DEFINING "REASONABLE" CYBERSECURITY: LESSONS FROM THE STATES

*Scott J. Shackelford**
*Anne Boustead***
*Christos Makridis****

25 YALE J.L. & TECH. 86 (2023)

Questions over what constitutes "reasonable" cybersecurity reporting and operating practices have long vexed businesses and policymakers. Given a lack of clear guidance from Congress, states have filled the vacuum by passing a series of laws requiring "reasonable" cybersecurity such as for manufacturers of Internet-connected devices. Other states have elected instead to provide safe harbors, like Ohio, which rewards companies for investing in a pre-determined list of recognized cybersecurity standards and frameworks—such as the National Institute for Standards and Technology (NIST) Cybersecurity Framework—by minimizing liability in the aftermath of a data breach. This Article: (1) summarizes the current state of state-level cybersecurity policymaking with a special emphasis on how states are defining "reasonable" cybersecurity; (2) discloses the results of a statewide survey on cybersecurity perceptions and practices among organizations in Indiana done in partnership with the Indiana Attorney General's Office; and (3) makes a series of suggestions based on these findings about how to better educate and incentivize firms about instituting reasonable cybersecurity best practices.

TABLE OF CONTENTS

I. INTRODUCTION

The expansion of the digital economy has brought sustained increases in productivity, but also new risks and vulnerabilities.[1] However, what constitutes "reasonable" cybersecurity has long vexed both businesses and policymakers. After all, even some of the most sophisticated operators have fallen victim to cyber attacks. Consider the December 2020 breach of the leading cybersecurity firm FireEye, which serves a who's who list of clients around the world and was allegedly breached by Russia's Cozy Bear group.[2] Although the red team attack tools released in the breach were worrisome enough, the full extent of the damage only emerged in the following weeks when it became public that the attackers had gained access through the vendor SolarWinds, which, like FireEye, also had government contracts. The SolarWinds breach ultimately led to revelations of widespread breaches at nine U.S. government agencies and more than 100 firms.[3] The episode underscored the main lesson that any organization can be breached—regardless of the cutting-edge array of cybersecurity best practices that they have deployed or how much they spend—due to vulnerabilities in supply chains that the SolarWinds campaign laid bare.[4] Yet, although cyber

---

*Provost Professor of Business Law and Ethics, Indiana University Kelley School of Business; Executive Director, Ostrom Workshop; Executive Director, Center for Applied Cybersecurity Research.

**Assistant Professor, University of Arizona School of Government and Public Policy.

*** Digital Fellow, Stanford University, and Assistant Research Professor, Arizona State University.

The authors wish to thank Jay Bhatia, Noah Holloway, Eric Spencer, and Allison Strong for their invaluable research support in this project, along with the participants in the 2021 Cybersecurity Law and Policy Scholars Conference, particularly Professor Jeff Kosseff for his invaluable comments and critiques. We also greatly appreciate the anonymous respondents who participated in our survey on behalf of their organizations.

[1] *See Defining and Measuring the Digital Economy*, BEA (Mar. 2018), https://www.bea.gov/research/papers/2018/defining-and-measuring-digital-economy [https://perma.cc/D72P-U6UA].

[2] *See, e.g.*, Lucian Constantin, *FireEye Breach Explained: How Worried Should You Be?*, CSO ONLINE (Dec. 10, 2020), https://www.csoonline.com/article/3600893/fireeye-breach-explained-how-worried-should-you-be.html [https://perma.cc/J6LH-4WN7].

[3] *See, e.g.*, Jeff Stone, *How FireEye Attributed the SolarWinds Hacking Campaign to Russian Spies*, CYBER SCOOP (June 15, 2021), https://www.cyberscoop.com/fireeye-russia-solarwinds-kevin-mandia-postcard [https://perma.cc/XF78-ECH4].

[4] *See SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response,* U.S. GOV'T ACCOUNTABILITY OFFICE (Apr. 22, 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic [https://perma.cc/C6ZX-NC3M]; Jason

risk can never be eliminated, it can be better managed through incentivizing—and even requiring—technical and organizational cybersecurity best practices.[5] There are diverging opinions and approaches, though, across jurisdictions about the best way to balance both rules and standards to enhance overall cybersecurity due diligence.

Given a lack of clear guidance from Congress as to what constitutes "reasonable" cybersecurity outside of certain critical infrastructure contexts such as healthcare and finance,[6] some states have filled the vacuum by passing a series of laws encouraging and requiring companies operating within their jurisdictions to instill reasonable cybersecurity practices such as California's 2020 mandate for manufacturers of Internet-connected devices.[7] Other states, including Ohio, have elected instead to provide safe harbors which reward companies for investing in a pre-determined list of recognized cybersecurity standards and frameworks—such as the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF)—by minimizing liability in the aftermath of a data breach.[8] There are benefits and drawbacks about both approaches, along with others including disclosure and even

---

Choi, *Hit or Myth? Understanding the True Costs and Impact of Cybersecurity Programs*, MCKINSEY (July 17, 2017), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs [https://perma.cc/VUE9-PS8R].

[5] *See, e.g.*, Steve W. Klemash, Jamie C. Smith, & Chuck Seets, *What Companies Are Disclosing About Cyber Risk and Oversight*, HARV. L. SCHOOL F. CORP. GOVERNANCE (Aug. 25, 2020), https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight [https://perma.cc/CM2Y-3KKP] ("Because the threat of a breach cannot be eliminated, some investors stressed that they are particularly interested in resiliency.").

[6] *See* U.S. DEP'T HOMELAND SEC., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, FISCAL YEAR 2017 REPORT TO CONGRESS 2–3 (Apr. 2, 2019), https://www.dhs.gov/sites/default/files/publications/cisa_-_improving_critical_infrastructure_cybersecurity.pdf [https://perma.cc/QZ8N-ZUFP].

[7] CAL. CIV. CODE § 1798.91.04 (West 2022); *see IoT Manufacturers – What You Need to Know About California's IoT Law*, NAT'L L. REV. (Jan. 28, 2020), https://www.natlawreview.com/article/iot-manufacturers-what-you-need-to-know-about-california-s-iot-law [https://perma.cc/RLN5-ANMU] (noting that "[t]he California IoT law requires manufacturers of connected devices to equip the device with a reasonable security feature or features that are all of the following: appropriate to the nature and function of the device; appropriate to the information the device may collect, contain, or transmit; and, designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.").

[8] *See* Michael Kassner, *Ohio Law Creates Cybersecurity 'Safe Harbor' for Businesses*, TECH. REP. (Jan. 3, 2019), https://www.techrepublic.com/article/ohio-law-creates-cybersecurity-safe-harbor-for-businesses [https://perma.cc/73E2-CTKM].

proposed strict liability regimes, that deserve deep analysis as a growing slate of states consider new regulations in this space.[9]

Yet, the literature to date has underappreciated this issue.[10] As such, we argue that—as new state and federal laws are considered—the time is appropriate to see what we can learn from these varied efforts at defining and enforcing "reasonable" cybersecurity to inform policymakers and practitioners alike. Our findings point to the need for an empirically grounded, flexible approach to the problem that combines a minimum (i.e., "common floor") set of standards comprised of widely recognized cybersecurity best practices with sector-specific guidance and an effort to inform consumers of their rights and importance of exercising them.

This Article is structured as follows. Part 1 introduces the multifaceted array of cyber threats facing organizations, and the resulting market failure in cybersecurity that has emerged in the absence of comprehensive federal guidance. Part 2 then summarizes the current status of state-level cybersecurity policymaking with a special emphasis on how states are defining "reasonable" cybersecurity. Part 3 discloses the results of a statewide survey on cybersecurity perceptions and practices organizations in Indiana are interpreting "reasonable" cybersecurity, which was done in partnership with the Indiana Attorney General's Office, the Indiana Business Research Center, and the Indiana Executive Council of Cybersecurity. Finally, Part 4 summarizes the preceding analysis and offers a series of policy suggestions based on these findings about how to better educate and incentivize firms to institute reasonable cybersecurity best practices, and in so doing better protect their networks, intellectual property, employees, customers, and national security.

II. INTRODUCING THE MULTIFACETED CYBER THREAT

Cybersecurity has been elevated as a national security threat and source of geopolitical risk over the past two decades.[11] For

[9] *See* Scott J. Shackelford & Scott O. Brander, *Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything*, 72 HASTINGS L.J. 627 (2021) (discussing various approaches to improving Internet of Things cybersecurity).

[10] Cf. Jeffrey F. Addicott, Impact of Data on Litigation: Enhancing Cybersecurity in the Private Sector by Means of Civil Liability Lawsuits - The Connie Francis Effect, 51 U. RICH. L. REV. 857, 864 (2017) (arguing that the concept of reasonableness with respect to cybersecurity will soon surpass current industry standards).

[11] CHRISTIAN RUHL ET AL., CYBERSPACE AND GEOPOLITICS: ASSESSING GLOBAL CYBERSECURITY NORM PROCESSES AT A CROSSROADS 1 (Feb. 2020), https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf [https://perma.cc/3BZT-DTQB].

example, the incidence of data breaches has been growing over time, more than tripling from 2005 to 2018[12] and costing between $57 billion and $109 billion per year, according to some of the more conservative estimates.[13] Some, however, suggest that the economic and social costs of the various types of cybercrime could be in the trillions,[14] while the global cybersecurity market is projected to grow to more than $340 billion by 2027.[15] Moreover, the threat vectors are heterogeneous, consisting of not only idiosyncratic malicious actors,[16] but also nation states.[17] As the digital economy continues to expand, these risks will continue to grow and require a proper identification of them to develop the right countervailing responses. This task, needless to say, is a tall order, particularly for small and medium sized businesses that are often bearing the brunt of cyber incidents, as is discussed further in Part 4.[18]

A. Dimensions

There are multiple dimensions of cybersecurity risk that influence how to think about "reasonable" cybersecurity measures. First, economic considerations. Malicious attacks cost the economy billions each year, arising from the direct cost on firm reputation or physical equipment and the indirect effects of allocating a portion of their budget towards information security that tends to have no

---

[12] 2019 Econ. Rep. President 363.

[13] THE COUNCIL OF ECON. ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 36 (Feb. 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [https://perma.cc/75QY-9UDB].

[14] *See* Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually By 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 [https://perma.cc/CLS7-CZBG].

[15] *Global Cybersecurity Market Size Worth US$ 346 Bn by the end of 2027| CAGR :13.40% | Astute Analytica*, YAHOO! (Jan. 12, 2022), https://www.yahoo.com/now/global-cybersecurity-market-size-worth-113000824.html [https://perma.cc/XG4H-7MY3].

[16] *See* Juta Gurinaviciute, *5 Biggest Cybersecurity Threats*, SEC. (Feb. 3, 2021), https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats [https://perma.cc/WRF5-U9DR].

[17] Perry Carpenter, *Cybersecurity and Nation-State Threats: What Businesses Need to Know*, FORBES (Apr. 16, 2021, 7:50 AM), https://www.forbes.com/sites/forbesbusinesscouncil/2021/04/16/cybersecurity-and-nation-state-threats-what-businesses-need-to-know [https://perma.cc/5VJ4-RTG5].

[18] *See, e.g.*, Ted Knutson, *Small Businesses Bearing Brunt of Ransomware Attacks, Senate Told*, FORBES (July 27, 2021), https://www.forbes.com/sites/tedknutson/2021/07/27/small-businesses-bearing-brunt-of-ransomware-attacks-senate-told/?sh=66fbd4d49556 [https://perma.cc/HY5V-4U6N]. *See infra* Part 4.

consumer benefit apart from protecting data.[19] That is, information security investments do nothing to deliver greater consumer value by themselves; rather, they simply mitigate the probability of future harm against the organization.[20]

One of the ways that organizations are exposed to cyber risk and incur economic costs is through their supply chains. Even when an organization insulates itself against risk, a breach to a vendor that has access to their network can create a ripple effect.[21] Recent empirical work suggests that accounting for these supply chain linkages makes the professional services sector the highest risk with the most vulnerabilities, which is intuitive since nearly every other sector depends on professional services, whether for software services or consulting.[22] These inter-sectoral linkages exacerbate the underinvestment in cybersecurity since no single organization fully internalizes the aggregate costs of these attacks.[23] Moreover, as we will discuss later, the varying degrees of inter-sectoral linkages is one reason that we suggest a combination of a common floor of best practices coupled with additional sector-specific guidance.

