/irsrr/guidelines.pdf [https://perma.cc/7A88-W2MH].

35. Incentives matter because cybersecurity staff frequently have more work than time, and an incentive program will help ensure that data is gathered, written down, and sent to an analysis center.

36. *See Adverse Events, Near Misses, and Errors,* PATIENT SAFETY NETWORK, https://psnet.ahrq.gov/primers/primer/34/adverse-events-near-misses-and-errors (last updated June 2017) [https://perma.cc/9YM4-FDFX]; such programs are not only in the U.S. For example, in "Learning from Near Misses," The Canadian Medical Protective Association opens with a reference to aviation: "A near miss in aviation refers to 2 aircraft in flight narrowly missing a collision with each other. A near miss in medicine is an event that might have resulted in harm but the problem did not reach the patient because of timely intervention by healthcare providers or the patient or family, or due to good fortune. Near misses may also be referred to as 'close calls' calls or 'good catches.'" *Learning from Near Misses*, CANADIAN MED. PROTECTIVE ASS'N, https://www.cmpa-acpm.ca/serve/docs/ela/goodpracticesguide/pages/adverse_events/Quality_improvement/learning_from_near_misses-e.html (last visited Mar. 24, 2018) [https://perma.cc/VM2S-VK8N].

37. The American Alpine Club publishes an annual series of books, of "Accidents in North American Climbing." ACCIDENTS IN NORTH AMERICAN CLIMBING, AMERICAN ALPINE CLUB (2017); *See also* MAUD VANPOULLE ET AL., INCIDENTS AND NEAR-MISSES IN MOUNTAIN SPORTS, (2017).

38. *See infra* Section I.

jeopardy,[39] investor reaction,[40] or even disclosing details of their network and its weaknesses to other attackers.

A second challenge is actually setting up the reporting system. Apart from the issue of who would run it or pay for it, actually handling the reports is challenging. It's hard to preserve necessary details while still obscuring the identity of the reporting organization; it's also difficult to protect individual employees from fear of possible retaliation.

Still, this seems to us to be the best approach to gathering and analyzing this very important data. Right now, it is difficult for defenders to learn what has or hasn't worked; voluntary reporting seems more feasible for learning useful defensive lessons than other approaches.

This paper will first address both the civil and regulatory liability companies face under the current regime, and how our current lack of clear definitions make navigating such liabilities difficult. It will then turn to current practices and the rationales behind them, how better information can enable scientific work to improve those practices, and how regulators can encourage experimentation and learning. Lastly, this paper will address why action is necessary, what specifically needs to be done, and explains why the proposal presented in this paper is the best solution.

I. LIABILITY CONCERNS INHIBIT LEARNING

The continuing failure to adequately develop cybersecurity has prompted calls for a new regulatory framework and government intervention.[41] In the absence of such an overarching federal

39. The Equifax breach cost the chief executive officer, chief information officer, and chief security officer their jobs. *See* Cyrus Farivar, *After Huge Equifax Breach, CEO 'Retires,'* ARS TECHNICA (Sept. 26, 2017, 7:42 AM)), https://arstechnica.com/tech-policy/2017/09/after-huge-equifax-breach-ceo-retires [https://perma.cc/Z82S-2RAG]; Cyrus Farivar, *Equifax CIO, CSO 'Retire' in Wake of Huge Security Breach*, ARS TECHNICA (Sept. 15, 2017, 4:54 PM), https://arstechnica.com/tech-policy/2017/09/equifax-cio-cso-retire-in-wake-of-huge-security-breach/ [https://perma.cc/8MBD-2RQX].

40. *See* Michael E. Kanell, *Equifax Faces Bumpy Road, but Expected to Survive*, MYSANANTONIO.COM (Nov. 24, 2017, 2:12 PM), http://www.mysanantonio.com/business/national/article/Equifax-faces-bumpy-road-but-expected-to-survive-12381707.php (stating that Equifax lost about a third of its market value following the breach) [https://perma.cc/W3G6-LJB7].

41. *See* Bruce Schneier, *Don't Waste Your Breath Complaining to Equifax about Data Breach,* CNN (Sept. 11, 2017, 6:23 PM), http://cnn.it/2gYLiM4 [https://perma.cc/8E5L-W9HG]; Bruce Schneier, *On the Equifax Data Breach*, SCHNEIER ON SECURITY (Sept. 13, 2017, 12:49 PM), https://www.schneier.com/blog/archives/2017/09/on_the_equifax_.html ("Market failures like [cybersecurity] can only be solved through government intervention. By regulating the security practices of companies that store our data, and fining companies that fail to comply, governments can raise the cost of insecurity high enough that security becomes a cheaper alternative.") [https://perma.cc/9AUH-R486]; *See also* Jack Detsch, *Cyber Risk Wednesday: Software Liability—the Good, the Bad, and the Uncomfortable,* ATLANTIC COUNCIL (Nov. 30, 2016), http://www.atlanticcouncil.org/events/past-events/cyber-risk-wednesday-software-liability-the-good-the-bad-and-the-uncomfortable (quoting Bruce Schnier, "'The market

cybersecurity law, numerous private and government organizations are pursuing different approaches to hold companies responsible for data breaches.[42] As a result, companies may be subject to a wide range of both regulatory (statutory) and civil liability—unfair or deceptive practices, breach of contract, negligence, unjust enrichment, and negligent misrepresentation among others—for failure to adequately protect data.[43] Particularly, enforcement and civil actions may be brought in the U.S. by the individuals about whom data was lost, other businesses impacted by the breach, shareholders of the company, government agencies such as the U.S. Federal Trade Commission (FTC), the U.S. Securities and Exchange Commission (SEC), state Attorneys General, or the U.S. Department of Justice (DOJ). Congress may even initiate inquiries into the breach.[44] Given the potential for liability, companies try to say as little as possible about issues, incidents, or breaches which they experience. They also have a complex set of tradeoffs to make about how to defend themselves. They need to set a level of investment and then allocate those resources to both offer technical protection, and to do so in a way that can be justified in front of a jury. As we will explain in Section II, this is very difficult.

A. Civil Liability

Civil liability from a data breach will often come in the form of contract damages or tort damages.[45] In those cases, a plaintiff will attempt to show that an implied contract existed to safeguard the data, that the company was negligent, or negligently misrepresented the level of security it used to protect data.[46] While data-breach claims are

---

can't fix this because neither the buyer and the seller care,' he said. 'Until now, we've given programmers the right to code the world that they saw fit. We need to figure out the policy.'") [https://perma.cc/5TCY-6584].

42. Jenny A. Durkan & Alicia Cobb, *After a Cyber Breach, What Laws Are in Play and Who Is Enforcing Them?*, THE CYBERSECURITY LAW REPORT (May 20, 2015) https://www.quinnemanuel.com/media/1125067/cslr_after-a-cyber-breach-what-laws-are-in-play-and-who-is-enforcing-them.pdf (arguing that there is a single liability regime in place for data breaches and that a company which is breached may seek investigations by the FBI, Secret Service, SEC, FCC, State A.G.s and the FTC) [https://perma.cc/VS6K-XFDU].

43. *See* JUDITH H. GERMANO & ZACHARY K. GOLDMAN, AFTER THE BREACH: CYBERSECURITY LIABILITY RISK 1–2 (2014), http://www.lawandsecurity.org/wp-content/uploads/2014/06/CLS-After-the-Breach-Final.pdf [https://perma.cc/2SN6-BJ22]. *But see* DAVID A. ZETOONY ET AL., 2017 DATA BREACH LITIGATION REPORT 1 (Bryan Cave 2017), https://d11m3yrngt251b.cloudfront.net/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf [https://perma.cc/D7NQ-DVGG].

44. GERMANO & GOLDMAN, *supra* note 43, at 1.

45. Wayne M. Alder, *Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim*, Becker & Poliakoff, 5, https://beckerlawyers.com/wp-content/uploads/2018/02/20151001_alder_data_breaches.pdf (last visited Apr. 2, 2018) [https://perma.cc/lx6p-hlf3].

46. *See id*. (stating that savvy companies will often seek to protect themselves by wording contracts such that the standard for data protection is set at the minimum that applicable laws allow).

often difficult to prove due to the lack of evidence of an actual harm, some circuit courts have allowed standing in cases of future harm.[47] Other circuit courts reasoned that the 'threat of future harm' is too speculative to proceed however,[48] resulting in a circuit split with plaintiffs in at least one case petitioning the Supreme Court to resolve the issue of standing, albeit unsuccessfully.[49] Regardless, a general plaintiff friendly trend is increasing the number and cost of settlements from data breaches.[50]

Even with the improved chance of standing in some courts, private parties still face an uphill battle in proving injury after a breach,[51] and private actions remain relatively unsuccessful.[52] Indeed, an exceedingly low percentage of publicly reported breaches actually lead to a class action.[53] While typical consumers may still be unable to prove injury in data breach cases, the company's business partners who experience much more direct financial loss are more easily able to

47. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("[A]llegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury . . . ."); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing . . . ."); Attias v. Carefirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017); Kevin M. LaCroix, *Deepening Circuit Split on Data Breach Suit Standing*, THE D&O DIARY: CYBER LIABILITY (Aug. 6, 2017), https://www.dandodiary.com/2017/08/articles/cyber-liability/deepening-circuit-split-data-breach-suit-standing/ ("[T]he D.C. Circuit held that the claimants' risk of future harm is sufficient to meet Article III standing requirements [in consumer data breach lawsuits]. . . . join[ing] a growing number of federal appellate courts . . . .") [https://perma.cc/XL6J-JLQE]. However, a circuit split exists on the standing argument as the 2nd & 4th Circuits have held the opposite. *See* Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017), *cert. denied*, Beck v. Shulkin, 137 S. Ct. 2307 (2017); Whalen v. Michaels Stores, Inc. 689 Fed. Appx. 89 (2d Cir. 2017).

48. *Beck*, 848 F.3d at 274 (reasoning that the threat of future harm is too speculative and thus not clearly imminent to allow standing); *In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) ("[C]onclud[ing] that the complaint has not sufficiently alleged a substantial risk of identity theft . . . and future injury" to support standing).

49. Attias v. Carefirst Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 86 U.S.L.W. 3409 (U.S. Feb. 20, 2018) (No. 17-641).

50. Carlton Fields et al., *Class Action and Regulatory Settlements Reflect the Rising Cost of Data Breaches*, JD SUPRA (July 12, 2017), https://www.jdsupra.com/legalnews/class-action-and-regulatory-settlements-28008/ [https://perma.cc/R4Y2-UH59]; *See, e.g.*, Bowdeya Tweh, *Anthem Agrees to $115 Million Settlement of Data Breach Lawsuit* (June 23, 2017, 4:56 PM), https://www.wsj.com/articles/anthem-agrees-to-115-million-settlement-of-data-breach-lawsuit-1498251371 [https://perma.cc/J8KP-F6CL]; Robert Hackett, *Data Breaches Now Cost $4 Million on Average*, FORTUNE (June 15, 2016), http://fortune.com/2016/06/15/data-breach-cost-study-ibm/ ("On average, the cost of a breach has risen to $4 million per incident—up 29% since 2013—according to research sponsored by IBM's security division. . .") [https://perma.cc/ABX4-MLMX].

51. ZETOONY ET AL., *supra* note 43.

52. Alex Pearce, *Defending The Business-To-Business Data Breach Lawsuit*, JD SUPRA (Nov. 14, 2017), https://www.jdsupra.com/legalnews/defending-the-business-to-business-data-70251/ [https://perma.cc/W3SU-797M].

53. ZETOONY ET AL., *supra* note 43, at 3 ("806 breaches were publicly reported during [2016]. . . . only 76 federal class action complaints were filed during the same timeframe, and these filings related to only 27 unique defendants" meaning only about 3.3% of such breaches led to class action litigation).

prove standing.[54] Even so, if companies have contractually limited their liability from a cybersecurity incident, an injured party may only recover on certain contract claims and not negligence claims stemming from the breach.[55] These difficulties suggest that it is the regulatory liability for which companies should be most concerned.

There is also the chance that a mandatory liability regiment will be imposed through international agreement. A recent French government document makes exactly this suggestion:[56]

> Il semble donc pertinent de poser au niveau international un principe de responsabilité de sécurité des acteurs privés systémiques dans la conception, l'intégration, le déploiement et la maintenance de leurs produits et services numériques. Cette responsabilisation pourrait se traduire par une obligation pour les entreprises systémiques de garantir la sécurité à long terme de leurs produits numériques, notamment en fournissant des correctifs appropriés en cas de vulnérabilité. Le niveau de responsabilité doit être fixé en fonction du rôle et de la taille de l'acteur concerné et pourrait se présenter comme une obligation de moyens plus que de résultats.
>
> (It therefore seems appropriate to establish at the international level a principle of safety responsibility for systemic private actors in the design, integration, deployment and maintenance of their digital products and services. This accountability could be translated into an obligation for systemic enterprises to ensure the long-term security of their digital products, including by providing appropriate fixes in case of vulnerability. The level of responsibility should be set according to the role and size of the actor concerned and could be an obligation of means rather than results.)[57]

B. Regulatory Liability

Enforcement actions stemming from a breach can be extremely costly to companies. Since its 2013 data breach, Target has reportedly spent over $200 million on legal fees and expenses, with settlements from suits by state Attorneys General rising to $18.5 million.[58] The recent Equifax breach has also caused a flurry of lawsuits—upwards

54. Pearce, *supra* note 52.

55. *See id*. (citing the decision in SELCO Cmty. Credit Union v. Noodles & Company, 267 F.Supp.3d 1288 (D. Colo. 2017) where the court agreed that the economic-loss rule "prevents plaintiffs who suffer economic loss stemming from contract to recover those losses through non-contract claims.").

56. SECRETARIAT-GENERAL FOR NAT'L DEFENCE AND SECURITY, REVUE STRATÉGIQUE DE CYBERDÉFENSE 89 (2018), http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf [https://perma.cc/BW3X-UUV3].

57. Translation primarily by Google Translate.

58. Fields et al., *supra* note 50.

of 200 class action suits, and investigations or suits by every state Attorney General—as well as investigations by the FTC, Congress, and the DOJ.[59] Equifax stands as an exemplar of the potential minefield of enforcement actions that can be brought following a data breach. We briefly discuss some of the government organizations involved in such enforcement actions to demonstrate the liability concerns that companies face.

The FTC has asserted some authority under Section 5 of the FTC Act to prevent unfair or deceptive practices in cybersecurity.[60] In its enforcement action against Wyndham Worldwide Corp ("Wyndham"), the FTC asserted that Wyndham was breached on three occasions within two years, exposing customer information which led to over $10.6 million in fraudulent charges.[61] The FTC asserted that Wyndham's security practices were unfair and exposed customer's data to theft by, among other things, failing to employ reasonable measures to detect and prevent unauthorized access to its network or conduct proper incident response procedures, allowing the hackers to use similar methods in each attack.[62] In a final settlement, Wyndham agreed to create a comprehensive information security program to protect cardholder data, and to conduct annual security audits and maintain safeguards in connections to its franchisees.[63]

---

59. Brenda R. Sharton & David S. Kantrowitz, *Equifax and Why It's So Hard to Sue a Company for Losing Your Personal Information*, HARV. BUS. REV. (Sept. 22, 2017), https://hbr.org/2017/09/equifax-and-why-its-so-hard-to-sue-a-company-for-losing-your-personal-information [https://perma.cc/4QJM-D8CD]; Patrick Rucker, *Exclusive: U.S. Consumer Protection Official Puts Equifax Probe on Ice - Sources*, REUTERS (Feb. 4, 2018, 11:14 PM), https://www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ [https://perma.cc/AZ4B-523P]; Brian Fung & Hamza Shaban, *The FTC is Investigating the Equifax Breach. Here's Why that's a Big Deal*, WASH. POST (Sept. 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/ [https://perma.cc/5CQL-29K9].

60. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (holding that an alleged failure to maintain reasonable data security could constitute unfair competition and that the FTC has authority over some cybersecurity issuers pursuant to section 5 of the FTC Act); *Privacy & Data Security Update (2016)*, FTC (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 ("The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior.") [https://perma.cc/75FB-P63A]. *See also* Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) at 636 ("Even vague promises of security such as providing 'reasonable security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal information' can be the basis of an FTC action.")

61. *Wyndham*, 799 F.3d at 240.

62. *Id*. at 241 (In a mockery of good security practice, Wyndham also allowed its hotels to store payment information in clear readable text, used easily guessed passwords and usernames, had no firewalls to protect the system, allowed hotels to connect with out-of-date software, etc.).

63. *Wyndham Settles FTC Charges it Unfairly Placed Consumers' Payment Card Information at Risk*, FTC (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment [https://perma.cc/X7U3-TYYE].

In another action, the FTC charged HTC America with failing to take reasonable steps to secure its mobile devices.[64] The final settlement requires HTC to patch vulnerabilities, establish a comprehensive security program, and undergo independent security assessments for the next 20 years.[65] Notably, there were no allegations of actual harm in that case.[66] The recent *LabMD* decision effectively recognizes the ability of the FTC to regulate cybersecurity, but requires the FTC provide greater specificity in issuing orders so that those charged with an unfair or deceptive practice may be on notice of how to remediate.[67] The result of FTC enforcement actions is that companies will face fines, and potentially more burdensome ongoing requirements.

Because there are no preemptive federal data breach laws, a company that is subject to a data breach also potentially faces a number of suits from state Attorneys General. Notably, the HITECH Act gave state Attorneys General the "authority to bring civil actions on behalf of their state residents to enjoin conduct and/or obtain damages for violations of the HIPAA Privacy and Security Rules."[68] Moreover, each state has its own data breach law, further complicating the defense of a suit stemming from a breach exposing data from consumers in multiple states.[69] The exposure resulting from a data breach can be staggering. Massachusetts law, for example, allows a maximum penalty of five thousand dollars for each violation.[70]

64. *HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers,* FTC (Feb. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile [https://perma.cc/9P58-GMLM].

65. *Id*.

66. *Id*.

67. LabMD, Inc. v. FTC, 891 F.3d 1286, 1302 (11th Cir. June 06, 2018) ("assuming arguendo that LabMD's negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a), the Commission's cease and desist order is nonetheless unenforceable … [because] [i]t does not enjoin a specific act or practice.").

68. Jenny A. Durkan & Alicia Cobb, *After a Cyber Breach, What Laws Are in Play and Who is Enforcing Them?*, CYBERSECURITY LAW REPORT (May 20, 2015) https://www.quinnemanuel.com/media/1125067/cslr_after-a-cyber-breach-what-laws-are-in-play-and-who-is-enforcing-them.pdf (citing 42 U.S.C. § 1320d-5(d)(1) (2018) and Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5, 124 Stat. 226, Sec. 13410(e) (2009)) [https://perma.cc/X3XA-5BGA].

69. *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Feb. 6, 2018) http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx ("Forty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.") [https://perma.cc/8R8M-G3DG]; *see also State Breach Notification Laws*, FOLEY & LARDNER, LLP (Jan. 17, 2018), https://www.foley.com/state-data-breach-notification-laws/ (a comprehensive chart looking at breach notification laws across the U.S.) [https://perma.cc/GDR7-E63S].

70. MASS. GEN. LAWS, ch. 93A, § 4 (2018); Commonwealth. v. AmCan Enter., Inc., 47 Mass. App. Ct. 330, 338, (1999); Chris Hoofnagle (@hoofnagle), Twitter (Nov. 21, 2017), https://web.archive.org/web/20171226224852/https://twitter.com/hoofnagle/status/93

Suggestive of the exposure companies face, the Equifax breach resulted in leaking of data on 143 million Americans. At $5,000 per violation, the cost could be as high as $700 billion from state action.[71]

Companies with international footprints also face severe penalties in jurisdictions outside the United States. Chief among these is the General Data Protection Regulation (GDPR) promulgated by the European Commission which took effect in May of 2018.[72] The GDPR dramatically expanded liability for companies, for example, to data processors, rather than just data controllers.[73] Moreover, companies cannot escape liability by merely relocating their physical infrastructure outside of the EU because the GDPR, "applies directly to any entity that processes personal data about EU residents in connection with (i) the offer of goods or services in the EU; or (2) the monitoring of behavior in the EU."[74] Failure to comply with the GDPR can also be extremely costly to companies, amounting to fines of €10 million or 2% of global annual turnover (revenue) from the prior year for non-compliance with technical measures or €20 million or 4% of global annual turnover in the prior year for non-compliance with key provisions of the GDPR.[75]

The evolution of data-breach litigation and corresponding laws suggests that companies should be extremely sensitive to the development of their cyber practices and that mere reputation harm is giving way to costly civil litigation and enforcement actions. Although private actions still lag in terms of likelihood of success, regulatory enforcement can subject companies to massive fines and corrective measures.

3135314045906944 (Hoofnagle strongly implies in a tweet that in California a "violation" is per person, "Uber will have direct liability if facts bear out. Total liability is # of non-disclosure * $2500 - whatever the judge thinks reasonable. My guess is in excess of $500mm.") [https//perma.cc/764E-Y3KS].

71. *See* AmCan Enter., 47 Mass. App. Ct. at 338 ("In awarding $1,000,000 against the defendants . . . [t]he judge correctly noted that each deceptive solicitation may be viewed as a separate statutory violation for which a judge may . . . impose a separate civil penalty.").