Second, social considerations. While there are admittedly technological vulnerabilities and issues at play, there is also a dimension of consumer psychology that is present in cybersecurity.[24] For example, a consumer that clicks on a phishing email and opens their computer up to malware makes an incorrect judgment call that, as recent breaches make clear, is difficult to

---

[19] *See* Samantha Schwartz, *Security Accounts for Just 5.7% of IT Spend: Gartner*, CYBERSECURITY DIVE (Oct. 28, 2020), https://www.cybersecuritydive.com/news/security-budget-gartner/587911 [https://perma.cc/EXW3-VKM7]; Saryu Nayyar, *Cybersecurity Budgets are Wasted by an Overabundance of Tools*, FORBES (Aug. 10, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/08/10/cybersecurity-budgets-are-wasted-by-an-overabundance-of-tools/?sh=35f97a146e75 [https://perma.cc/4GD5-2Q52].

[20] *See, e.g.*, Matthew Moynahan, *How Not to Waste a Trillion Dollars on Cybersecurity*, FORBES (Nov. 9, 2021), https://www.forbes.com/sites/forbestechcouncil/2018/11/09/how-not-to-waste-a-trillion-dollars-on-cybersecurity/?sh=4377add8df9a [https://perma.cc/5JRA-MEHA].

[21] *See* Brian Thomas, *4 Ways to Minimize the Risk of a Third-Party Data Breach*, BITSIGHT (Nov. 20, 2019), https://www.bitsight.com/blog/4-ways-to-minimize-the-risk-of-a-third-party-data-breach [https://perma.cc/9NYV-68D8].

[22] *See, e.g.*, Christos Makridis & Deven R. Desai, *Identifying Critical Infrastructure in a World with Network Cybersecurity Risk*, 62 JURIMETRICS 173 (2021).

[23] See, e.g., Lawrence A. Gordon et al., Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model, 6 J. INFO. SEC. 24, 25 (2015).

[24] *See* Stephanie Pappas, *The Psychology of Cyberthreats*, 50 MONITOR ON PSYCH. 44 (2019); Lily Hay Newman, *How to Avoid Phishing Emails and Scams*, WIRED (Feb. 16, 2021, 8:00 AM), https://www.wired.com/2017/03/phishing-scams-fool-even-tech-nerds-heres-avoid [https://perma.cc/W7PD-488C].

insulate from impacting the wider organization and ecosystem.[25] Recent empirical research finds that most consumers are inattentive to these threats: countries with greater cyber vulnerabilities do not seem to have consumers that are more worried or concerned about the potential for internet fraud, for example.[26]

One reason behind many of these vulnerabilities and the lack of an intentional market response stems from the lack of salience behind the attacks. Although some of the largest data breaches are associated with declines in the organization's brand and reputation, the average-sized data breach is associated with an increase in brand power driven by an increase in favorability towards the brand.[27] However, data breaches among firms in consumer-centered sectors are associated with declines in brand trust.[28] These patterns suggest that average-sized malicious attacks against organizations may simply raise the profile of the company in consumers' minds unless consumers interact with them frequently.[29]

Third, geopolitical considerations. Cybersecurity attracts not only idiosyncratic criminals, but also nation states. For example, the WannaCry ransomware attack that took place in May 2017 spread through Microsoft Windows and held users' files hostage, demanding a Bitcoin ransom in exchange for ownership back.[30] While Microsoft had released a patch to their system that protected users against the system exploit, many consumers and organizations do not regularly update their operating system, leaving their systems exposed. In the end, the ransomware attack affected roughly 230,000 computers globally, costing an estimated $4 billion in losses. While the origins of the attack are not fully known, the United States and United Kingdom generally attribute it to North Korea.[31] The prevalence of nation-state sponsored cyber attacks is deeply related to reasonable cybersecurity standards given that deterring such sophisticated cyber attacks requires defense-in-depth

---

[25] Newman, *id.*

[26] *See, e.g.*, AJ Grotto & Christos Makridis, *Perception of Digital Risks: Evidence from 54 Countries*, SSRN (Dec. 8, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3711862 [https://perma.cc/X46H-N39Q].

[27] See Christos A. Makridis, Do Data Breaches Damage Reputation? Evidence from 43 Companies Between 2002 and 2018, 7 J. CYBERSECURITY (2021).

[28] *Id*.

[29] See id.

[30] *What is WannaCry Ransomware?*, KASPERSKY, https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry [https://perma.cc/6YRQ-HBND] (last visited Aug. 15, 2021).

[31] *Cyber-Attack: US and UK Blame North Korea for WannaCry*, BBC (Dec. 19, 2017), https://www.bbc.com/news/world-us-canada-42407488 [https://perma.cc/6YRG-ZERF].

as part of a deterrence-by-denial strategy discussed below, which goes beyond basic cyber hygiene.

Fourth, legal considerations. One of the primary reasons deterrence is so difficult within the cybersecurity landscape stems from the difficulty of attribution. That is, identifying the culprit of an attack, especially in real time, is both technologically and legally challenging.[32] Malicious attackers tend to obscure their true location, allowing them to mask their identity and sometimes even misattribute the blame. Moreover, because vulnerabilities often are present in a system well in advance, malicious attackers can dwell in the network without being noticed. That being said, important progress has been made that is making it possible to attribute cyber attacks with previously unimagined accuracy back to specific organizations and even individuals.[33] Yet under international law, it is difficult for a state to be held accountable for an attack unless it can be uniquely attributed to the state.[34] Building consensus on the contours of an effective regime to do just that has proven challenging, though important progress was made in 2021 as a result of both the UN Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) reports.[35]

As we will see, questions of "reasonable" cybersecurity—a hallmark of so-called "deterrence-by-denial"[36] conceptions of cybersecurity—inevitably lead to questions about the role that

---

[32] See Christian Payne & Lorraine Finlay, Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack, 49 GEO. WASH. INT'L L. REV. 535, 536 (2017).

[33] See, e.g., The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, WHITE HOUSE (July 19, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china [https://perma.cc/4AWQ-MWUJ].

[34] *See* William Banks, *Cyber Attribution and State Responsibility*, 97 INT'L L. STUD. 1039, 1071 n.152 (2021) ("To date, however, attributions do not typically call out cyberattacks as international law violations. At most, they characterize cyberattacks as violations of international norms.").

[35] *See* Josh Gold, *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?*, CFR (Mar. 18, 2021), https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what [https://perma.cc/P22M-87VV]; UNITED NATIONS, OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY (Mar. 10, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [https://perma.cc/7SRM-X5AX].

[36] "Deterrence by denial" refers to a cybersecurity strategy that aims to make cyberattacks "less attractive . . . from a cost-benefit calculation by prolonging the engagement and/or utilizing more resources." Ann E. Hammer et al., *Cyber Resilience as a Deterrence Strategy*, SANDIA NAT'L LAB'YS 1, 11 (Sept. 2020), https://www.osti.gov/servlets/purl/1668133 [https://perma.cc/EQ8F-QX3Y].

governments need to play to proactively protect the private and public sectors against cyber-enabled threats and thus ward off market failures.[37] Yet active defense,[38] also known as persistent engagement or defend forward, also has its disadvantages, since it invites other nations to reciprocally target U.S. organizations even in peacetime.[39] We will argue that a combination of a common floor of standards, coupled with greater education and sector-specific guidance, can go a long way towards improving best practices and the mitigation of risk even independent of additional international cyber engagement. In short, there is not a one-sized-fits-all approach to managing the full range of cyber risks facing organizations. "Reasonableness," then, depends on the unique cyber risk exposure experienced by different industries, sectors, and geographic regions, which as has been discussed is driven in turn by larger technological and regulatory trends.

B. Case for a Cybersecurity Market Failure

That cybersecurity threats have been increasing over time, along with the damages suffered by these organizations, begs the question: why has the market not solved the problem, given the obvious demand for a solution? Unfortunately, market imperfections exist in cybersecurity for at least two reasons.[40] First, cyber attacks are not always immediately visible and attribution is challenging even over time.[41] If organizations are not always able to detect an attack, then imperfect information leads to a deterioration of incentives within organizations. For example, managers are more likely to focus on short-run quarterly earnings targets than invest in long-term cybersecurity infrastructure in an organization, especially

---

[37] *See, e.g.*, David S. Levine, *School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 WASH. & LEE L. REV. ONLINE 323, 338 (2015) ("Perhaps it is time for Congress to focus more on the question of what responsibility U.S. industry has to engage in self-help, and less on the tricks that it has to ignominiously face. It may be time to take 'reasonable efforts' more seriously, or redefine its meaning in a cybersecurity context. Perhaps we should consider adopting a more robust and specific 'reasonable cybersecurity.'").

[38] "Active defense" refers to a range of activities where entities that are likely to be the target of cyberattacks engage in affirmative, offensive steps to prevent such an attack from occurring, or to identify (and potentially punish) those who engage in such an attack. For further discussion of active defense, *see* Scott J. Shackelford et al., *Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking*, 41 UNIV. PENN. J. INT'L L. 377, 383-88 (2020).

[39] *See id.* at 399-400.

[40] *See* Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610–613 (2006).

[41] *See* Rhea Siers, *The Cyber Attribution Challenge*, CIPHER BRIEF (Nov. 26, 2015), https://www.thecipherbrief.com/the-cyber-attribution-challenge [https://perma.cc/3NAQ-M8GY].

if detecting these threats is challenging. Second, cyber attacks have spillovers, or "negative externalities" on other firms, particularly in interconnected supply chains.[42] Absent collective action, that mutes the effectiveness of counters to potential attacks from any individual organization.

These limitations within organizations are compounded by the lack of attentiveness and information among consumers.[43] Since consumer ownership of their own data varies a good deal from state to state as is explored in Part 2, they lack incentives to care as much about what happens to it, especially since there is so little understanding and awareness over the ramifications and implications of data breaches.[44] For example, some estimates suggest that the average person's data is worth less than a dollar.[45] If consumers do not understand what they are giving up when they release information to businesses they buy from, and they do not demand greater security of their data, then companies will not face competitive pressure to implement more robust cybersecurity measures.

C. Absence of Federal Guidance

Given the absence of a fully functioning market for information security, there is an important role for public policy. However, leadership has often been lacking, relegated to lip service rather than concrete action and institutional change. For example, in a 2018 report, the Office of Management and Budget and the Department of Homeland Security found that seventy-one of the ninety-six federal agencies that were surveyed had cybersecurity programs that were either "at risk," or "high risk."[46] Moreover, 38% of the federal cyber incidents that were reported in 2018 did not even identify an attack vector and only 49% of the agencies have the

---

[42] Anderson & Moore, *supra* note 40, at 612-13.

[43] Frank Konkel, *Survey: Most Americans Don't Worry About Cybersecurity Despite Increased Attacks*, NEXTGOV (June 23, 2022), https://www.nextgov.com/cybersecurity/2020/06/survey-most-americans-dont-worry-about-cybersecurity-despite-increased-attacks/166373 [https://perma.cc/CGH9-AMHS]. *But see* Mary Madden & Lee Rainie, *American's Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance [https://perma.cc/2QQJ-RYRH] ("The surveys find that Americans feel privacy is important in their daily lives in a number of essential ways.").

[44] Frank Konkel, Id.; see infra Part 2.

[45] *See, e.g.*, Emily Steel et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth [https://perma.cc/XRT7-8JPJ].

[46] Off. of Mgmt. and Budget, Federal Cybersecurity Risk Determination Report and Action Plan 3 (2018).

ability to detect whether software pre-approved as safe is running on their systems.[47] An even smaller share of 27% of federal agencies report having the ability to detect and investigate attempts to access large volumes of data and only 16% achieved the government-wide target of encrypting inactive data.[48]

Responsibility for cybersecurity is parsed out among an array of federal government agencies, and public-sector partnerships. These include the National Institute for Standards and Technology (NIST), which have developed an assortment of influential cybersecurity, privacy, and supply chain frameworks.[49] The Cybersecurity and Infrastructure Security Agency (CISA) at DHS has become an important player in protecting the U.S.'s sixteen critical infrastructure sectors, which includes elections and as of 2022 enjoys new authority to track ransomware rates.[50] U.S. Cyber Command centered at Fort Meade has become an epicenter for both offensive and defensive military cyber operations supporting U.S. cyber doctrine, though in practice the line between it and DHS's mandate on issues like safeguarding the grid from foreign nation state cyber attacks has been blurry. The National Cyber Director's Office at the White House serves an important coordinating role between these agencies as "principal advisor to the President on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders."[51]

In part because of ongoing turf wars, the Federal Trade Commission (FTC) has emerged as the "de facto" authority on privacy protection.[52] For example, in 1999, Congress gave the FTC the authority to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information" and "protect

---

[47] *Id.* at 6, 14.

[48] *Id.* at 15, 18; Suzette Kent, *Release of the Federal Cybersecurity Risk Determination Report and Action Plan to the President of the United States*, CIO.GOV (May 30, 2018), https://www.cio.gov/2018/05/30/Risk-Report [https://perma.cc/C35N-ZF2H].

[49] *See, e.g.*, Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U. OF CAL. DAVIS BUS. L. J. 217 (2016).

[50] *Critical Infrastructure Sectors*, CYBERSECURITY AND INFRASTRUCTURE AGENCY, https://www.cisa.gov/critical-infrastructure-sectors [https://perma.cc/QS5Y-BJLW]; *see* Scott Shackelford et al., *Making Democracy Harder to Hack*, 50 U. MICH. J.L. REFORM 629 (2017).

[51] OFFICE OF THE NATIONAL CYBER DIRECTOR, https://www.whitehouse.gov/oncd [https://perma.cc/H8X8-S52N] (last visited Sept. 15, 2022).

[52] *See* Steven Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 109 (2000).

against unauthorized access."[53] Moreover, the FTC later received enforcement authority against companies that do not comply with the Safe Harbor Agreement between the U.S. and European Union.[54] Although the legal framework in the U.S. generally favors self-regulation towards privacy and cybersecurity questions, the FTC is able to prompt companies into action through deterrence—that is, encouraging compliance by signaling the potential for an audit, which is expensive and time consuming.[55]

Starting with a 2002 case against Microsoft and its Passport and Passport Wallet services where the FTC said that Microsoft failed to use "sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information,"[56] the FTC adopted a Decision and Order (D&O) that ordered Microsoft to "not misrepresent" its security practices and to "establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[57]

It is worth noting, too, that the FTC has taken strides in implementing its "Safeguards Rule,"[58] which requires financial institutions to establish "reasonable" cybersecurity measures. In brief, the Safeguards Rule, which is propagated under the Gramm-

---

[53] 15 U.S.C. §§ 6801 (2018); *see* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014).

[54] The Safe Harbor Agreement between the U.S. and European Union created a framework to allow companies to transfer data to and from the EU in compliance with EU data protection directives, provided that they certified their compliance with a set of data management principles. *See Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks*, FTC, https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor [https://perma.cc/CC4Y-JXU5] (last visited Sept. 1, 2021).

[55] *See* Solove & Hartzog, *supra* note 53, at 606.

[56] Complaint at 2, In re Microsoft Corporation, F.T.C. No. C-4069 (Dec 20, 2002), https://www.ftc.gov/sites/default/files/documents/cases/2002/12/microsoftcmp.pdf [https://perma.cc/7CXK-3VGB].

[57] Decision and Order at 2, In re Microsoft Corporation, F.T.C. No. C-4069 (Dec 20, 2002), https://www.ftc.gov/sites/default/files/documents/cases/2002/12/microsoftdecision.pdf [https://perma.cc/FW8P-TMEZ]; *see also* Randy Milch & Sam Bieler, *A New Decade and New Cybersecurity Orders at the FTC*, LAWFARE (Jan. 29, 2020), https://www.lawfareblog.com/new-decade-and-new-cybersecurity-orders-ftc [https://perma.cc/AUB6-HHN7].

[58] James Eastman, Avoiding Cyber-Pearl Harbor: Evaluating Government Efforts to Encourage Private Sector Critical Infrastructure Cybersecurity Improvements, 18 COLUM. SCI. & TECH. L. REV. 515, 533 (2017) (addressing the FTC's implementation and enforcement of the "Safeguard Rule" which requires financial institutions to establish "reasonable" cybersecurity measures).

Leach-Bliley Act, requires particular agencies to establish safeguards for financial institutes, including to "ensure the security and confidentiality of customer records," to guard against "anticipated threats or hazards," and to "protect against unauthorized access."[59] It also requires that firms "develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards."[60] Since its enactment in 2002, the FTC has filed a variety of complaints against businesses for failing to implement "reasonable" cybersecurity policies, as seen in settlement orders including Trendnet[61] and LabMD.[62]

In light of the historical record, what is "reasonable" cybersecurity according to the FTC? Although the FTC never stated an explicit definition, they implied that reasonably designed programs are ones that (1) "contain[s] administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers"[63] and that the program must have a designated employee to "coordinate and be accountable" for the program, (2) identify "material internal and external security risks" through a risk assessment process, (3) design and implement safeguards and monitoring processes to control identified risks, and (4) evaluate and adjust the program in light of the required testing and monitoring requirements.[64]

The FTC's power to regulate "reasonable" cybersecurity stems from its authority under Section 5 of the Federal Trade Commission Act to protect consumers from "unfair or deceptive

---

[59] *Id.* (quoting 15 U.S.C. § 6801(b) (2018)).

[60] Standards for Safeguarding Customer Information, 16 CFR § 314 (2020).

[61] Decision and Order, In re Trendnet, Inc., F.T.C. No. C-4426 (Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf [https://perma.cc/5ZWL-2K79] (ordering respondent corporation to implement reasonable cybersecurity safeguards).

[62] Final Order, In re LabMD, F.T.C. No. 9357 (July 29, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmdorder.pdf [https://perma.cc/9GVH-NLHZ] (ordering respondent corporation to implement reasonable cybersecurity safeguards). Following new guidance in 2007 through the Guidance Software D&O, a fifth requirement was added that requests companies demonstrate the "development and use of reasonable steps to retain and monitor service providers capable of appropriately safeguarding personal information," which helped align broader requirements with those that were imposed on financial services following the Gramm-Leach-Bliley Act in 2003. Milch & Bieler, *supra* note 57.

[63] Final Order, *supra* note 62, at 2.

[64] *See id.* at 2-3.

acts or practices."[65] As has been discussed, the FTC has engaged in enforcement actions targeting firms that exhibit unreasonable cybersecurity practices. These efforts were upheld in 2015 in *F.T.C. v. Wyndham Worldwide Corp* ,[66] at which point unreasonable cybersecurity became equated with unfair competition. This case, along with the more than fifty other such cybersecurity settlement orders, provide invaluable guidance to firms on what constitutes "reasonable" cybersecurity under Part 5.

Yet this broad power to define "reasonable" cybersecurity was called into question following the 2018 *LabMD Inc. v. Federal Trade Commission* case,[67] in which the Eleventh Circuit required the FTC to be more specific in its required cybersecurity standards such as by tying it to a sector-specific law such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[68] Here, the Eleventh Circuit declined to address whether or not the use of a reasonability argument in a negligence tort would have been sufficient in this case to justify the FTC's intervention and settlement order,[69] though regardless a negligence cause of action in state court would remain open to victims (pending challenges such as the economic loss doctrine), [70] along with state-level relief, as is discussed in Part 2. This case marked a change in terminology used

---

[65] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/EB73-NRCT] (last visited Nov. 11, 2020) (quoting 15 U.S.C. § 45(a)(1) (2018)).

[66] Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015). Here, the FTC alleged that, "at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." *Id*. The FTC based its reasoning on a failure to use "readily available security measures"—such as firewalls—to "limit access between [the] hotels' property management systems, . . . corporate network, and the Internet*"* along with Wyndham's practice of storing payment card data in clear text, its lack of password security, and failure to police third-party vendors, among other lapses. *Id*. at 240-41.

[67] *See* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018).

[68] *Id.* at 1224.

[69] The FTC argued that "its enforcement action was grounded in the common law of negligence because LabMD unintentionally allowed the invasion of its customers' privacy." Alison Frankel, *There's a Big Problem for the FTC Lurking in 11th Circuit's LabMD Data-Security Ruling*, REUTERS (June 27, 2018, 4:39 PM), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2 [https://perma.cc/FYP9-2B9M].

[70] See, e.g., David W. Opderbeck, Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry, 75 MD. L. REV. 935, 936–38 (2016).

by the FTC from a standard based on "reasonability" to one focusing on cybersecurity "at a minimum."[71]

Unfortunately, "at a minimum" is often equally vague and puts courts in a difficult position of arbitrating the details of technically complex cases about what constitutes "reasonable" cybersecurity practices.[72] While some evolution in the definition is natural, given the changing nature of cybersecurity threats and varying technological capabilities, converging towards a set of reasonable cybersecurity practices that are more concrete and verifiable is important for the FTC and the marketplace at large: absent predictability, companies will underinvest and seek to evade guidance and the FTC and other rulemaking authorities will be unable to enforce a moving target. Still, investigators have been more active in penalizing firms for not taking reasonable steps to ensure the cybersecurity of their networks, such as the $5 billion 2021 FTC fine[73] against Facebook, or the $30 million fine against Robinhood Crypto from New York.[74] In all, there seems to be a growing willingness on the part of regulators and policymakers to make firms liable for lax cybersecurity practices, though defining that threshold has remained challenging.

Along with the FTC, there is also an important case to be made for the NIST Cybersecurity Framework v1.1 being a useful datapoint in establishing a standard of cybersecurity care, including questions of "reasonableness."[75] The success of the original NIST CSF, as is discussed further in Part 2 in the context of state-level safe harbor laws, has led to a proliferation of new NIST-sponsored cybersecurity, privacy, and supply chain frameworks; so many, in fact, that there is a growing backlash on the part of some groups.[76]

---

[71] Milch & Bieler, *supra* note 57.

[72] *Id*.

[73] Leah Nylen, *Facebook Paid Billions Extra to the FTC to Spare Zuckerberg in Data Suit, Shareholders Allege*, POLITICO (Sept. 21, 2021), https://www.politico.com/news/2021/09/21/facebook-paid-billions-extra-to-the-ftc-to-spare-zuckerberg-in-data-suit-shareholders-allege-513456 [https://perma.cc/25C3-2R7Z].

[74] *Robinhood Crypto Fined $30M (€29.4M) for 'Significant Failures' in AML & Cybersecurity*, AML INTELLIGENCE (Aug. 3, 2022), https://www.amlintelligence.com/2022/08/robinhood-crypto-fined-30m-for-significant-failures-in-aml [https://perma.cc/EU9Z-N8VU].

[75] See Gabriella C. Ferraro, Data Breaches Should Not be a Virtual Certainty: Adopting the NIST Standard for Cybernegligence, 59 WASHBURN L.J. 489, 490 (2020); Scott J. Shackelford et al., Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices, 50 TEX. INT'L L.J. 305, 342 (2015).