72. *GDPR Portal: Site Overview*, EUGDPR.ORG, https://www.eugdpr.org/ (last visited Mar. 24, 2018) [https://perma.cc/K3EU-K4L5].

73. Jonathan Millard & Tyler Newby, *EU's General Data Protection Regulation: Sweeping Changes Coming to European and U.S. Companies*, ABA: SECTION OF LITIG. (May 23, 2016), http://apps.americanbar.org/litigation/committees/technology/articles/spring2016-0516-eu-general-data-protection-regulation.html [https://perma.cc/8JTX-G7U9].

74. *Id*. (An American near-miss analysis center is unlikely to be offering goods or services, or to monitor behavior in the EU, and so is likely outside the GDPR. Multi-national entities contributing data might choose to report [Systems administrator] rather than a name, or the analysis center might have appropriate confidentiality measures).

75. Technical measures such as impact assessments, breach notifications and certifications.

C. *Defining Incidents and Near Misses*

Given the potential legal minefield, it is important to take a step back and discuss the difference between an incident and a near miss,[76] so we can better understand the underlying incentives to share information.

Borrowing from the aviation industry's successes, we briefly sketch how defining incident and near miss works there. The aviation sector is comprehensively regulated by the FAA, and an aircraft accident is defined by law.[77] Near misses are defined as "when a person was able to avoid injury and/or illness, and when no property damage occurs" and that "documentation of near-misses is important for developing mishap prevention strategies."[78] Clear definitions of terms allows the FAA to say that near misses are events which are neither accidents nor crimes. The clear line between accident and near miss helps set minds at ease about reporting.

Generally, near-miss events occur when some controls function as intended, and others do not. This allows us to observe the failure of some controls and learn from those. Learning from near misses is something that safety engineers have long implemented in their practices.[79] Some define near misses as an "infrequent alarm or warning signal," cautioning that the definition cannot be too loose that near misses will be so common that they are ignored as "pesky nuisances."[80]

The concept of learning from what did work is very important. This was a lesson learned during World War II. Studying combat damage to returned aircraft, the military tended to add armor in the places that showed more hits. An American statistician, Abraham Wald, reasoned that this was incorrect: the planes that had returned were those that had survived; hits in those places were thus less likely to be fatal. By contrast, planes hit in other areas were shot down; thus, those areas—ones that had not been hit in the surviving planes—were

76. The profusion of definitions made for trouble even in writing this paper, with disagreement between authors on which word to use, and when to use them.

77. 49 C.F.R. § 830.2 (2016) ("[A]n occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight and all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage.").

78. FAA, CHAPTER 7. MISHAP REPORTING (Sept. 26, 2003), at 125 https://www.faa.gov/documentLibrary/media/order/occ_safety/order3900/media/ch07.pdf (definition of Near Miss) [https://perma.cc/383K-2283]; Richard Korman, *How Airlines Decide What Counts as a Near Miss,* THE ATLANTIC (Dec. 2, 2016), https://www.theatlantic.com/technology/archive/2016/12/aviations-opaque-definition-of-the-near-miss/509027 (Others have questioned the opacity of how the aviation industry determines what is "a forgettable mishap and [what is an] investigation-worthy mistake.") [https://perma.cc/A22M-5CN2].

79. Russell Cameron Thomas, *The Cost of a Near-Miss Data Breach*, THE NEW SCHOOL OF INFORMATION SECURITY: BLOG (Oct. 6, 2009), https://newschoolsecurity.com/2009/10/the-cost-of-a-near-miss-data-breach/ [https://perma.cc/VU45-Q47M].

80. Korman, *supra* note 78.

what needed armor.[81] A near-miss is thus the best thing to study: it represents not an attack that was easily deflected by common techniques, but one that just barely missed being successful, i.e., a serious danger point.[82]

One model for understanding near-misses is Reason's Swiss Cheese model.[83] Controls are represented as multiple "slices of swiss cheese." As a problem progresses, it may either bounce off the cheese or go through a hole. If it hits cheese, it falls away "harmlessly" as a "near miss." Only if it goes through the holes in each piece of cheese can it cause harm. This allows us to use near-misses to understand control failures, even if no harm occurs, because at least one "slice" has prevented the problem from progressing.[84]

In the cyber context, distinctions between a near-miss and an incident are not as clear, creating a perception that sharing information about what's going wrong may expose organizations to liability. As discussed above, there are many regulators and enforcers and many definitions for cyber incidents which they may cover.[85] For example, a computer security incident may be a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."[86] Even though such definitions are designed with the best of intentions to include "imminent threat," and computer security policies, they nonetheless create a problem for sharing near-miss information. If "incident" includes "imminent threats", then prudent legal practice may dictate treating those "imminent threats" as potential focal points for investigation or lawsuit.

Most of the efforts around defining incidents are focused on expanding and creating inclusive definitions. If companies are unclear as to the effects of disclosure of incidents or near misses and how such disclosure can potentially harm companies in subsequent civil litigation, they will be less likely to share near-miss information.[87] It may be possible for expansive definitions of incident and near-miss to co-exist peacefully in situations where reports go to different places,

81. W. Allen Wallis, *The Statistical Research Group, 1942-1945*, 75 J. AM. STATISTICAL ASS'N 320, 322–23. (1980).

82. This also illustrates that the dichotomy of "near miss" or "incident" may be too constraining, and public policy or a CSRS may benefit from a third category which is damaging but not catastrophic.

83. James Reason, *The Contribution of Latent Human Failures to the Breakdown of Complex Systems*, 327 PHIL. TRANSACTIONS OF THE ROYAL SOC'Y B: BIOLOGICAL SCI. 475 (1990).

84. *See* JAMES REASON, THE HUMAN CONTRIBUTION: UNSAFE ACTS, ACCIDENTS AND HEROIC RECOVERIES, 95–103 (2008).

85. Our discussion above is focused on liability for an organization that is breached. A comprehensive definition of incident might need to account for intrusions that violate the Computer Fraud and Abuse Act or other laws without meeting the criteria of a breach.

86. *About Us*, US-CERT, https://www.us-cert.gov/about-us [https://perma.cc/78KQ-ZJ8E].

87. *See* GERMANO & GOLDMAN, *supra* note 43, at 2.

and incentives are structured as influence on regulatory judgement. Reporting could then be something that both creates no additional jeopardy, and reporting an incident as if it were a near-miss produces no substantial benefit. Regardless, clear definitions cannot help but reduce uncertainty.

II. IMPROVE SCIENCE TO IMPROVE OUTCOMES

By observation, it is hard to secure systems.[88] We would like to be able to emulate the engineers who build bridges, and who assert that each new bridge will withstand the forces that will be brought to bear on it.[89] We'd like to be able to state that we have engineered in a safety factor, so even if our calculations are off, the bridge will not collapse. Neither the security of software nor computer operations have achieved an engineering discipline like that. We cannot describe the basic forces at work, the needed strengths of components, or assess a safety factor.[90] Engineers study both their practices and their outcomes. Their practices are the tasks, skills and methods that they bring to bear in a project, and the outcomes are the observed result of those practices.

In this section, we will discuss practices and outcomes that we believe are important to security and why, including: identifying what drives the selection of practices or controls in use today; determining how we assess the controls we're using, and how and what information is shared; and how new types of information flows could dramatically improve practices and outcomes.

A. What Security Practices and Outcomes are Important?

Organizations invest resources in information security practices, hoping to reduce the frequency and likelihood of incidents, which are a form of bad outcome.[91] Global spending on security products and

88. Tajha Chappellet-Lanier, *Audit: OPM Still Faces Information Security Weaknesses 2 Years After Breaches*, FEDSCOOP (July 11, 2017), https://www.fedscoop.com/opm-security-audit-2017/ [https://perma.cc/GWW8-EU9U].

89. *See* HENRY PETROSKI, ENGINEERS OF DREAMS: GREAT BRIDGE BUILDERS AND THE SPANNING OF AMERICA 75 (1996) (for background on bridge building practices; for an inquest into wind pressure involved in the collapse of the Tay Bridge).

90. *See generally* GARY MCGRAW, SOFTWARE SECURITY: BUILDING SECURITY IN (2006); STEVEN BELLOVIN, THINKING SECURITY: STOPPING NEXT YEAR'S HACKERS (2015); ADAM SHOSTACK, THREAT MODELING: DESIGNING FOR SECURITY (2014).

91. "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure" and "Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks."). NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1–2 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf ("Other outcomes to avoid include systems not delivered, systems

services is now approaching $100 billion.[92] In spite of these investments however, security incidents seem to be getting worse and more frequent.[93] Practitioners bemoan the difficulty of assessing risk to a granularity such as "very risky" or "not very risky," never mind quantifying risk. Such quantification is a precursor to being able to answer the question "does this practice or control change our risk?"

Security practice in industry is driven by a mix of standards and a desire to innovate to defeat emergent attack techniques, with the majority of spending historically focused on compliance with standards.[94] (There are exceptions, of the "proving the rule" sort.) However, standards are lagging, and so some organizations invest in innovation of various sorts.

It is reasonable to think that before a control is added to a standard, someone rigorously assessed it for effectiveness. The assessment could be done by a standards body, or they could rely on someone else's rigorous assessment. Unfortunately, we have few ways to assess effectiveness, and their rigor is open to question. In the matter of D-Link, the FTC relied on "the OWASP top ten" vulnerability list as part of their determination of what constitutes "reasonable" security.[95] But the process for determining that top ten list has come under scrutiny with some questioning whether one of the elements in a new draft version is merely a "vendor pitch."[96]

---

which are unusable, or which exceed their time or cost budgets…") [https://perma.cc/JLH4-3AM3].

92. *Gartner Says Detection and Response is Top Security Priority for Organization in 2017*, GARTNER (Mar. 14, 2017), http://www.gartner.com/newsroom/id/3638017 [https://perma.cc/PN6C-6TP5].

93. The U.S. does not mandate reporting of security incidents except in exceptional circumstances, and there is no centralized register of incidents which would allow us to authoritatively state that either the number or severity is rising. As required by FISMA, the U.S. Government does report on its own incidents. In the 2016 report, the Acting Federal Chief Information Security Officer says "the FY 2016 incident data is not comparable to prior years' incident data." Grant Schneider, *Federal Cybersecurity: Administration Releases Annual Report on Agency Cyber Performance*, FISMA, https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/FISMA_blog_v-7.pdf (last visited Mar. 24, 2018) [https://perma.cc/RT8U-TQA4].

94. Warwick Ashford, *Security Spending Not on Most-Effective Controls, Report Reveals*, COMPUTER WEEKLY (Jan. 25, 2018), https://www.computerweekly.com/news/252433722/Security-spending-not-on-most-effective-controls-report-reveals ("The report notes that while in the past, compliance has been the primary driver for setting security spending priorities, the fear of the financial penalties from data breaches has taken over the top spot, with 39% citing it as the top stimulus for security spending, up from 35% a year ago.") [https://perma.cc/8MMX-JNHK].