[76] Frank Ready, *A New NIST Cybersecurity Framework Could Be One Too Many for Software Developers,* LAW.COM (Aug. 31, 2021), https://www.law.com/legaltechnews/2021/08/31/a-new-nist-cybersecurity-

The result of this patchy approach to federal cybersecurity oversight has led to calls for reform. There has been no shortage of candidates, or attempts over the years. For example, the 2018 Data Breach Protection and Compensation Act would have established an Office of Cybersecurity at the FTC, which would supervise cybersecurity practices including at credit reporting agencies including by establishing a ten-day data breach notification window (responding to the Equifax hack discussed in Part 3).[77] Other potential solutions include standing up a federal incentive-based cybersecurity safe harbor regime, as is discussed further in Parts 2 and 3, creating a National Fund for Identity Theft modeled on the Worker's Compensation fund to take advantage of economies of scale and correct for market imperfections (and failures).[78] Most of the actual experimentation, though, has been done at the state level, which is the domain we turn to next.

First, though, in thinking through the current state of "reasonable" cybersecurity definitions, it is helpful to consider how the topic is being treated across related contexts, and by using analogies. This section briefly reviews this issue, including related federal and state case law.

D. How "Reasonable" is Defined

The notion of defining "reasonability" has received an inordinate amount of attention in legal literature, much of which is beyond the scope of this Article.[79] In many cases, such as the Fourth Amendment context, it has been determined that "[t]he test of reasonableness . . . is not capable of precise definition or mechanical application."[80] And for many, it has a normative dimension, being associated with "the right and the good" of a given action.[81]

---

framework-could-be-one-too-many-for-software-developers [https://perma.cc/UR7J-PFY4].

[77] Matthew S. Smith, *Companies are Sorry about Security Flaws. Just not Sorry Enough to Change*, DIGITAL TRENDS (Feb. 9, 2018), https://www.digitaltrends.com/computing/companies-responsible-for-security-breaches [https://perma.cc/HN9B-AS44] .

[78] See Max Meglio, Embracing Insecurity: Harm Reduction Through A No-Fault Approach to Consumer Data Breach Litigation, 61 B.C. L. REV. 1223, 1223 (2020).

[79] *See, e.g.*, Robert Alexy, *The Reasonableness of Law*, *in* REASONABLENESS AND LAW 5, 8 (Giorgio Bongiovanni, Giovanni Sartor, & Chiara Valentini eds., 2009) ("In order to acquire a complete concept of rationality, that is reasonableness, three kinds of requirements have to be added: (1) those that concern coherence, (2) those that concern the interpretation and criticism of interests, and (3) those that give expression to the idea of generalizability or impartiality.").

[80] Joseph L. Hoffmann & William J. Stuntz, Defining Crimes 873 (2021).

[81] *See* Alexy, *supra* note 79, at 6.

Regarding cybersecurity debates in particular, there is a growing literature on defining "reasonableness," such as with regards to the protection of trade secrets. John Villasenor, for example, has argued that the "first" and most "obvious" way to address trade secret cyberespionage is for companies to take "all reasonable steps to minimize the ability of cyber-intruders to get into their systems and make off with their trade secrets[ ]").[82] His recommendations include an array of cybersecurity best practices, including network segmentation,[83] considering cybersecurity throughout the product and service development process, and for trade secrets in particular not over-relying on non-disclosure agreements (NDAs).[84] David Levine has made similar arguments in the context of the reasonable effort standards in trade secrets law,[85] while also making the larger point that such secrecy can conflict with "the methods and purpose of transparent and accountable democratic governance."[86]

Several commentators, including Daniel Shinkle, have similarly investigated the raft of state-level cybersecurity laws relating to reasonability that were explored in Part 2. For example, he argues that the Ohio Safe Harbor Law could well serve as a "bellwether" and experiment that other states and the federal government, will likely look to as they consider their own reforms.[87] Such a menu of options can be useful for at-risk organizations, particularly small businesses that have borne the brunt of many cyber attacks as seen in Part 4, given that they are often more vulnerable due to a lack of resources and know-how.[88] Yet across many states, especially those without a safe harbor law in place, the standard remains one of reasonability. As Loren Selznick and Carolyn LaMacchia note with regards to how courts are weighing

---

[82] John Villasenor, *Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur* (Hoover Inst. Working Grp. on Intellectual Prop., Innovation, and Prosperity, Working Paper No. 14012, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2488756 [https://perma.cc/7LRS-3BTA].

[83] Network segmentation is the process of putting sensitive information on separate sub-networks within a computer network, so that if one sub-network is breached all sensitive information would not simultaneously be exposed. *Id.* at 17.

[84] *Id*.

[85] See David S. Levine, *School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation,* 72 WASH. & LEE L. REV. ONLINE 323, 324 (2015).

[86] David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure,* 59 FLA. L. REV. 135, 138 (2007)

[87] Daniel Shinkle*, The Ohio Data Protection Act: An Analysis of the Ohio Cybersecurity Safe Harbor,* 87 U. CIN. L. REV. 1213, 1235 (2019).

[88] *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?*, 13 J. BUS. & TECH. L. 217, 247-49 (2018) (addressing liability risks to small businesses that did not implement reasonable cybersecurity measures).

whether "reasonable" data security was demonstrated: "Courts generally take into account the financial resources of the business in determining what is reasonable[, but] [t]he law should also take into account the technological expertise and education of the small business owner."[89] It is worth noting, though, that law firms of all sizes are also frequently in the crosshairs, and have similarly struggled to implement cybersecurity policies for their clients that demonstrate "reasonable efforts" to protect their confidential information, potentially including trade secrets.[90] In fact, the argument has been made that lawyers and law firms have an ethical obligation to create a reasonable "security-aware culture" that goes beyond what the law requires, in keeping with their fiduciary responsibilities to their clients.[91]

Indeed, there is a movement as will be analyzed further in Part 2 toward a standards-based approach to defining "reasonability" in the cybersecurity context, led in part by the FTC in the aftermath of the *Wyndham* case.[92] Such specificity is welcome by both courts and practitioners, in many ways, given that, as has been argued by Vince Vela, the line between reasonable and unreasonable is often blurry at best: "the threshold between reasonable and unreasonable cybersecurity measures can be anywhere from a simple encryption method to a limited data access point from specific personnel only."[93] Such a moving target, continually shifting with the technological and regulatory tides, has put state and federal courts in a challenging position.

III. SUMMARY OF STATE-LEVEL CYBERSECURITY LAWS

U.S. states have become active laboratories for cybersecurity policymaking in the absence of federal leadership on the topic in areas including data disposal, data breach notification, and data security.[94] According to the National Conference of State

---

[89] *Id*. at 253.

[90] See Eli Wald, Cyberwars: Navigating Responsibilities for the Public and Private Sector: Legal Ethics' Next Frontier: Lawyers and Cybersecurity, 19 CHAP. L. REV. 501, 502 (2016).

[91] Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data,* 38 AM. J. TRIAL ADVOC. 549, 550 (2015).

[92] Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 426 (2016).

[93] Vince Vela, *Doctoring Up Cybersecurity Standards: A Solution to Adequate Internet Security Measures Post* Wyndham, 3 TEX. A&M J. PROP. L. 243, 261 (2016).

[94] *See* Rodika Tollefson, *Which States Have the Toughest Privacy Laws?*, INFOSEC INST. (May 20, 2019), https://resources.infosecinstitute.com/topic/which-states-have-toughest-privacy-laws/#gref [https://perma.cc/9JY4-4J2D].

Legislatures (NCSL), in 2019, 43 states and Puerto Rico considered nearly 300 bills or resolutions that dealt significantly with cybersecurity.[95] Of those states, 31 have enacted legislation.[96] These figures mark a significant rise from 2015 when only 26 states considered resolutions, with just 8 states enacting new cybersecurity laws.[97] This situation is especially confusing to firms that have customers, and process data from individuals of multiple states, requiring them to follow often confusing, and sometimes conflicting, cybersecurity laws.[98] This section investigates a subset of these efforts, beginning with California and other Western states, before proceeding through the Midwest, to the Atlantic coast, as is illustrated in Figure 1. These groupings are not intended to be thematically significant since, as shown in Figure 1 there are clusters of cybersecurity policy experimentation occurring nationwide, but are merely intended as an overall survey of recent efforts.

In brief, though, there is a general trend across many states to require firms to implement "reasonable" cybersecurity best practices without clearly defining what those entail.[99] Some laws, though, are more specific—including New York and Ohio's cybersecurity laws—and we discuss these more thoroughly below.

---

[95] *Cybersecurity Legislation 2019*, NCSL (Jan. 10, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx [https://perma.cc/5HWE-5KS8].

[96] *Id. Cf*. JEFF KOSSEFF, CYBERSECURITY LAW 48 (2d ed. 2019) ("As of early 2019, more than 20 states have enacted statues that impose data security requirements on companies that own or process personal information from the states' residents.").

[97] *Cybersecurity Legislation 2015*, NCSL (Dec. 31, 2015), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2015.aspx [https://perma.cc/Z97T-LX4J].

[98] *See* KOSSEFF, *supra* note 96, at 392-433.

[99] *See id*. at 62 (noting that this is the case across Arkansas, California, Connecticut, Florida, Indiana, Maryland, Texas, and Utah).

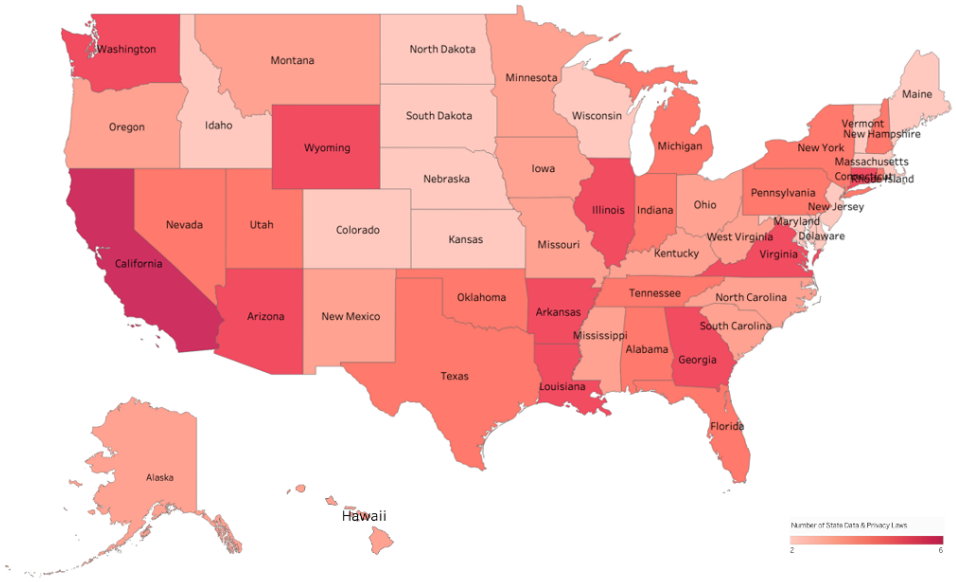


Figure 1: State-Level Cybersecurity Laws (2020)

A. California

California has long been a pioneer in both cybersecurity and data privacy legislation. In 2002, for example, California became the first state to enact a data security breach notification law, S. B. 1386, that went into effect in July 2003.[100]

This law required that any agency that owns or licenses data that includes personal information of California residents to provide, in writing or electronically, notification in the event their unencrypted information has been compromised.[101] At the end of June 2018, just weeks after Alabama became the final state to enact a data breach notification law[102] California passed groundbreaking

---

[100] *See, e.g.*, Gordon Bass, *Case Study: One Company's Response to the California Identity Theft Law*, SANS INST. (Sept. 15, 2003), https://www.sans.org/reading-room/whitepapers/privacy/case-study-companys-response-california-identity-theft-law-1260 [https://perma.cc/U9YM-7H2F].

[101] *See Data Security Breach Reporting*, CAL. DEP'T JUSTICE, https://oag.ca.gov/privacy/databreach/reporting [https://perma.cc/3C9B-V4JP] (last visited June 16, 2021) ("California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Cal. Civil Code § 1798.29(a) [agency], Cal. Civ. Code § 1798.82(a) [person or business].").