95. Complaint for Permanent Injunction and Other Equitable Relief at 5, FTC v. D-Link Corp., No. 3:17-cv-00039 (N.D. Cal. 2017), https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf (OWASP is a non-profit that assembles a top ten list of vulnerabilities, but knowing that list is usually referred to simply as "the top ten" gives a sense of its pervasiveness.) [https://perma.cc/SW4F-HKSE].

96. Steve Ragan, *Contrast Security Responds to OWASP Top 10 controversy*, CSO (Apr. 26, 2017, 4:00 AM), https://www.csoonline.com/article/3192505/security/contrast-security-responds-to-owasp-top-10-controversy.html (discussing the charges that a new addition to the top 10 was merely a marketing campaign for existing Contrast Security products) [https://perma.cc/PN4K-DEM5].

Overall, the standards process suffers from a variation of the difficulty of assessing risk, which is that when a new practice or control is suggested for a standard, it is hard to assess: if the control works (or in what circumstances it works); if the new control offers good return on invested effort; or if the control offers better or worse returns than other proposed controls.

The outcomes which are most noticeable today are "breaches" of control over personal information. Usually, but not always, they are disclosed because of breach disclosure laws and attendant publicity.[97] Other breaches are publicized because the attacker publicizes it by defacing a website,[98] using a Twitter account to say things derogatory to its owner,[99] or the data is leaked, for example, the Panama Papers.[100]

Many incidents are not disclosed.[101] There are substantial disincentives to disclosure.[102] If you disclose penetrations, lawsuits follow,[103] and investigations by regulators or enforcement agencies may also follow. Penalties for failing to disclose breaches vary by state, with some states imposing penalties per failure to notify, per breach, or for knowing violations.[104] We do not here take a position on the

97. *See* NAT'L CONFERENCE OF STATE LEGISLATURES, *supra* note 69; *see also* Data Security and Breach Notification Act, S.2179, 115th Cong. (2017) (Bill proposed in congress creating a federal disclosure requirement of breaches following the cover up of a breach by Uber).

98. ZHONE-H: UNRESTRICTED INFORMATION, http://www.zone-h.org/archive [https://perma.cc/XPV3-8FF5] is a collection of such events, as is FREEDOMHACKER, https://freedomhacker.net/category/website-defacement/ [https://perma.cc/C4QL-H3Z7].

99. *See* Chris Crum, *Skype Blog Hacked To Tell People Not To Use Microsoft Email*, WEBPRONEWS (Jan. 2, 2014), https://www.webpronews.com/skype-blog-hacked-to-tell-people-not-to-use-microsoft-email-2014-01/ (Syrian Electronic Army took over the @skype Twitter handle, and tweeted a link to a Skype blog which said, "Don't use Microsoft emails (hotmail, outlook), They are monitoring your accounts and selling the data to the governments.") [https://perma.cc/YKU2-QXXD].

100. Luke Harding, *What are the Panama Papers? A Guide to History's Biggest Data Leak*, THE GUARDIAN (Apr. 5, 2016, 5:42 AM), https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers [https://perma.cc/J44S-SFQZ].

101. *See* Robert McMillan, *Most Retailer Breaches Are Not Disclosed, Gartner Says*, CIO (May 23, 2008, 8:00 AM), https://www.cio.com/article/2436102/infrastructure/most-retailer-breaches-are-not-disclosed—gartner-says.html ("In a new study based on interviews with 50 U.S. retailers, Gartner found that 21 of them were certain they had had a data breach. However, just three of the retailers had disclosed the incident to the public.") [https://perma.cc/E6GC-C5G4]. Security experts understand that measuring hidden data is hard, and that these numbers remain broadly indicative of the levels at which incidents are concealed or disclosed. As we were writing this, it came out that "Uber concealed [a] data breach affecting 57 million people." *See Uber Concealed Data Breach Affecting 57 Million People*, BNONEWS (Nov. 21, 2017, 5:50 PM), http://bnonews.com/news/index.php/news/id6751 [https://perma.cc/P5CE-7AFG].

102. *See* Danny Yadron, *Executives Rethink Merits of Going Public with Data Breaches*, WALL ST. J. (Aug. 4, 2014, 7:17 PM), https://www.wsj.com/articles/a-contrarian-view-on-data-breaches-1407194237 [https://perma.cc/TKA3-SFJW].

103. One attorney said "And your disclosure letter will be exhibit A!" (personal communication).

104. For example, Alaska has a "Civil penalty payable to state of up to $500 for each state resident who was not notified, except that the total civil penalty may not exceed $50,000"; Hawaii says, "Any business that violates any provision of this chapter shall be subject to penalties of not more than $2,500 for each violation." *State Breach Notification Laws*, FOLEY & LARDNER, LLP (Jan. 17, 2018), https://www.foley.com/files/Publication/c31703ac-ee93-40a5-

desirability of such penalties. The argument for a penalty is that without one, no one would take on the risks that accompany reporting a breach. The argument against is twofold: first, computers often behave oddly, and to attribute malice or recklessness to what might be randomness can be expensive; second, warnings are often vague. For example, "[i]n its initial contact with the DNC last fall, the FBI instructed DNC personnel to look for signs of unusual activity on the group's computer network, one person familiar with the matter said. DNC staff examined their logs and files without finding anything suspicious, that person said."[105] In this example case, is it fair to penalize the DNC for not finding anything suspicious? A system that balances these disincentives with incentives could substantially improve computer security.

We would like to reduce the number of important incidents in cyber, by increasing the predictability of those events, and reducing their impact.[106] Both of these goals are quantitative. Each requires some form of data gathering. Assessing the predictability of events can be done bottom-up, that is, how likely is this entity to suffer an event; or top-down, that is, out of this population, how many entities will suffer? Impact can also be quantified, by dollar losses, stock price losses, or estimating with other yardsticks. As long as the estimation methods are consistent, then we can assess whether the impact of

---

b295-7e1d9fe45814/Presentation/PublicationAttachment/d6373e89-f460-44fa-afec-a2cbe9fa23fd/17.MC5826%20Data%20Breach%20Chart%200817%20R1.pdf [https://perma.cc/N7XN-B2HQ]. Massachusetts specifies, "[t]he Attorney General may seek injunctive relief, a $5,000 penalty for each violation, and reasonable costs and attorney's Fees." Missouri, in contrast, says, "[t]he Attorney General shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation." STATE DATA BREACH LAW SUMMARY, BAKERHOSTETLER (2017), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf [https://perma.cc/N9S3-FF6L]. Notably, Alabama and South Dakota do not have breach notification laws as of September 1, 2017. *State Date Security Breach Notification Laws*, MINTZ LEVIN, https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (last updated Sept. 1, 2017) [https://perma.cc/9CF3-HGFS]. *See also* Data Security and Breach Notification Act, S. 2179, 115th Cong. (2017) (bill imposes mandatory reporting following a breach and creates criminal penalties for intentional and willful concealment of a breach).

105. *See* Mark Hosenball et al., *FBI Took Months to Warn Democrats of Suspected Russian Role in Hack: Sources*, REUTERS (Aug. 2, 2016, 8:55 PM), https://www.reuters.com/article/us-usa-cyber-democrats-reconstruct/fbi-took-months-to-warn-democrats-of-suspected-russian-role-in-hack-sources-idUSKCN10E09H?feedType=RSS&feedName=technologyNews [https://perma.cc/M8WC-EJEQ]; *Cf.* Adam Shostack, *FBI Says their Warnings were Ignored*, ADAM SHOSTACK & FRIENDS (Aug. 17, 2016), https://adam.shostack.org/blog/2016/08/fbi-says-their-warnings-were-ignored/ (the FBI had evidence that the DNC was being hacked by the Russians, and they said "look around for 'unusual activity.'") [https://perma.cc/E8PF-8V4L].

106. There are quantitative approaches to risk assessment. *E.g.*, JACK FREUND & JACK JONES, MEASURING AND MANAGING INFORMATION RISK: A FAIR APPROACH (2015); DOUG HUBBARD ET AL., HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK (2016). However, the data which is used as input to those mechanisms is not standardized, shared, or scrutinized, and both authors would agree that their methods could work much better with better data.

events is increasing or decreasing over time.[107] How many entities will suffer, and how badly they will suffer, depends on their practices and the effectiveness of those practices. As discussed above, this is hard to measure.

B. The Importance of Data

Today's information sharing can usefully be broken into "sharing" and "publication." Information is often shared, with rules about where it can be sent, and some of it, often relating to vulnerabilities, is then published and made available to all comers. But a great deal of data, including "indicators of compromise"[108] is never published.[109]

Published information about vulnerabilities enables several valuable tasks. First, it can help to prioritize the application of fixes or patches. Second, it can help with finding variations or similar vulnerabilities. Third, the open publication of vulnerability information enables research in a variety of ways.[110] That research includes statistical analysis of vulnerability characteristics, and research into defensive techniques such as address space layout randomization.

Perhaps the best example of this research is the class of problems called "buffer overflows."[111] Knowledge of such problems were kept

107. Dan Geer, *A Quant Looks at the Future: Extrapolation via Trend Analysis*, http://geer.tinho.net/geer.cerias.21iii07.pdf ("First, trend analysis is what a statistician will recommend when the underlying topic of interest is changing and the method of measuring it is uncertain. In such a circumstance, and so long as the measurement you do have can be applied consistently, the trend data can be relied on and it is what you need for decision support.") [https://perma.cc/Y5YB-HAXJ]. Most events are reasonably measurable, as the majority of costs are operational expenses in response, capital expenses for upgrades, one-time costs of notification, or impact to reputation/goodwill. There are events that are difficult to quantify, such as the leak of John Podesta's emails during the 2016 Presidential election, which is challenging because of scope. Are we to assess the damage to the Democratic National Committee, the impact on the election, or the impact of the election on the country?

108. Nate Lord, *What are Indicators of Compromise?* DATA GUARDIAN (July 27, 2017), https://digitalguardian.com/blog/what-are-indicators-compromise (indicators of compromise are "pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.") [https://perma.cc/YA6Q-4ZXW]. The frequency of discussion around "what may I say about this" has led the Forum of Incident Response Security Teams to create a "traffic light protocol" as shorthand for sharing rules, *e.g.*, *Traffic Light Protocol*, FIRST, https://www.first.org/tlp/(last visited Mar. 5, 2018) [https://perma.cc/M8UN-RBES], which has been adopted by many others. These rules are so frequently invoked that it is not unusual in to hear something like "Tee-Ell-Pee red" in response to the question, "can I share that?"