[102] *Alabama Becomes Final State to Enact Data Breach Notification Law*, HUNTON ANDREWS KURTH (Apr. 3, 2018), https://www.huntonprivacyblog.com/2018/04/03/alabama-becomes-final-state-enact-data-breach-notification-law [https://perma.cc/Z9QX-HQHH].

legislation with the California Consumer Privacy Act.[103] The law, which went into effect on January 1, 2020, affords California residents more control of their personal information with privacy rights such as the right to notice, the right to access, right to opt out (or opt in), and right to non-discrimination.[104] It is important to note that CCPA "limits the private right of action to only those instances where the underlying business fails to maintain 'reasonable' security."[105] Recent court decisions have also limited the scope of the CCPA's private right of action. In *Gardiner v. Walmart Inc. et al*., a case involving a data breach at Walmart, the court found that in order to have a viable claim for violations of the CCPA, plaintiffs must make specific allegations of unauthorized disclosures of personal information.[106] The court implied that only unauthorized disclosures involving categories of personal information specifically listed in the CCPA would be actionable.[107] Although time will tell the effects of these laws on consumers and innovation, empirical research has found that Internet regulation can have different effects depending on whether the law focuses more on empowering consumers versus enumerating restrictive behavior on firms.[108]

---

[103] *See* California Consumer Privacy Act of 2018, CAL. CIVIL CODE §§ 1798.100–1798.199.100 (West 2021); *One Year of CCPA*, HUNTON ANDREWS KURTH (June 28, 2019), https://www.huntonprivacyblog.com/2019/06/28/one-year-of-ccpa [https://perma.cc/V8EB-A5CX] ("Namely, a consumer has the right, subject to certain exceptions, to (1) request that a covered business provide the consumer with access to and certain details about the personal information collected about her in the preceding 12-month period; (2) request that a covered business delete any personal information about the consumer which the business has collected from the consumer; (3) direct a covered business not to sell the consumer's personal information; and (4) be free from discrimination for exercising individual rights under the CCPA.").

[104] See Data Security Breach Reporting, supra note 103.

[105] Peter Stockburger, *Decoding "Reasonableness" Under California's IoT Law*, DENTONS (Apr. 7, 2021), https://www.dentons.com/en/insights/articles/2021/april/7/decoding-reasonableness-under-californias-iot-law [https://perma.cc/L3S3-YZ9Y].

[106] No. 20-CV-04618-JSW, 2021 WL 2520103, at *2 (N.D. Cal. Mar. 5, 2021); Michael Buchanan et al., *Win for Walmart as District Court Gives Strict Reading to CCPA*, JDSUPRA (Mar. 19, 2021), https://www.jdsupra.com/legalnews/win-for-walmart-as-district-court-gives-9410660 [https://perma.cc/WLA9-U2EY].

[107] *See Spring 2021 Privacy Law Update: CCPA, CPRA, State Laws and Recent Court Decisions*, COBLENTZ PATCH DUFFY & BASS LLP 1, 9 (May 7, 2021), https://www.coblentzlaw.com/news/spring-2021-privacy-law-update-ccpa-cpra-state-laws-and-recent-court-decisions [https://perma.cc/EX23-DKCJ]; Michael Buchanan et al., *supra* note 106.

[108] Anastasia Litina, Christos A. Makridis, & George Tsiachtsiras, *Do Product Market Reforms Raise Innovation? Evidence from Micro-data Across 12 Countries*, TECH. FORECASTING AND SOC. CHANGE 169, 169 (2021).

Later, in September 2018, California enacted the California Internet of Things (IoT) Security Law, which sets a new benchmark for other states to follow. This law requires all connected devices to have "reasonable" security features appropriate to the protection of the device and information it collects.[109] Specifically, as of January 2020, under California Senate Bill 327, "any manufacturer of a device that connects 'directly or indirectly' to the internet must equip it with 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure."[110] Although the law does not define what constitutes "reasonable" cybersecurity in this context, it does note that the security features of internet-connected devices must be: (1) "appropriate to the nature and function of the device; (2) appropriate to the information the device may collect, contain, or transmit; and (3) be designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."[111] Further, "connected devices," which are defined as "any device, or other physical object, that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol or Bluetooth address[,]" exercise "reasonable" security if they either: include a unique, preprogrammed password, or require the user to generate a new means of authentication prior to first use.[112]

Given this lack of clarity on "reasonable" cybersecurity practices in California, in 2016 the California Attorney General's Office did note in reference to the California Records Act that this requirement may be satisfied when, "at a minimum, implementing all the controls that apply to an organization's environment as set forth in the Center for Internet Security's Critical Security Controls ("CIS Controls")."[113] Beyond this security floor, the AG's Office also recommended that organizations make use of other cybersecurity best practices including multi-factor authentication, strong encryption, and encouraging users who may have been impacted by a breach to use fraud alerts to help protect their

---

[109] Cal. Civil Code §§ 1798.91.04 (West 2021).

[110.] Adi Robertson, *California Just Became the First State with an Internet of Things Cybersecurity Law*, VERGE (Sept. 28, 2018, 6:07 PM), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law [https://perma.cc/H7P2-T24K]; *see also* Lindsey O'Donnell, *IoT Security Regulation Is on the Horizon*, THREAT POST (June 6, 2019, 8:44 AM), https://threatpost.com/iot-security-regulation-horizon/145406 [https://perma.cc/4TQB-T448] (noting that the law requires "reasonable security feature or features that are appropriate to the nature and function of the device").

[111] Stockburger, *supra* note 105.

[112] *Id*.

[113] *Id*.

credit.[114] The AG's Office also called for harmonizing divergent state laws, explored below, on this topic. It remains unclear whether or not this definition of "reasonable" security from 2016 jives with California's 2020 IoT cybersecurity law, or whether it will need to be supplemented by other leading standards and frameworks.[115] These could include some combination of the International Standards Organization ("ISO") 27001, the NIST CSF, new draft NIST guidance on IoT Device Cybersecurity Requirements,[116] or sector-specific frameworks.[117]

B. Ripple Effects

What is clear is that there have been important ripple effects from California's efforts to protect consumer privacy, and device security. Yet, as will be seen, these laws vary greatly with regards to defining key terms including "reasonable" security, what actions constitute notification, and who must be notified in the event of a breach.[118] Covered firms in Connecticut, Florida, and New Jersey, for example, must send notifications when there has been unauthorized access to personal information, while entities in states such as Colorado, Delaware, Hawaii, and Kentucky are not required to send notifications if there is not a reasonable likelihood of harm.[119] The majority of states require notification without reasonable delay, with a specific limit written into most state laws. This timeframe can vary widely from thirty days, like in Colorado, to ninety days afforded to entities in Connecticut,[120] although industry best practice seems to be converging on seventy-two hours

---

[114] *Id*.; Jason C. Gavejian, *Reasonable Data Security Defined by California Attorney General*, NAT'L L. REV. (Feb. 24, 2016), https://www.natlawreview.com/article/reasonable-data-security-defined-california-attorney-general [https://perma.cc/ZPJ9-RCPC].

[115] Stockburger, *supra* note 105.

[116] *See* Chad Boutin, *NIST Releases Draft Guidance on Internet of Things Device Cybersecurity*, NIST Press Release (Dec. 15, 2020), https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity [https://perma.cc/MLF9-XMMA].

[117] *Id*. (These include "the Common Security Framework developed by the Health Information Trust Alliance ('HITRUST'), the HIPAA Security Rule, or the U.S. Transportation Services Administration 2011 Pipeline Security Guidelines or the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards.").

[118] Tollefson, *supra* note 94.

[119] *Data Breach Charts*, BAKER HOSTETLER (July 2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf [https://perma.cc/ZR5N-KC59].

[120] *Id*.

thanks to the influence of the EU's General Data Protection Regulation (GDPR).[121]

The scope of personally identifiable information (PII) also varies greatly.[122] Arizona, Colorado, and Delaware, amongst others, have included biometric data in "personal information" while still other states include health information, passport numbers, or login information that would allow access to online accounts.[123] Meanwhile, Hawaii, Maryland, Massachusetts, Mississippi, New Mexico, and Washington introduced bills that focused on limiting the power of companies collecting personal information and provide more control to consumers including in the event of a breach as is illustrated in Figure 2, though these efforts ultimately proved unsuccessful due in part to enforcement issues.[124] Thirteen states as of April 2021 have also adopted the National Association of Insurance Commissioners (NAIC) model data security law, which "requires insurance organizations to have a comprehensive, written security program that is appropriate to the insurer's size and complexity, as well as a written incident response plan, employee training and oversight by the insurer's board of directors, and oversight of third-party service providers through due diligence and security requirements."[125]

---

[121] *See* Luke Irwin, *Data Breach Notification Requirements*, IT GOVERNANCE (Dec. 16, 2019), https://www.itgovernanceusa.com/blog/when-should-an-organization-report-a-data-breach [https://perma.cc/A78R-VNMX].

[122] In general, an individual's first name or first initial and last name with one of more of the following constitutes "personal information": (1) social security number, (2) driver's license number or state issued ID card number, or (3) account number, credit card or debit card number combined with information to access those accounts. *Id*.

[123] *Breach Notification Law Adds Biometrics, Passport Data*, RIPPLESHOT (Oct. 25, 2019), https://www.rippleshot.com/post/breach-notification-law-adds-biometrics-passport-data [https://perma.cc/34GF-AUX5].

[124] *Cybersecurity Legislation 2019*, NAT'L CONF. ST. LEGIS. (Jan. 10, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx [https://perma.cc/6E94-VH28].

[125] *Two More States Adopt NAIC Model Data Security Law*, AKIN GUMP (Apr. 23, 2021), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/two-more-states-adopt-naic-model-data-security-law.html [https://perma.cc/X6A8-2S2K].

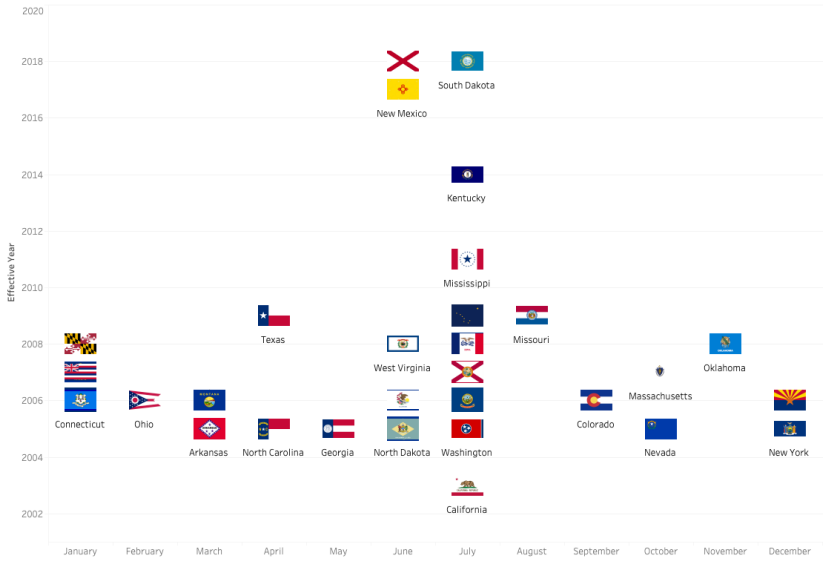


Figure 2: State Breach Notification Laws

C. Nevada

Nevada was successful in passing a law emulating CCPA, but only in part.[126] For example, while Nevada's Internet Privacy Act does provide its residents more control over websites and online services selling their personal information to third parties,[127] unlike CCPA it does not establish a private right to action for consumers.[128] Yet it does require firms "that maintain records containing Nevada residents' personal information to 'implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."[129] It is also unique in requiring firms to encrypt data before transmitting the personally identifiable information of Nevada residents, and protecting the movement of data through storage devices "beyond the logical or physical controls of the data collector."[130] The type of encryption is not specified, but references are made to leading standards-setting bodies including NIST.[131]

---

[126] *See* Alexandra Scott & Lindsey Tonsager, *Nevada's New Consumer Privacy Law Departs Significantly From The California CCPA*, INSIDE PRIVACY (June 10, 2019), https://www.insideprivacy.com/united-states/state-legislatures/nevadas-new-consumer-privacy-law-departs-significantly-from-the-california-ccpa [https://perma.cc/9AHU-VZPM].

[127] *Id.*

[128] *Id.*

[129] KOSSEFF, *supra* note 96, at 51 (citing NEV. REV. STAT. § 603A.215 (2019)).

[130] *Id.* at 52 (citing NEV. REV. STAT. § 603A.210 (2019)).

[131] *Id. at* 96; NEV. REV. STAT. § 603A.215(5)(b) (2021).

D. Oregon

Oregon revised its reasonable cybersecurity law in 2015 and requires firms that "own or possess Oregon customer's personal information to develop and implement reasonable cybersecurity safeguards."[132] Under this regime, "reasonableness" includes an information security plan featuring administrative, technical, and physical safeguards, complying with Gramm-Leach-Bliley[133] or the Health Information Portability and Accountability Act, or another state or federal law with more robust cybersecurity protections than Oregon.[134]

E. Ohio

Progress on state-level cybersecurity policy is certainly not limited to the West, or the coasts. According to the National Conference on State Legislatures, from 2018 to the summer of 2020, state governments of Illinois, Indiana, Iowa, Michigan, Ohio, and Wisconsin considered more than 120 bills related to cybersecurity, with more than twenty-six being eventually enacted.[135] This legislation ranges from a 2018 Iowa law allowing for at least one voting machine examiner to be trained in cybersecurity rather than computer programming and operations to an Ohio law that creates a civilian cyber security reserve force.[136]

In August 2018, Ohio became the first state in the Midwest to enact legislation to incentivize businesses to implement data security standards with the Ohio Data Protection Act (DPA).[137] The Ohio DPA is part of a larger CyberOhio Initiative whose stated goal is "to provide the best legal, technical, collaborative cybersecurity environment possible to help Ohio's businesses thrive and keep

---

[132] *Id.* at 50.

[133] Among other things, the Gramm-Leach-Bliley Act required financial services companies to safeguard their customer information and disclose to their customers how this information was being used. *See* Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497 (2002).

[134] KOSSEFF, *supra* note 96, at 50–51.

[135] *Cybersecurity Legislation*, NAT'L CONF. ST. LEGIS. (Feb. 8, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx [https://perma.cc/MU7B-G2XA].

[136] See id.

[137] *See* Sarah Harvey, *What is the Ohio Data Protection Act?*, KIRKPATRICKPRICE (Nov. 29, 2018), https://kirkpatrickprice.com/blog/what-is-the-ohio-data-protection-act [https://perma.cc/E5ZR-GA8M] .

Ohioans' data and personal information secure."[138] Unlike the New York state SHIELD Act, the Ohio Data Protection Act is voluntary and has clauses for the size and scope of covered entities and is designed to provide an affirmative defense for liability in the wake of a breach.[139] Importantly, Ohio's approach to a cyber safe harbor identifies five schemes that are deemed to be compliant: (1) NIST special publication 800-171, (2) NIST special publications 800-53 and 800-53a, (3) "federal risk and authorization management program (FedRAMP) security assessment framework," (4) "center for internet security critical security controls for effect cyber defense," or (5) "international organization for standardization/international electrotechnical commission 270000 family — information security management systems."[140] To be eligible, a covered entity must "create, maintain, and comply with a written cybersecurity program that "reasonably conforms" with the above-mentioned frameworks, and the entity bears the burden of proving that its program satisfies these requirements.[141]

As we will see, this relatively broad definition of "reasonable" cybersecurity—in contrast to California, for example—provides firms with a range of options for fulfilling their cybersecurity due diligence responsibilities to consumers, and the state.[142]

F. Illinois

In contrast to Ohio, the State of Illinois Cybersecurity Strategy for 2021 to 2025 laid out five strategic goals to help make

---

[138] *CyberOhio*, OHIO.GOV, https://cyber.ohio.gov/wps/portal/gov/cyber [https://web.archive.org/web/20210924084829/https://cyber.ohio.gov/wps/portal/gov/cyber] (last visited June 18, 2021).

[139] OHIO REV. CODE ANN. § 1354.04 (LexisNexis 2018); Daniel Shinkle, *The Ohio Data Protection Act: An Analysis of the Ohio Cybersecurity Safe Harbor*, 87 U. CIN. L. REV. 1213, 1214 (2019); David J. Oberly, *Ohio's Data Protection Act*, OHIO ST. BAR ASSOC. (July 1, 2019), https://www.ohiobar.org/member-tools-benefits/practice-resources/practice-library-search/practice-library/2019-ohio-lawyer/ohios-data-protection-act [https://perma.cc/5V2K-GMSA].

[140] Shinkle, *supra* note 139, at 1219.

[141] *Ohio Enacts Cybersecurity Safe Harbor Law*, ALSTON & BIRD (Sept. 20, 2018), https://www.alstonprivacy.com/ohio-enacts-cybersecurity-safe-harbor-law [https://perma.cc/VZ8T-EHHW].

[142] *See* Matt Scherocman, *The New Ohio Data Protection Act & What it Means for Your Company's Safety*, INTERLINK (Sept. 20, 2020), https://www.interlink.com/blog/entry/ohio-data-protection-act-what-it-means-for-your-company-s-safety [https://perma.cc/475Y-N5MD]; Joanna Grama, *Ohio's 'Data Protection Act' Can Shield Higher Ed Against Breach Lawsuits*, EDSCOOP (Jan. 28, 2019), https://edscoop.com/ohios-data-protection-act-can-shield-higher-ed-against-breach-lawsuits [https://perma.cc/48A5-5FCL].

Illinois become one of the most cyber-secure states in the nation.[143] Illinois relies on public-private partnerships to help meet its cybersecurity goals, which include protecting consumers and encouraging businesses to adopt cybersecurity best practices.[144] It has also adopted two laws—the Personal Information Protection Act (PIPA)[145] and the Biometric Information Privacy Act (BIPA)[146] — which require, among other things, that any company or organization that has suffered a breach with more than 500 Illinois' residents being affected to notify the Attorney General's Office.[147] Further, PIPA requires companies and organizations to implement and maintain "reasonable security measures" to protect data from being compromised.[148] The unique aspect of the PIPA is the inclusion of biometric information in its definition of personal information.[149] BIPA came to national attention after Facebook settled a class action suit with Illinois users after violating BIPA for $550 million.[150]

G. Indiana

Indiana, on the other hand, does not have a state-level law defining "reasonable" cybersecurity for Hoosier firms. What it does have is a suite of executive order and related state laws. Executive Order 17-11, for example, established the Indiana Executive

---

[143] *State of Illinois Cybersecurity Strategy 2021-2025*, ILLINOIS.GOV 1, 3 (2021) https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Documents/CyberSecurity-Strategy-2021-25.pdf [https://web.archive.org/web/20221127164007/https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Documents/CyberSecurity-Strategy-2021-25.pdf] (including these goals: "(1) Build a Culture of Cyber Awareness, (2) Prepare and Plan for Cyber Incidents, (3) Mature Cyber Capabilities, (4) Build a Cyber Workforce, and (5) Collaborate and Share Information").

[144] *Id*.

[145] 815 ILL. COMP. STAT. 530 (2022).

[146] 740 ILL. COMP. STAT. 14 (2022).

[147] *See* Joseph J. Lazzarotti et al., *Illinois Enhances its Data Breach Notification Requirements*, NAT'L L. REV. (Sept. 5, 2019), https://www.natlawreview.com/article/illinois-enhances-its-data-breach-notification-requirements [https://perma.cc/4NDS-R7EZ].

[148] Personal Information Protection Act, 815 ILL. COMP. STAT. 530 / 10(e)(2) (2022).

[149] *Id*. at 530 / 45.

[150] *See Facebook Agrees to Landmark 550 Million Dollar Settlement in BIPA Class Action*, HUNTON ANDREWS KURTH (Jan. 30, 2020), https://www.huntonprivacyblog.com/2020/01/30/facebook-agrees-to-landmark-550-million-dollar-settlement-in-bipa-class-action/#more-18285 [https://perma.cc/RVZ3-FWM7].

Council on Cybersecurity (IECC) on January 9, 2017.[151] The IECC is led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, and is composed of various government (local, state, and federal), private-sector, military, research and academic entities.[152] In September 2018, the IECC delivered the Indiana Cybersecurity Strategic Plan to Governor Holcomb.[153]

Indiana has three main cybersecurity laws that protects its residents from cyber harm—the Security Breach Notification Law,[154] the Anti-DDoS Law,[155] and the Anti-Spyware Law[156]—as well as a proposed but ultimately unsuccessful safe harbor law.[157] Indiana's Security Breach Notification Law includes similar conditions to the general state breach notification laws but fails to contain broader clauses included with other states such as a private right to action. The statute's narrower view of personal information includes breached Social Security Numbers that are unencrypted or redacted or an individual's first name, or first initial, and last name and one of the following (1) driver's license number, (2) state identification card number, (3) a credit card number, or (4) financial account number or debit card number along with information to access that account.[158] Indiana's data breach law requires a person required to make a notification to do so "without unreasonable delay."[159] The standard timeframe among states with a specific clause is 45 days.[160] Violations of the data breach notification law can only be brought against an entity by the Indiana Attorney General, whereas in California, Illinois, and Washington there is a private right to action.[161]

---

[151] Executive Council, Executive Order 17-11, https://www.in.gov/cybersecurity/executive-council [https://perma.cc/SEM4-DY3C] (last visited June 18, 2021).

[152] *Id*.

[153] *See Indiana Cybersecurity Strategic Plan*, INDIANA CYBERSECURITY HUB https://www.in.gov/cybersecurity/executive-council/indiana-cybersecurity-strategic-plan [https://perma.cc/253Y-SKZT] (last visited June 18, 2021).

[154] IND. CODE § 24-4.9-2-2 (2017).

[155] IND. CODE § 35-43-2-3 (2018).

[156] IND. CODE § 24-4.8-2-2 (2017).

[157] *See* Press Release, Indiana Attorney General, AG Curtis Hill Urges Gov. Holcomb to Approve Cybersecurity Rule (Jan. 9, 2021), https://events.in.gov/event/ag_curtis_hill_urges_eric_holcomb_approve_safe_harbor?utm_campaign=widget&utm_medium=widget&utm_source=State+of+Indiana [https://perma.cc/BS93-SCDC].

[158] IND. CODE § 4-1-11 (2018); *see Data Breach Charts*, *supra* note 120.

[159] IND. CODE § 24-4.9-3-3 (2021).

[160] *See Data Breach Charts*, *supra* note 119.

[161] *Id*.

According to the Cisco Annual Internet Report (2018-2023), the total number of DDoS attacks[162] will double from 7.9 million in 2018 to 15.4 million by 2023.[163] In 2017, the average cost from a DDoS attack for small and medium-sized businesses (SMBs) was $120,000.[164] Despite the increasing risk and cost of these attacks, Indiana's anti-DDoS statute punishes offenders at only a Class A misdemeanor level.[165] However, Indiana's Anti-Spyware law provides for civil action of actual damages, or $100,000, whichever is greater.[166]

As of July 8, 2020, the Indiana Attorney General's office issued a notice of intent to adopt a rule to establish a safe harbor standards for a database owner's duty to implement and maintain a data security plan. The plan, as published, would have had Indiana join Ohio in establishing a safe harbor cybersecurity plan, though it would have favored the NIST CSF.[167] However, the effort ultimately fizzled, which makes it a prime case study that we return to in Part 4.