109. Since the data is not published, it is hard to assess relative quantities.

110. Researchers are often hesitant to plan work whose initiation or publication includes needless uncertainty.

111. In buffer overflow attacks, an attacker sends a program more data than it is expecting, originally intended for what is known as an "input buffer." If the program does not detect and handle this situation, other areas of memory can be overwritten, with dire consequences. Conceptually, imagine a clerk writing down someone's name, but the name as given is so long that it doesn't fit in the box on a form and spills over into the "Official Use Only" section of the form. A carefully constructed overflow can install new computer code,

as tribal knowledge for at least 25 years[112] before they were published in detail for others to learn from. Within a few years of the first detailed description, a systematic fix was developed.[113] Additional prominent examples include Hoare's Turing Lecture, in which he describes a choice to perform bounds checking in a 1960 compiler.[114] Each of these discussions chose not to describe the attack technique in depth, perhaps to avoid providing a "roadmap for attackers." However, attackers had their own roadmap. The 1988 Morris worm exploited a buffer overflow in fingerd[115] as one of its propagation mechanisms.[116] In 1996, a hacker known as Aleph One published a paper now recognized as seminal, "Smashing the Stack for Fun and Profit."[117] The paper detailed the problem, and techniques for exploiting it to gain privileges beyond what the system designers intended.[118] Within a year[119], Crispan Cowan and colleagues built "StackGuard," and their

code written by the attacker. For more information, *see generally* SEAN SMITH & JOHN MARCHESINI, THE CRAFT OF SYSTEM SECURITY 6.1 (2008).

112. The trouble with tribal knowledge is that it is undocumented. One author attempted to find earlier, written, references, to back up personal recollections. Adam Shostack, *Buffer Overflows and History: A Request,* ADAM SHOSTACK & FRIENDS (Oct. 20, 2008), https://adam.shostack.org/blog/2008/10/buffer-overflows-and-history-a-request/ [https://perma.cc/V3LK-8AZF].

113. The earliest such fix we could find in the literature was in 1971. *See* JAMES P. ANDERSON, COMPUTER SECURITY PLANNING STUDY 61 (1972), http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf, ("In one contemporary operating system, one of the functions provided is to move limited amounts of information between the system and user space. The code performing this function does not check the source and destination addresses properly, permitting portions of the monitor to be overlaid by the user. This can be used to inject code into the monitor that will permit the user to seize control of the machine.") [https://perma.cc/V8U6-F9X2].

114. C.A.R. Hoare, Lecture at Communications of the ACM: The Emperor's Old Clothes (Oct. 27, 1980) ("A consequence of this principle is that every occurrence of every subscript of every subscripted variable was on every occasion checked at run time against both the upper and the lower declared bounds of the array. Many years later we asked our customers whether they wished us to provide an option to switch off these checks in the interests of efficiency on production runs. Unanimously, they urged us not to—they already knew how frequently subscript errors occur on production runs where failure to detect them could be disastrous. I note with fear and horror that even in 1980, language designers and users have not learned this lesson. In any respectable branch of engineering, failure to observe such elementary precautions would have long been against the law.").

115. Fingerd was a standard network server on the computers of the day.

116. *See* Jon A. Rochlis & Mark W. Eichin, *With Microscope and Tweezers: The Worm from MIT's Perspective,* 32 COMMUNICATIONS OF THE ACM 689 (1989); the resulting indictment was the first case brought under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012); *see* United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

117. Aleph One, *Smashing the Stack for Fun and Profit,* PHRACK (Nov. 8, 1996), http://phrack.org/issues/49/14.html [https://perma.cc/H7GN-VWH9].

118. Generally, that was either an elevation from "not authorized to use the system" to "can run code on the system," or from "unprivileged and able to run code" to administrative privilege.

119. The publication dates appear slightly further apart, but note that the call for papers, *7th USENIX Security Symposium*, USENIX, http://www.usenix.net/legacy/publications/library/proceedings/sec98/cfp.html (last visited Mar. 12, 2018) [https://perma.cc/2JYC-TWXK], had a submission deadline of September, 1997, which was 10 months after the publication of Smashing the Stack, and that the paper has a full section of experimental results.

paper presents experimental results.[120] Even with the first version built, the team wanted to continue to improve Stackguard[121] In 1998, one author of this paper (Shostack) was an executive at an early vulnerability scanning company (Netect), and at a trade show, Cowan approached us to see if we could provide him with a feed of vulnerabilities which he could use to test StackGuard.[122] So even after the paper was published, there was a real engineering need for more and detailed information to test defensive mechanisms.

The endurance of problems like buffer overflows and the Morris worm are symptoms of a failure to learn from mistakes. Both were largely resolved when the attacks were described in depth to the public. Publishing such data is critical to improving the overall security of systems, and we need mechanisms to investigate, gather, analyze or disseminate root cause information.

The lack of suitable real-world data has led parts of the security research community to use "synthetic datasets" instead.[123] Unfortunately, constructing a suitable synthetic dataset is difficult. That said, researchers have been driven to using them despite their known deficiencies. For example, the so-called Lincoln Labs intrusion detection test dataset is known to be flawed:[124]

> "The corpus generated by Lincoln is unique in the Intrusion Detection arena and, as such, is the only substantial body of data that can be used for repeatable comparisons of IDS systems. At the same time, it may suffer from problems such as those noted above and may not provide results that reflect field performance. It appears to be used by researchers who were not part of the DARPA evaluation who should be aware of both its strengths and limitations."[125]

Information about breaches is published,[126] but usually in the context of how many "records" were stolen. Information about the proximate causes of the breach is rarely published. Claims such as "a

120. CRISPAN COWAN ET AL., STACKGUARD: AUTOMATIC ADAPTIVE DETECTION AND PREVENTION OF BUFFER-OVERFLOW ATTACKS (1998), http://www.usenix.net/legacy/publications/library/proceedings/sec98/full_papers/cowan/cowan.pdf [https://perma.cc/AD2K-8DN8].

121. This is standard engineering practice, to build a version 1, a version 2, et cetera, and should not be read as a criticism of the approach or the first release of StackGuard.

122. Personal communication with author Shostack.

123. A synthetic dataset contains artificial data, generated to resemble real data but having no basis in any actual occurrences.

124. The dataset is so well known in the intrusion detection community that it is mentioned without any formal citation. John McHugh, *Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory*, 3 ACM TRANSACTIONS ON INFO. & SYSTEM SEC. 262 (2000).

125. *See generally id.*

126. Generally, legislators have discussed publication as a punishment, a deterrent, and as a source of learning.

sophisticated criminal" are common. Such claims do not allow us to learn. Rarely, there is a public investigation, such as into the 2017 Equifax breach. There, the company revealed that a failure to patch a server allowed an attacker to break in, but what went wrong is unclear.[127]

In the case of Equifax, we seem to have an unusual amount of information about the failures. From the congressional hearing transcript:

> Mr. Smith. "[T]he security team notified a wide range of people in the technology team who were responsible for then finding the vulnerability, applying the patch, and then, days later as is typical protocol, to deploy a technology scanner to go then look for the vulnerability, find the vulnerability, if it found a vulnerability it knew it was not patched. Both human deployment of the patch and the scanning deployment did not work. The protocol was followed."[128]
>
> Mr. Smith. "The human error was the individual who is responsible for communicating in the organization to apply the patch did not [so communicate]."[129]
>
> The Chairman. "So does that mean that that individual knew that the software was there and it needed to be patched and did not communicate that to the team that does the patching? Is that the heart of the issue here?"[130]
>
> Mr. Smith. "And I should clarify there that the rationale or the reason why the scanner or the technology piece did not locate the vulnerability is still under investigation by outside counsel."[131]

This seems like quite a bit of information, but when we ask questions, answers are less forthcoming. Questions we can ask include: what was "the protocol?" In what way was it followed if "the individual who is responsible for communicating in the organization to apply the patch" did not do so? How many patches are

127. *Oversight of The Equifax Data Breach: Answers for Consumers, Hearing before the H. Comm. On Digital Commerce and Consumer Protection, Comm. On Energy and Commerce*, 115th Cong. 33-36 (2017), http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Transcript-20171003.pdf [hereinafter *Equifax Hearing*] (Testimony of Richard Smith) [https://perma.cc/44LV-TQM8]; *See Oversight of the Equifax Data Breach: Answers for Consumers*, COMM. ON ENERGY & COMMERCE (OCT. 3, 2017), https://energycommerce.house.gov/hearings/oversight-equifax-data-breach-answers-consumers/ (describing details of the hearing) [https://perma.cc/FK7R-5WU8].

128. *Id*. at 34.

129. *Id*. at 35–36.

130. *Id*. at 36.

131. *Id*. at 37.

communicated about per day? Through what medium—email, ticketing, post-it notes—is communication performed? Was there a protocol for ensuring that the technology located vulnerabilities? Obviously, we know that there was a failure, but not what it was. Moreover, we do not know how the breach was detected. We do not know how data was exfiltrated. We do not know what controls Equifax had in place at the time of the breach to detect a breach or to detect data loss.

If a corporate board were to ask a security expert to evaluate if the specific issues which happened at Equifax could happen to them, that expert could not give a complete answer given the limited data available.

Moreover, the information from which lessons might be learned from the breach is subject to several filters. Those filters include that the former CEO was discussing them, that there is an active law enforcement investigation, that many lawsuits have been filed, and that the questioners were not technically savvy.

There are certainly lessons which can be extracted from the testimony, but those lessons are a small subset of what might be learned. Those lessons must be extracted from the messy transcripts and many news stories, such as "The Equifax Hack Has the Hallmarks of State-Sponsored Pros."[132] The process of extracting lessons from many news stories is time consuming and expensive. We have no way to ask the question "is my vulnerability scanner better than Equifax's?" We cannot answer the question "what vulnerability scanner failed, and why" to start the comparison.

III. POLICY ENTREPRENEURSHIP CAN STIMULATE SCIENTIFIC EFFORTS

We recommend the creation of a Cyber Safety Reporting System to better equip companies to answer the hard questions discussed in Section II. This plan involves a mixture of industry involvement and policy entrepreneurship from government, and is one we think necessary to improving the flow of security information between defenders. In this section, we explore the policy entrepreneurship needed to create a CSRS, and why government would want this innovation. We also explore ways to structure a CSRS, and consider the benefits of a centralized reporting system.

Policy entrepreneurship in this area would include two pillars. The first pillar is shaping industry incentives—considering participation as a factor in regulatory judgement when determining liability. The second would be protecting confidentiality.

132. Michael Riley et al., *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG (Sept. 29, 2017, 7:09 AM), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros [https://perma.cc/RCS3-NSEH].

Most regulators today have a set of factors they take into account in determining liability. Those factors might be read to include participation in a near-miss program or experiment, or they might be extended.

The second pillar is explicitly shielding the confidentiality of reports and reporters. No organization wants to create a roadmap to its own prosecution by an overzealous prosecutor or regulator. Regulators could help by explicitly stating that experiments or activity in near-miss reporting would receive Cybersecurity Information Sharing Act (CISA) protections,[133] and that they would not seek to test that protection.

A. The First Pillar: Encouraging Experimentation and Providing Leniency

As a matter of public policy, regulators should incentivize and remove roadblocks to experimentation, especially when dealing with a rapidly changing technology.[134] When designed to address regulatory challenges, such experimentation helps agencies and companies "earn regulatory authority."[135] The earned regulatory authority model asserts that authority is developed through "experimentation and effective administration," whereby innovative regulatory policies are rewarded with "more formal authority and budgetary support," often by Congress.[136] Regulators should encourage and be encouraged to explore new solutions to existing problems; in this case the use of leniency towards cybersecurity information sharing regimes can remove roadblocks to sharing.

Collection of information is essential to the success of the this proposed CSRS, however the liability concerns discussed in Section I can present a significant disincentive for companies to share. This principally stems from the risk that sharing of near-miss information can still result in liability for companies if the near-miss is actually an incident. Relevant enforcement agencies must therefore be willing to grant leniency for companies that choose to participate in the program,

133. Brad S. Karp et al., *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCHOOL F. (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ ("These protections include protections from liability, non-waiver of privilege, and protections from FOIA disclosure, although, importantly, some of these protections apply only when sharing with certain entities.") [https://perma.cc/6YR4-4H28].

134. Phil Weiser, *Entrepreneurial Administration*, 97 B.U. L. REV. 2011, 2013 (2017) ("[I]n the case of technologically developing fields where experimental regulatory strategies—as opposed to traditional notice-and-comment rulemaking or adjudication—are often essential.").

135. *Id.* at 2013–14 (discussing earned authority in the context of ENERGY STAR, a program developed by the EPA, and later codified by congress, and the LEED building standard which is developed and overseen by a private organization, but which has been endorsed by several agencies).

136. *Id.* at 2067–68.

and may do so through explicit statutory safe harbors (as in the case of CISA discussed above), memoranda of understanding committing to "avert their eyes,"[137] regulatory forbearance, or prosecutorial discretion. Ultimately, a CSRS program might be codified in a statute to provide certainty of protection after experimentation to achieve an optimal structure.

By exploring how experimentation is implemented in other instances, we might better understand how to apply it to cybersecurity information sharing regimes.

In the case of ASRS, the FAA recognizes that "[t]he effectiveness of this program in improving safety depends on the free, unrestricted flow of information. . . ."[138] To help ensure that goal is met, the FAA delegated to NASA the job of collecting and analyzing near-miss information to protect anonymity including anonymity with respect to "the regulator," and generally increase the effectiveness of the program.[139] Companies can be more confident that they are protected from liability and thus be more willing to disclose the information to improve everyone's practices because of regulatory restrictions on the FAA's use of ASRS reports.[140]

FTC enforcement actions often consider the general culpability of the company and whether it was helping or hindering the investigation.[141] Such prosecutorial discretion acts as both a carrot and a stick to motivate companies to behave well and disclose more information over the course of the investigation, or risk more severe penalties later. The FTC has also sometimes expressed a preference for self-regulation, and self-regulatory approaches may be easier to achieve than new regulation or legislation.[142]

---

137. Such a memoranda exists, for example, between the FAA and NASA—"NASA, rather than the FAA, accomplished the receipt, processing, and analysis of raw data [to]ensure the anonymity of the reporter . . . [and] increase the flow of information necessary for the effective evaluation of the safety and efficiency of the system." *Immunity Policies*, AVIATION SAFETY REPORTING SYSTEM, https://asrs.arc.nasa.gov/overview/immunity.html (last visited Mar. 24, 2018) [https://perma.cc/BX2R-VLJ8].

138. *Id.*

139. *Id.* ("NASA ASRS provides for the receipt, analysis, and de-identification of Aviation Safety Reports. In addition, ASRS publishes and distributes periodic reports of findings obtained through the reporting program to the public, the aviation community, and the FAA.").

140. *See* 14 C.F.R. § 91.25 (2018) (stating that the Federal Aviation regulations prohibit the use of reports submitted to ASRS program in disciplinary actions, unless it concerns accidents or criminal investigations, which are otherwise excluded from the program.).

141. Mark Eichorn, *If the FTC Come to Call*, FTC (May 20, 2015, 10:51 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (The FTC will "consider the steps the company took to help affected consumers, and whether it cooperated with criminal and other law enforcement agencies . . . a company that has reported a breach to the appropriate law enforcers and cooperated . . . [would be viewed] more favorably than a company that hasn't cooperated.") [https://perma.cc/P6DE-DDVB].

142. *Self-Regulatory Principles for Online Behavioral Advertising*, FTC (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [https://perma.cc/7L4T-B2ZV].

The Federal Communications Commission (FCC) uses regulatory forbearance as a tool to achieve public policy goals in a flexible manner. The Telecommunications Act grants the FCC significant discretion as to whether it will forbear from some or all provisions of the Act.[143] This grant of flexibility was used most notably in the Open Internet Order whereby the Commission forbore from over 27 provisions of the Act and 700 different rules and regulations following its conception of "light-touch" regulation.[144] While some view forbearance with skepticism and alarm due to potential abuses, others have demonstrated that it is more appropriately seen as a form of implementation of statutes that Congress writes, filling in gaps in the law, and addressing perennial governance problems often anticipated by Congress itself.[145]

The SEC maintains significant regulatory authority over the financial sector, both mandating industry behavior and disciplining bad actors. The SEC will often work in conjunction with the DOJ in pursuing joint or individual enforcement actions against persons for charges of insider trading.[146] This prosecutorial discretion in bringing actions allows the SEC to more efficiently allocate its scarce resources and to provide the flexibility necessary to ensure fairness in its enforcement process.[147] The SEC requires companies to operate compliance hotlines, and operates a whistleblower program for accounting fraud. At the same time, they are actively probing companies regarding their cyber practices and disclosures.[148] Recently, they have issued guidance that companies should "require employees to appropriately record, process, summarize and report up the

143. 47 U.S.C. § 160 (2012) ("[T]he Commission shall forbear from applying any regulation or any provision. . . [if] enforcement of such regulation or provision is not necessary to ensure that the charges. . . are just and reasonable and are not unjustly or unreasonably discriminatory. . . enforcement of such regulation or provision is not necessary for the protection of consumers; and forbearance from applying such provision or regulation is consistent with the public interest.").

144. *Protecting and Promoting the Open Internet*, GN. Dkt. No. 14-28, Report & Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, 5604 n.6 (2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf [hereinafter Open Internet Order] [https://perma.cc/YER6-FXE3].

145. *See* Daniel T. Deacon, *Administrative Forbearance*, 125 YALE L.J. 1548 (2016).

146. *See* Mitchell E. Herr, *SEC Enforcement: A Better Wells Process,* 32 SEC. REG. L.J. 56 (2004). The Assistant U.S. Attorneys in combination with the SEC will often exercise prosecutorial discretion when, for example, "no federal interest would be served by prosecution. . . . the person is subject to effective prosecution in another jurisdiction. . . . [or] there exists an adequate non-criminal alternative to prosecution." U.S. DEP'T OF JUST., U.S. ATTORNEYS' MANUAL, 9-27.230, 9-27.220, https://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution#9-27.230 (last visited Mar. 24, 2018) [https://perma.cc/9VFM-U9M9].

147. Herr, *supra* note 146, at 57.

148. *See* Derek Bambauer, *Ghost in the Network*, 162 U. PENN. L. REV. 1011, 1038 (2014) (noting section 404 of the Sarbanes–Oxley Act of 2002 requires firms to "document their internal controls for financial reporting, including those reliant on information technology, and then demonstrate to their auditors' satisfaction that they have implemented those controls").

corporate ladder any information related to cybersecurity risks and incidents that is potentially required to be disclosed in public filings."[149] Requirements for disclosure are being revisited, and large ($35m) fines have been imposed.[150] Financial institutions under the Gramm-Leach-Bliley Act of 1999 are also mandated to protect consumers' personal information by requiring that "firms assess the risks they face, design a set of countermeasures, implement it, test it, and adjust the countermeasures as circumstances change."[151] While the authority of the SEC under these statutes is limited to the financial sector, a sector specific CSRS would nevertheless align with the desire to create a robust cybersecurity system for large companies and financial institutions.

The Department of Health and Human Services stands as a case where explicit regulatory authority should be met with greater experimentation.[152] Under the auspices of HIPAA and HITECH Act, HHS has formal regulatory authority to push improved cybersecurity practices.[153] Unfortunately, the HHS's "Security Rule is not clearly defined, has failed to incorporate relevant NIST guidance, and is poorly enforced."[154] Indeed, this failure in oversight forced the FTC to intervene in the case of LabMD as discussed in Section I above.[155] Congress reacted to the HHS's problems in passing the 21st century Cures Act to both empower the enforcement of greater information sharing by the inspector general, and to convene industry to create a model framework for securely sharing information.[156]

Among these various examples, we see that government agencies are often willing to experiment with different regulatory levers to achieve public policy goals. Whether the lever be explicit in statute as in the case of CISA, less defined but congressionally blessed as in the case of the FCC or FTC, or the prosecutorial discretion common to all

149. See Proskauer, *SEC Issues Updated Guidance on Public Company Cybersecurity Disclosures*, March 5, 2018, https://www.proskauer.com/alert/sec-issues-updated-guidance-on-public-company-cybersecurity-disclosures [https://perma.cc/YQA9-7YWS].

150. See SEC, *Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million*, April 24, 2018, https://www.sec.gov/news/press-release/2018-71 ("Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors. The fact of the breach was not disclosed to the investing public until more than two years later…") [https://perma.cc/5LS5-5F9L]. Such regulatory entrepreneurship creates demand for ways to demonstrate good faith, and near-miss reporting could serve that purpose.

151. *Id.* at 1039 (citing to the Financial Services Modernization Act of 1999, 12 U.S.C. § 1811 (2012)).

152. Weiser, *supra* note 134, at 2068–72 (discussing the HHS's failure to spur steps to encourage better cybersecurity practices and to facilitate information sharing despite having authority to do so).

153. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936; Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5, 124 Stat. 226 (2009).

154. Weiser, *supra* note 134, at 2069 (citing a GAO report).

155. *See id*. *See also* discussion *supra* Part I.

156. Weiser, *supra* note 134, at 2072.

of the enforcement agencies, it should be no different in the case of cybersecurity information sharing, in order to optimize the amount of data available so that companies may learn to better protect themselves.

Regulatory judgement should nonetheless remain intact, with the caveat that good faith participation in the CSRS program would act as a factor in determining the culpability of the company should an incident occur. A key benefit of the CSRS program, much like its ASRS counterpart, is the ability to work ex ante to prevent problems rather than waiting until an incident has happened to make improvements. In this way, a company can act proactively to defend its systems and customers. The reporting of information must therefore be protected to ensure that companies disclose meaningful information freely. Such protection does not mean however, that a company is insulated from all consequences of a failure to adequately protect data, rather it seeks to encourage the production of data necessary to generate meaningful reports regarding how companies may improve their cybersecurity.