H. Massachusetts

Massachusetts has one of the most robust regimes among the Eastern states for defining and enforcing "reasonable" cybersecurity. It enacted "the most detailed and comprehensive general data security requirements in the United States," according to Professor Jeff Kosseff, which have become "de facto national

---

[162] Distributed denial-of-service—or DDoS—attacks function by bombarding a website or service with a large number of phony requests for information, so that legitimate users cannot access it. DDoS attacks have been behind a number of efforts to disable important services world-wide, including a 2013 attack on Chase Banks. *See* Steven Musil, *Denial-of-Service Attack Takes Down JP Morgan Chase Sites*, CNET (Mar. 12, 2013), https://www.cnet.com/news/privacy/denial-of-service-attack-takes-down-jp-morgan-chase-sites [https://perma.cc/8ZLJ-4NEG].

[163] CISCO ANNUAL INTERNET REPORT (2018-2023) WHITE PAPER (Mar. 9, 2020), https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html [https://perma.cc/7CUK-BRQU].

[164] Dan Kobialka, MSSP Alert (Feb. 25, 2018), https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m [https://perma.cc/RE7V-ALZD] .

[165] IND. CODE § 35-43-2-3(c) (2018).

[166] *See* L. Elizabeth Bowles, *Survey of State Anti-Spyware Legislation*, 63 BUS. LAW. 301, 309 (2007).

[167] *See Indiana Attorney General Proposes Safe Harbor Rule to Protect Against Cyberattacks*, IAPP (Sept. 25, 2020), https://iapp.org/news/a/indiana-ag-proposes-safe-harbor-rule-to-protect-against-cyberattacks [https://perma.cc/PL45-WXT2].

standards for midsize and large businesses."[168] Among other things, the statute requires firms to "insure the security and confidentiality of customer information," "protect against anticipated threats," and "protect against unauthorized access."[169] To do so, it requires that covered firms have a comprehensive cybersecurity plan including administrative, technical, and physical safeguards which require specifying a point person for cybersecurity, evaluating and improving cyber hygiene training at the organization, establishing "[d]isciplinary measures for information security violations," and documenting post-breach response.[170]

I. New York

Unlike the CCPA, Nevada's Internet Privacy Act, and other laws centered on consumer data rights, New York state's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), enacted in March 2020, focuses on businesses.[171] The SHIELD Act requires businesses to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information.[172] In contrast, the New York Department of Financial Services (NYDFS) introduced cybersecurity regulations that specifically require "banks, financial services institutions, and insurance companies to create cybersecurity and data privacy compliance programs that protect their own IT systems and customer's confidential information from attacks by cybercriminals."[173] Together, these requirements place New York among the leading states to require reasonable cybersecurity best practices across a range of sectors and industries that are designed

---

[168] KOSSEFF, *supra* note 96, at 57.

[169] MASS GEN. LAWS ch. 93H, §2(a) (2019).

[170] KOSSEFF, *supra* note 96, at 58.

[171] See Brian G. Cesaratto, The New York State "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act) Becomes Effective March 21, 2020: Is Your Organization Ready to Achieve Compliance?, NAT'L L. REV. (Feb. 6, 2020), https://www.natlawreview.com/article/new-york-state-stop-hacks-and-improve-electronic-data-security-act-shield-act [https://perma.cc/M7LC-BEKE].

[172] *Id*.

[173] *The New York Shield Act vs. NYDFS*, GOLD SKY SECURITY (Apr. 5, 2021), https://goldskysecurity.com/the-new-york-shield-act-vs-nyfds [https://perma.cc/XX4Q-X5L3] ("According to Section 899-BB of the New York State Data Security Protection Law, small businesses with less than 50 employees should tailor their security programs to fit their size, the nature and scope of their activities, and the sensitivity of the personal information collected and stored. Compliance with NYDFS and other New York State data security regulations is the same as compliance with the reasonable safeguards requirements section of the SHIELD Act that includes administrative safeguards, technical safeguards, and physical safeguards.").

to "protect the security, confidentiality, and integrity of the private data of New York residents."[174]

J. Relevant Federal & State Court Decisions

The topic of reasonableness has received increasing attention in the cybersecurity context, but has yet to be fully examined as was discussed in Part 1. Yet we can glean clues for how courts at both the federal and state level may rule on the topic by investigating available jurisprudence. For example, *In re Anthem, Inc. Data Breach Litig*, the plaintiffs alleged that the company aggregated millions of subscribers' personal health information (PHI) but failed to meet its own policies or reasonable safeguards to protect these data, resulting in the breach.[175] The court, though, ruled that these terms did not constitute a promise on the part of Anthem to use "reasonable and adequate safeguards" to protect their customers' PHI.[176] Other courts have placed limits on certain practices, such as the use of aerial photography, as being "improper" to obtain trade secrets in the context of discussing reasonable security standards.[177]

On the flip side, an early seminal case testing the bounds of a court's willingness and ability to require new technologies even when they were not yet industry standard was *T.J. Hooper v. Northern Barge Corp*.[178] In this case, which is also known as the "radio-less industry standard case"), the court held that tugs were not seaworthy because they were not able to withstand a coastal storm and that this was worsened by the fact that they could not receive radio reports via radio, despite the fact that radios were not the industry standard at the time.[179] As such, this case suggests that as technology changes, so too do expectations of reasonability, arguably including in the cybersecurity context. For example, there has already been instances in which the Coast Guard's cybersecurity guidance is setting the bar for "reasonable" maritime cybersecurity practices.[180] As the Coast Guard has noted: "Maintaining effective

---

[174] *Id*.

[175] In re Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 314 (N.D. Cal. 2018).

[176] *Id*. (ruling that plaintiffs' complaints alleging company's failure to meet reasonable security standards did not provide cognizable legal claims).

[177] E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970).

[178] The T.J. Hooper, 60 F.2d 737 (2d Cir. 1932).

[179] *Id*. at 740. ("Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.").

[180] Erik Dullea et. al., *Coast Guard Cybersecurity Guidance Puts Shippers On Notice*, LAW360 (Aug. 20, 2019, 3:18 PM EDT),

cybersecurity is not just an IT issue but is rather a fundamental operational imperative in the 21st century maritime environment."[181] Such trends point to the need to practice proactive cybersecurity risk management, including by investing in new technologies even before they become the industry standard. For firms that remain reactive, there is a clear risk, as has been demonstrated in cases such as *Equifax*.[182] Here, the district court ruled that Equifax had "a duty to protect the personal information of the defendant's customers in the context of allegations that the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years and even took affirmative steps to stop its employees from fixing known security deficiencies."[183]

Litigation involving state laws, such as California, has also provided further guidance. Following the well-publicized Yahoo! breach, for example, a district court in the Northern District of California ruled[184] that Yahoo! did not, in fact, exhibit "reasonable" cybersecurity under the California Customer Records Act (CRA).[185] This Act requires that a business: "that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[186]

A separate, but related, issue of defining "reasonable" cybersecurity involves overcoming standing limitations. This is getting easier for plaintiffs given the passage of recent state-level laws in states like California as was described in Part 2, and due to decisions such as *In re Marriott Intl., Inc.*, which held that plaintiffs demonstrated adequate injury-in-fact due to losses from identity theft and other costs that were related to the data breach.[187] Even

---

https://hbfiles.blob.core.windows.net/webfiles/8-20-19%20Law360%20Coast%20Guard%20Cybersecurity%20Guidance%20Puts%20Shippers%20On%20Notice%20AUTHORED.pdf [https://perma.cc/9PPZ-7ZU6].

[181] *Id*.

[182] In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1323 (N.D. Ga. 2019).

[183] *Id*. at 1309, 1323.

[184] In re Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1145 (N.D. Cal. 2018).

[185] CAL. CIV. CODE § 1798.81.5(b) (West 2022).

[186] *Id*.

[187] In re Marriott Intl., Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 495 (D. Md. 2020) (holding consumers "adequately alleged injury-in-fact in the form of losses from identity theft, imminent threat of identity theft, costs

plaintiffs spending more time on a given software product than they otherwise would have if they had known that the software company was not providing "reasonable security" has found to be sufficient to overcome standing concerns.[188]

These cases, along with the state laws examined above, point toward the development of a more supportive foundation for plaintiffs to defend their rights in the aftermath of a breach, along with some support for a greater propensity for courts to hold firms accountable for not demonstrating "reasonable" cybersecurity practices.

K. Summary

As is apparent from the foregoing discussion, there is a great deal of experimentation and divergence with regards to defining "reasonable" cybersecurity across the nation. Consider four states—California, Ohio, Oregon and New York—which passed such laws between 2018 and 2020. There is no consensus on whether to include a safe harbor incentive to encourage firms to adopt cybersecurity best practices with only half of these states (Ohio and New York) including such provisions, nor is there agreement on which cybersecurity frameworks to encourage. On the latter point, though, there does seem to be convergence around some combination of the NIST CSF and CIS Top 20 Security Controls, as is shown in Figure 3.

---

spent mitigating the harms from the data breach, loss of the benefit-of-their-bargain, and loss of value of their personal information" under various state laws).

[188] In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1224, 1229 (N.D. Cal. 2014) (finding that plaintiffs were injured when they alleged they did not receive the benefit-of-the-bargain because had they known Adobe was not providing reasonable security, they would not have paid as much for Adobe products).

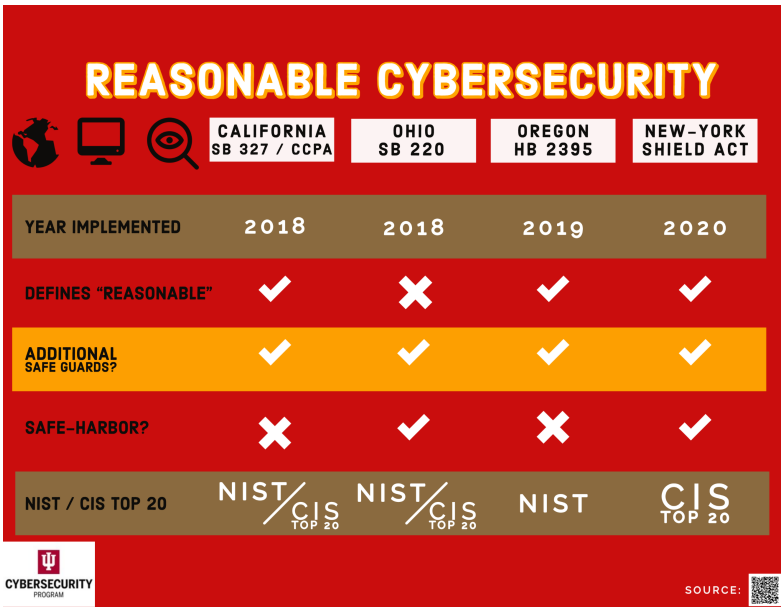


Figure 3: "Reasonable" Cybersecurity Summary Table

One surprising omission from these state-led efforts are tailored policies to manage cyber extortion generally, and ransomware in particular. As of July 2021 only ten states have statutes that address ransomware, or computer extortion; however, other state laws prohibiting malware and computer trespass may be used to prosecute these crimes as well.[189] Why more states have not specifically targeted ransomware given the surge in such attacks especially during the COVID-19 pandemic as was discussed in Part I, or have not encouraged the update of reasonable cybersecurity practices to guard against such incidents, remains a mystery.