Without leniency, the risk of legal exposure from enforcement or other civil actions may be prohibitive for companies considering reporting, absent other countervailing incentives. This concern may be traversed by appropriately structuring the sharing regime. First, the willingness to participate in the program should be taken into account and factored into the leniency of the regulatory agency, as is the case of FTC. In the case of ASRS as noted above, the regulation specifically estops the FAA from using the data shared unless the data is otherwise not part of the ASRS program.[157] The ASRS model splits the work among several agencies to help ensure the data is protected, whereby NASA gathers and analyzes the data, but the FAA will have an option to use the data if the disclosure falls outside of specific definitions of the program. While not a perfect solution for companies which may inadvertently disclose something that can harm them, explicit protections can help companies to make informed decisions about what information they share and—if appropriately incentivizing—allows information to flow more freely.

B. The Second Pillar: Confidentiality and Anonymity Must be Protected

Even with explicit protections, companies may still be worried about the sensitivity of the information being supplied and the possibility that such information would be subject to subpoenas or Freedom of Information Act (FOIA) requests. In response, we can observe how ASIAS has handled such concerns. ASIAS is run by the

157. 14 C.F.R. § 91.25 (2018).

MITRE corporation, and is thus not subject to FOIA requests,[158] and while ASIAs has never been subpoenaed, MITRE notes that it has a plausible defense and that companies themselves are more likely to be subpoenaed for the information than MITRE is.[159] While not ironclad, a similar design for a CSRS could involve providing notice to the reporting company if the CSRS was ever subpoenaed. Even if the ultimate organization housing the ASRS program is a government entity such as NASA, an exemption to FOIA requests exists for confidential commercial information,[160] and another for those sharing certain cybersecurity data.[161]

C. Organizing a CSRS

There are many possible structures for the organization and funding of a new Cyber Safety Reporting System or Cyber Resilience Reporting System. There are two major questions: a home for the organization, and the source of support. As illustrated by the NASA-FAA partnership, they can be separate.[162] Organizationally, our choices are: stand up a new organization, host it in an existing non-profit, or host it within a government agency. It could nominally exist within a for profit company, but that would be self-defeating. Similarly, creating a new organization adds to the challenges of getting started, and there are no obvious commensurate benefits. We explore a few of the options for housing the project below. This discussion is designed to illustrate opportunities, rather than to state that these are the only appropriate homes or authorities which could work.[163]

158. ASIAS, GENERAL AVIATION ASIAS FAQS 6 (2016), http://www.aeronomx.com/uploads/1/0/9/6/10969420/ga_asias_faqs_pr_11-2016_rev2.pdf [https://perma.cc/Z4VQ-5K3H].

159. *Id.*

160. *What are FOIA Exemptions*, FOIA, https://www.foia.gov/faq.html#exemptions (Exemption 4, "Trade secrets or commercial or financial information that is confidential or privileged.") (last visited Mar. 24, 2018) [https://perma.cc/S28T-PVM7].

161. Weiser, s*upra* note 134, at 2067.

162. Some agencies are encouraging the reporting of near misses. For example, the New York Department of Financial Services says: "The Department believes that analysis of unsuccessful threats is critically important to the ongoing development and improvement of cybersecurity programs. . . Notice of the especially serious unsuccessful attacks may be useful to the Department . . . and the knowledge shared through such notice can be used to timely improve cybersecurity generally . Accordingly, Covered Entities are requested to notify the Department of those unsuccessful attacks that appear particularly significant. . ." However, they recognize that reporting a near miss to a regulator may raise concerns about being penalized: "The Department trusts that Covered Entities will exercise appropriate judgment as to which unsuccessful attacks must be reported and does not intend to penalize Covered Entities for the exercise of honest, good faith judgment." *Frequently Asked Questions Regarding 23 NYCRR Part 500*, N.Y. DEP'T OF FIN. SERVICES, https://www.dfs.ny.gov/about/cybersecurity_faqs.htm (last updated Mar. 23, 2018) [https://perma.cc/4CDY-3SQ4].

163. Additionally, we only discuss existing authorities, but note that learning from near misses does not fall cleanly into established policy battles, and it may represent a rare opportunity for bi-partisan cooperation.

Which regulatory agencies would want to see such a program flourish, and secondarily, have clear authority to fund or operate such a program? The FAA determined in the 1970s that the ASRS, designed to learn from incidents and near misses, would enhance the safety of the aviation system.[164] In an analogous manner, the FTC can improve cyber for consumer-facing applications, the Department of Homeland Security (DHS) for critical infrastructure, or the SEC for improving disclosure of cybersecurity practices to investors. This structure might also be best housed in a scientific agency such as NIST in an analogous fashion to the ASRS program.

DHS already oversees multiple regimes aimed at improving critical infrastructure cybersecurity information sharing, with a core mission focused on safeguarding and securing cyberspace,[165] and remedying information shortfalls.[166] DHS currently acts as the overseeing agency to the Computer Emergency Response Team (US-CERT), a program which provides protection to federal agencies through intrusion detection and prevention, exchanges critical cybersecurity information, and analyzes emerging cyber threats among other activities.[167] Moreover, President Obama's Executive Order 13636 directed DHS to create the Critical Infrastructure Cyber Community (C3), a public-private partnership led by DHS to facilitate critical infrastructure management using the NIST framework.[168] The Emergency Services Sector (ESS) Information-Sharing Initiative, which coordinates an information sharing and analysis center and stakeholders for effective information dissemination further illustrates DHS's mission.[169] Given this well-developed mission to share, DHS could serve as an excellent home for a CSRS system.

NIST is a respected scientific agency with expertise in cybersecurity, issuing many standards. NIST is probably better than other government agencies from the perspective of multinational companies, but suffered a reputational blow in 2014 for its close collaboration with NSA.[170]

---

164. *ASRS Program Briefing*, AVIATION SAFETY REPORTING SYSTEM (2016), https://asrs.arc.nasa.gov/docs/ASRS_ProgramBriefing2016.pdf [https://perma.cc/K5F4-FKHK].

165. *Our Mission*, DHS, https://www.dhs.gov/our-mission (last visited Mar. 24, 2018) [https://perma.cc/75AL-KJ65].

166. *Information Sharing*, DHS, https://www.dhs.gov/topic/information-sharing (noting that "[r]emedying information shortfalls was a principal recommendation of the 9/11 commission") (last visited Mar. 19, 2018) [https://perma.cc/NKX5-8ZQB].

167. *About Us*, US-CERT, https://www.us-cert.gov/about-us (last visited Mar. 19, 2018) [https://perma.cc/SZM8-AS2B].

168. *Using the Cybersecurity Framework*, DHS (July 14, 2017), https://www.dhs.gov/using-cybersecurity-framework [https://perma.cc/48AV-HBHX].

169. *Emergency Services Sector Information – Sharing Initiative*, DHS (June 20, 2017) https://www.dhs.gov/emergency-services-sector-information-sharing-initiative [https://perma.cc/65AJ-MRTU].

170. *See, e.g.*, Susan Landau, *On NSA's Subversion of NIST's Algorithm*, LAWFARE (July 25, 2014, 2:00 PM), https://lawfareblog.com/nsas-subversion-nists-algorithm ("Of all the revelations from the Snowden leaks, I find the NSA's subversion of the National Institute of

The funding question is complex; there are single funder models, and multi-funder models. There are a number of agencies, including DHS, FTC, and NIST who have a direct and broad interest in the sorts of guidance a CSRS could offer. Funding does not need to be dramatic. The likely initial size and funding of an experiment tilt towards a single funder. It could well make sense to host it within a Federally Funded Research and Development Center (FFRDC) within non-profits such as MITRE, SRI or RAND, which currently operate FFRDCs and have a reputation for scientific and operational excellence. It also makes sense for the organization to be structured in a way that takes advantage of the protections offered to information sharing and analysis organizations[171]

Ultimately, agencies which may bring actions against organizations for breaches will need to either promulgate rules to provide specific protections, or will need to put out memoranda of understanding to give companies notice and comfort as to the expectation of protection from sharing.

The foregoing reasons explain why incident or near-miss reporting is a good idea. We now examine why our proposal—voluntary reporting, along the lines of the aviation safety system—is better than other alternatives.

D. Single Reporting Regime

Assume that we are correct, that near-miss reporting is important. A single repository is superior to multiple ones, for a number of reasons.

One important reason is that the precise information collected will be important. A recent Inspector-General report on information-sharing from the Department of Homeland Security, pursuant to the Cybersecurity Act of 2015,[172] noted this issue in a slightly different context:[173] "By design, Automated Indicator Sharing and Cyber

---

Standards's (NIST) random number generator to be particularly disturbing. [. . .] This has undermined NIST's role in developing security and cryptography standards and is likely to have serious long-term effects on global cybersecurity.") [https://perma.cc/9DS8-8KD8]; Peter Woit, "*The NSA, NIST, and the AMS*, NOT EVEN WRONG (July 21, 2014), http://www.math.columbia.edu/~woit/wordpress/?p=7045 ("One way this goes beyond the now-withdrawn NIST standard is that the committee also looked at other NIST current standards now in wide use, which in at least one other case depend upon a specific choice of elliptic curves made by the NSA, with no explanation provided of how the choice was made. In particular, Rivest recommends changing the ECDSA standard in FIPS186 because of this problem.") [https://perma.cc/F8MW-LFL4].

171. *See* Karp et al., *supra* note 133 (Information Sharing and Analysis Organizations were created by CISA).

172. Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242.

173. In the Cyber Information Sharing and Collection Program (CISCP), analysts are examining submissions directly, while automated indicator sharing (AIS) is strictly automated information. *See* OFFICE OF INSPECTOR-GENERAL, BIENNIAL REPORT ON DHS' IMPLEMENTATION OF THE CYBERSECURITY ACT OF 2015 12 (2017),

Information Sharing and Collection Program feeds have different methods to populate information and therefore exhibit considerable disparity in data quality… This enables the analysts to provide recipients with more contextual information for determining the appropriate course of action to mitigate potential threats against their networks."[174] While it could be argued that having multiple repositories (and hence multiple questionnaires) will result in at least some good ones being developed, that same argument implies that others will be not so good. We believe that it is better to expend effort on a single high-quality site.

A central archive is also more likely to provide the broader view needed in today's environment.[175] With multiple repositories, analysts would need to poll them all to understand what is going on; furthermore, collecting somewhat different data from each site will vastly increase the analytic difficulties,[176] and attackers are unlikely to organize their activities to comport with our organizational battle lines. If some data is unavailable, analysis will be hurt. DHS suffers from precisely this problem because classified and unclassified data items are stored separately.[177]

Finally, we note that the success of this scheme depends on incentivized cooperation, and hence on finding the right balance between trust and desire to receive the benefit. It's likely that investment in trust-building activity, including outreach and ongoing delivery of confidentiality and anonymity will be required. If there are multiple repositories, some are likely to be more trusted than others; the less-trusted ones will likely receive fewer reports and less informative reports.

E. Analytic Regimes

By contrast, there is no *a priori* reason why there cannot be multiple analyses. Indeed, multiple analytic perspectives can be valuable, in that different researchers can take different approaches and derive different insights. The problem, however, is that the collected data may be believed by the organization to be somewhat sensitive.[178] Furthermore, near-miss data is often less sensitive. Had Equifax fended off the attackers, they could have reported "danger of

https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf [https://perma.cc/RJ4E-2FD5].

174. *Id.*

175. *Id.* at 4 ("contextual data [is] needed to effectively defend against ever-evolving threats").

176. *See id.* at 13.

177. *Id.* at 13 ("This separation restricted the analysts' ability to compile a complete situational awareness of a potential threat.").

178. *See supra* Section II (but without experience in collecting near-miss data, it remains to be seen how organizations will see it, once the newness wears off).

a failure of a vulnerability or patch scanner," or the "danger of a large exposure of personal information," as opposed to "data on 145 million people was exposed." The latter is far more revelatory: not many organizations have that much data. There are questions of how the data is gathered and processed, and also, questions of how analyses are released. ASRS and ASIAS both take the approach that data is gathered confidentially, and analysis is released after careful anonymization.

One tempting approach is to gather and release anonymized data—replace identifiers with arbitrary different ones.[179] In general, this approach is unlikely to work well. Apart from the normal risks of anonymization,[180] the data we urge be collected will contain implicit and explicit identifying information, information that is difficult to anonymize or redact.

Some of the issue relates to free-form text fields. These are widely recognized to be a problem; HIPAA, for example, requires that they be anonymized as well.[181] But there is also implicit identifying information in, *e.g.*, a description of the reporter's network topology.[182]

179. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 UCLA L. REV. 1701, 1703 (2010) ("Imagine a database packed with sensitive information about many people . . . . Now imagine that the office that maintains this database needs to place it in long-term storage or disclose it to a third party without compromising the privacy of the people tracked. To eliminate the privacy risk, the office will anonymize the data, consistent with contemporary, ubiquitous data-handling practices. First, it will delete personal identifiers like names and social security numbers. Second, it will modify other categories of information that act like identifiers in the particular context—the hospital will delete the names of next of kin, the school will excise student ID numbers, and the bank will obscure account numbers.").

180. *See* Arvind Narayanan & Vitaly Shmatikov, HOW TO BREAK ANONYMITY OF THE NETFLIX PRIZE DATASET 2 (2008), https://arxiv.org/pdf/cs/0610105v1.pdf ("How much does the attacker need to know about a Netflix subscriber in order to identify her record in the [anonymized] dataset . . . very little.") [https://perma.cc/4P9D-D88M]; Paul Ohm & Scott Peppet, *What if Everything Reveals Everything?*, *in* BIG DATA IS NOT A MONOLITH 4647 (2016) (discussing what the authors believe to be a not-so-distant world where any piece of information reveals all pieces of information).

181. *See* OFFICE OF CIVIL RIGHTS, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE §3.10 (2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf ("The de-identification standard makes no distinction between data entered into standardized fields and information entered as free text (i.e., structured and unstructured text)—an identifier listed in the Safe Harbor standard must be removed regardless of its location in a record if it is recognizable as an identifier.") [https://perma.cc/QQ6A-HADK].

182. Different organizations use different paradigms for organizing their networks. *See, e.g.*, Neil Spring et al., *Measuring ISP Topologies with Rocketfuel*, 32 COMPUTER COMMUN. REV. 133, 137 (2002) ("It is evident that the style of backbone design varies widely between ISPs. Figure 7 shows three sample backbones overlaid on a map of the United States"). While these are in general not public knowledge, it is often possible for knowledgeable individuals to deduce or even measure them. *Id*.

Again, this sort of risk is recognized by the HIPAA anonymization guidance.[183]

Ideally, as much of the information as possible will be in structured form rather than as text; this will permit automated queries, use of machine learning techniques, etc.[184]

To be sure, it may be possible to anonymize a structured subset of reports. Methods of incident data anonymization have been developed.[185] Again, though, de-anonymization is often possible if some extra information is available.[186] It is worth noting that the minimum population size considered adequate for suitable anonymization under HIPAA is 20,000 people;[187] there are not likely to be nearly as many records in any useful time frame.

A third possibility is to use an anonymization technique such as differential privacy.[188] This offers mathematically provable privacy guarantees, but is only suitable for certain sorts of statistical queries; it is not at all useful for analyzing free-text reports.

We conclude from these techniques that release of confidential data is unlikely to balance privacy with performing interesting analyses. The conclusion, then, is that a single agency, and one with sufficient scientific expertise to process the data, should be responsible for all analyses. Fairly obviously, it would be easier if this agency were also the party that collected the data. Outside researchers could, perhaps, be invited in to work with the in-house researchers, but this would have to be done pursuant to suitable non-disclosure agreements and perhaps prepublication review of any resulting papers.[189]

---

183. *See* OFFICE OF CIVIL RIGHTS, *supra* note 181, at §2.6 ("A higher risk 'feature' is one that is found in many places and is publicly available. These are features that could be exploited by anyone who receives the information.").

184. *See, e.g.,* Joe Calandrino, *Government Datasets that Facilitate Innovation*, FREEDOM TO TINKER (Mar. 1, 2010), https://freedom-to-tinker.com/2010/03/01/government-datasets-facilitate-innovation/. *See generally* FREEDOM TO TINKER, https://freedom-to-tinker.com (subsequent articles also supporting this argument) [https://perma.cc/3QA9-CA7P].

185. *See generally, e.g.*, Janak J. Parekh, *Privacy-Preserving Distributed Event Corroboration* (2007) (unpublished Ph.D. dissertation) (on file with Columbia University), http://www.cs.columbia.edu/~janak/research/thesis-20070501.pdf [https://perma.cc/EJ2S-WKFL].

186. *See* Ohm & Peppet, *supra* note 180.

187. *See* OFFICE OF CIVIL RIGHTS, *supra* note 181, at §1.4.

188. *See* Cynthia Dwork, *Differential Privacy: A Survey of Results*, *in* THEORY AND APPLICATIONS OF MODELS OF COMPUTATION 1 (Manindra Agrawal et al. 2008) (commonly cited survey on the subject).

189. Presumably, the classified networks would have their own incident reporting system and repository; as with the DHS effort, the classified and unclassified data would have to be stored separately. *See* OFFICE OF INSPECTOR-GENERAL, *supra* note 173. It might be useful to have a single analytic system that could process both classes of data. OFFICE OF INSPECTOR-GENERAL, *supra* note 173 ("By acquiring a cross-domain solution, DHS can provide more detailed cyber information, improve the quality and usefulness of cyber threat reports, and correlate cyber threat indicators and defensive measures across its unclassified and classified environments.").

F. Light-Touch Cooperation

While a mandatory regulatory scheme might be preferable,[190] such an approach seems unlikely today. Even apart from the current political tensions, there is a profound partisan divide on the desirability and utility of regulations. We are thus suggesting a "light-touch" voluntary scheme. While we do not know for certain that there will be cooperation, we are cautiously optimistic. The same sort of approach has succeeded in aviation and many other fields;[191] we believe that it will help here.

The proof, of course, will be in whether the resulting information actually helps. Based on DHS's results with threat information, we suspect that it will.[192] We also interviewed representatives of selected DHS components and Federal entities—consumers of this information—and found that they generally used this information to improve their network security controls. However, they also used the cyber threat indicators to detect malicious actors, and mitigate anomalies and possible threats to their networks.

The key, of course, will be the published analyses: is enough information disseminated, to the right people, and quickly enough?

CONCLUSION

It is clear that there is a serious cybersecurity problem. While the ultimate solutions will likely have to be technical—neither criminal hackers nor hostile nations will vanish any time soon—today's efforts are hampered by a lack of information. We can augment today's "indicator-centric" information sharing schemes with new types of analysis. A voluntary and incentivized scheme focused on the collection, analysis, and publication of lessons is an important part of how other fields improve their safety and security. The complexity of gathering information about real cyber incidents leads us to suggest an effort focused on near misses. Experience in other fields has shown that trying to bring voluntary reports to regulatory agencies often fails.

Public policy must balance between ensuring the public is protected, while providing sufficient incentives for information gathering, analysis, and publication. On the one hand, companies must be provided with sufficient certainty that their disclosures will not come back to haunt them, but should not be able to avoid liability by virtue of their disclosures.

Against the backdrop of liability for data breaches, the question becomes obvious: how long can we keep saying "that was close!"? Without an effective cybersecurity plan, companies risk increasingly

190. *See* Bellovin, *supra* note 8.
191. *See supra* Section III.A.
192. *See* OFFICE OF INSPECTOR-GENERAL, *supra* note 173.

serious backlash from government and consumers. However, these same companies lack the visibility into ongoing threats which other similarly situated companies may have successfully prevented. As a result, companies make the same mistakes repeatedly and inadvertently subject themselves to massive liability. The development of a near-miss reporting system seeks to alleviate company stress from attackers and threats of liability by incentivizing companies to share what they experience.[193]

A. Industry Should Experiment With Near-Miss Reporting

Industry should take steps to experiment with near-miss reporting. That includes creating working definitions of accident and near miss, crafting forms and databases to hold the input, and experimentally processing them to inform discussion of effort. If a new organization were to stand up to collect data, how much would it get? We could run an experiment to find out.

There has been some work on definitions,[194] but more work with the goal of specifying near misses would help set minds at ease. If industry creates a working definition, that definition could later be adopted into law or incorporated by the information reporting agency to allow for greater clarity in what creates liability for the reporting entity.

B. Regulators Should Reward Reporting of Near Misses

Regulators should create incentives and remove roadblocks to learning from our mistakes[195]. The challenges of securing systems today are obvious, and they will get worse. Initially, this should be incentives for experimentation as needed, with a clear path to building systematic capabilities for securing our society.

193. Organizations may experience events and not have the resources to investigate or analyze it. Expertise is in short supply and strange events are common. Additionally, a single event may happen absent context that a broader scientific agency might be able to see.

194. *See, e.g.*, C. Matthew Curtin & Lee T. Ayres, *Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry*, 4 J. L. & POL'Y FOR THE INFO. SOC'Y 569 (2008).

195. The precise nature of such rewards varies across disciplines. In cybersecurity, it may vary from reduced penalties to significant rewards for well executed reporting of interesting misses. Most important is an incentive which is sufficient to generate a norm of reporting without creating moral hazards.