IV. EMPIRICAL RESULTS

The overlapping patchwork of cybersecurity laws currently in effect in the United States—and interest in requiring stronger cybersecurity practices amongst both federal and state lawmakers—raise the question of how public and private organizations perceive

[189] These states include California (CAL. PENAL CODE § 523 (West 2018)), Connecticut (CONN. GEN. STAT. § 53a-262 (West 2017)), Indiana (2021 IND. H.B. 1169), Louisiana (LA. REV. STAT. §§ 51:2111 to 51:2116 (West 2021)), Maryland (2021 MD. H.B. 425 / 2021 S.B. 623), Michigan (MICH. PENAL CODE §§ 750.409b, 777.16t (2018), North Dakota (2021 N.D. H.B. 1314), Oklahoma (2021 OKLA. H.B. 1759), Texas (TEX. PENAL CODE § 33.02 (2015)), and West Virginia (W. Va. Code §§ 61-3C-3 to 61-3C-4 (2020)). *See Computer Crime Statutes,* NAT'L CONF. OF STATE LEGISLATURES (May 4, 2022), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Hacking [https://perma.cc/X7SX-VZ2D].

and respond to cyber risk under the current regime. A clearer picture of this behavior and how it varies across organization type could help policymakers characterize the status quo, craft policy to encourage most urgently needed cybersecurity practices, and predict how implementation costs/difficulty might vary across organization type. For example, if small businesses are systematically engaged in lower levels of cybersecurity protections than medium and large businesses, a state might elect to engage in specialized outreach to small businesses to ensure they understand and can comply with new regulations. Characterizing the variation in cybersecurity practices can also help policymakers identify areas where there is ambiguity about best practices or organizations differ in their understanding of risk. However, there is little data currently available on organizational cybersecurity behavior, including adoption of practices (such as use of the NIST CSF) that have formed the basis for the definition of "reasonable" cybersecurity in proposed and enacted state laws.

In order to address this gap, we conducted a survey in conjunction with the Indiana Executive Cybersecurity Council and the Indiana Business Research Center to elicit information from organizations in Indiana about their cybersecurity practices. This survey focused on a number of areas, including cyber risk perceptions, cyber risk management and planning, and cyber risk insurance use. In the remainder of this section, we describe the methodology and results of this survey.

A. Methodology and Limitations

Our first step in designing a survey to elicit information about cybersecurity perceptions and practices amongst organizations in Indiana was to consult with a range of stakeholders on both general topics that should be addressed and specific questions that should be asked. Based on this feedback, we designed a multi-section survey that elicited information about cyber risk perceptions, cyber risk management and planning, cyber risk insurance use/non-use, and respondent characteristics. This preliminary survey was then rigorously reviewed by representatives from the public and private sector to ensure that the questions being asked would be understandable to respondents and likely to elicit truthful responses, rather than overly optimistic ones, through proper framing.

The survey was distributed in conjunction with the Indiana Executive Cybersecurity Council and the Indiana Business Research Center. These partners emailed a list of more than 3,000 public and private organizations in Indiana with a request to participate in this study and a link to the survey. We received 336 responses, including

197 complete responses and 139 incomplete responses. After dropping incomplete responses before analysis, we had an overall response rate of about 6%.

Sixty-three percent of our respondents indicated that their organization was part of a critical infrastructure sector.[190] The government facilities sector was the most common critical infrastructure sector identified by respondents, with about 36% of respondents overall identifying their organization as falling within this sector. About 43% percent of our respondents were from organizations with 10 or fewer employees; 15% were from organizations with 11-50 employees; 20% were from organizations with 51-250 employees; 19% were from organizations with more than 250 employees; 3% did not indicate the size of their organization. For purposes of the following analysis, we defined "small" organizations as those with 50 or fewer employees and "medium and large" organizations as those with more than 50 employees. As such, 57% of our respondents were from small organizations and 43% were from medium and large organizations.

To benchmark our sample, Figure 4 below compares the size distribution of our respondents with the size distribution of Indiana organizations as a whole based on data from the County Business Patterns. Our sample includes a lower proportion of small organizations and a greater proportion of large organizations than is apparent in the population of Indiana organizations as the whole. About 83% of our respondents were from organizations with a local geographic scope and about 8% were from organizations with a state geographic scope; the remainder were regional, national, and multi-national organizations.

[190] Critical infrastructure sectors include "physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety." *Infrastructure Security*, CISA, https://www.cisa.gov/infrastructure-security [https://perma.cc/KP3S-MXBE] (last visited Sept. 2022).

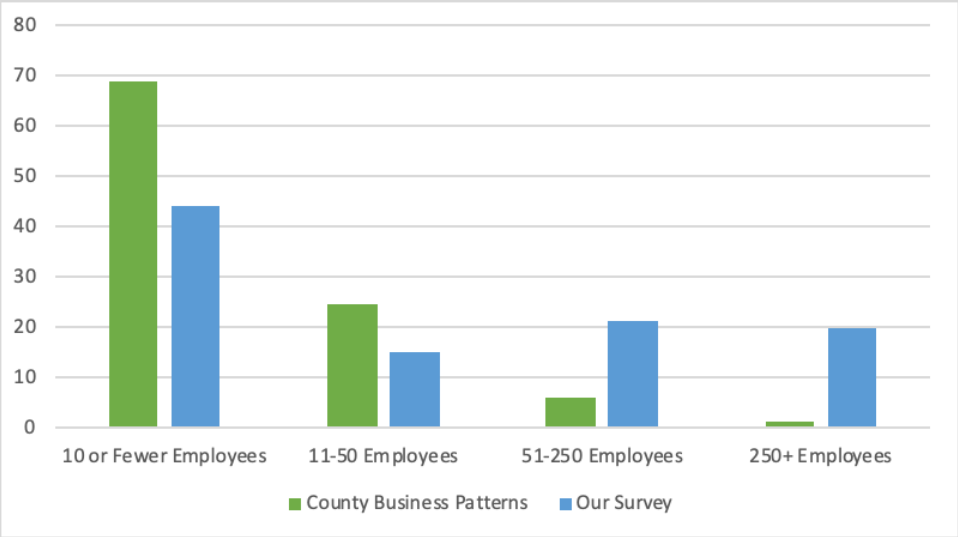


Figure 4: Comparison of Survey Respondents to County Business Patterns Across Organization Size

There are a number of limitations to this study that must be considered with interpreting the following results. Our response rate of 6% is relatively low. Although that is common for standard surveys (even among premier pollsters, like Gallup),[191] we analyze the data with an exploratory goal to look at patterns of behavior amongst our respondents, rather than conducting a parameter estimate of the prevalence of these behaviors in Indiana organizations as a whole. This low response rate raises particular concerns that our respondents were willing to take our survey because they were especially concerned about or interested in cybersecurity, suggesting that our respondent pool may disproportionately include representatives from organizations with strong cybersecurity practices.

Additionally, our respondent pool oversamples the largest organizations in Indiana: establishments with over 250 employees comprise about 19% of our sample versus about 1% in the Indiana economy overall. We also oversample establishments with between 50 and 249 employees, and undersample those with 1-9 and 10-49 employees. As we will discuss in the remainder of our results section, stronger cybersecurity amongst larger organizations suggests that the frequency of cybersecurity practices in our respondent pool is likely higher than the prevalence of these practice amongst Indiana organizations as a whole. Consequently, these

[191] *See* Stephanie Marken, *Still Listening: The State of Telephone Surveys*, GALLUP (Jan. 11, 2018), https://news.gallup.com/opinion/methodology/225143/listening-state-telephone-surveys.aspx [https://perma.cc/5WN8-6SNG].

results should be taken as exploratory rather than representative of Indiana organizations as a whole.

B. Perceptions and Experience with Cyber Incidents

Participants in our study were first asked about their perceptions of the level of cyber risk faced by their organization. On the whole, the risk of a cyber incident appears to be of substantial concern to Indiana organizations, with about 46% of respondents indicating that their organization was somewhat concerned about the risk of a cyber incident and about 49% of respondents indicating that their organization was very concerned about the risk of a cyber incident. These levels of concern appear to vary across respondents from critical infrastructure and non-critical infrastructure organizations, with about 52% of respondents from critical infrastructure sectors indicating that their organization was very concerned, as compared with about 43% of respondents from non-critical infrastructure organizations. Reported levels of concern were also different across respondents from small and medium/large organizations, with about 38% of respondents from small organizations indicating that their organization was very concerned about the risk of a cyber incident, in comparison with about 64% of respondents from medium/large organizations.

In order to investigate perceptions potentially underlying these concerns, respondents were then asked about the likelihood of that their organization would face a cyber incident, and the level of harm that they thought their organization would face if they experienced a cyber incident. On a 0-100 scale (0 being very unlikely, 100 being very likely), respondents on average indicated an average likelihood level for a cyber incident at around 50; for comparison, respondents placed the likelihood of loss due to fire, lawsuit due to workplace injury, and natural disaster at around 30 on the same scale, and the likelihood of theft by insiders or outsiders even lower. The perceived likelihood of a cyber incident was comparable, but not identical across respondents from critical infrastructure and non-critical infrastructure organizations, with respondents from critical infrastructure organizations indicating on average a slightly higher level of concern than non-critical infrastructure organizations (52 compared with 48 on a 101-point scale). Small organizations on average indicated a substantially lower level of concern than medium and large organizations (43 compared with 61 on a 101-point scale). These descriptive statistics suggest that much more variation in overall attitudes is driven by firm size, rather than sector.

Respondents on average indicated that they thought their organization would face a harm level of around 59 on a 0-100 scale

(0 being very little harm, 100 being a great deal of harm) if they were subject to a cyber incident. This is comparable to the average harm level respondents believed their organization would face if subject to a loss due to fire or a natural disaster (61 and 62 on a 101-point scale respectively), and higher than the harm level respondents believed their organization would face if subject to a lawsuit due to an outsider theft, insider theft, or lawsuit due to a workplace injury (40, 36, and 36 on a 101-point scale respectively. Perceptions of potential harm from a cyber incident varied across organization type in a similar way to perceptions of the likelihood of a cyber incident, with respondents from critical infrastructure organizations on average having a comparable but not identical level of perceived potential harm as those from non-critical infrastructure organizations (60 compared with 56 on a 101-point scale) and respondents from smaller organizations on reporting a substantially lower level of perceived potential harm compared with respondents from medium and large organizations (52 compared 67 on a 101-point scale).

Respondent perceptions of the likelihood that their organization may face a cyber incident—and the harm that may occur if they do—may be shaped by knowledge of whether their organization had experienced a cyber incident in the past. About 19% of respondents indicated that their organization had experienced a successful cyber incident in the past three years, about 67% indicated that their organization had not experienced a successful cyber incident in the past three years, and about 13% declined to respond to the question.

Analyzing data from those respondents who provided an answer to this question, we also find considerable variation across organization type. Fewer respondents from critical infrastructure organizations indicated that their organization had been subject to a successful cyber incident in the past three years than respondents from non-critical infrastructure organizations (16% as compared with 32%). Fewer respondents from small organizations indicated that their organization had been subject to a successful cyber incident in the past three years than respondents from medium and large organizations (9% as compared with 41%). These numbers should be interpreted with particular care, as there was a substantial level of non-response to this question and there are reasons to believe that respondents from some types of organizations may be more hesitant to disclose that their organization had been subject to a cyber incident. Levels of non-response were similar across respondents from critical and non-critical infrastructure organizations (13% as compared with 12%), but were slightly higher amongst respondents from medium/large organizations in

comparison with respondents from small organizations (15% as compared with 12%).

C. General Prevention and Mitigation Practices

The Indiana organizations we surveyed reported frequently engaging in cyber incident prevention practices, with almost 82% of respondents saying that their organization had taken steps to prevent cyber incidents. This percentage was similarly high across critical infrastructure organizations and non-critical infrastructure organizations. Respondents from medium and large organizations reported that their organization engaged in prevention activities more frequently than those from small organizations, with about 94% of respondents from medium and large organizations reporting prevention activities as compared with about 74% of respondents from small organizations.

Those respondents who reported that their organization engaged in cyber incident prevention practices were then asked about the specific practices used. On average, respondents indicated that their organization engaged in 4.3 of the prevention practices listed on the survey (counting the "other" category as a single practice). This number was relative stable across respondents from critical infrastructure organizations (4.4 prevention practices) and non-critical infrastructure organizations (4.1 prevention practices), and was fairly similar across small organizations (3.9 prevention practices) and medium/large organizations (4.7 prevention practices). Figure 5 shows most respondents reported that their organizations prevented cyber incidents through installing anti-virus software, updating/patching software, and training their employees.

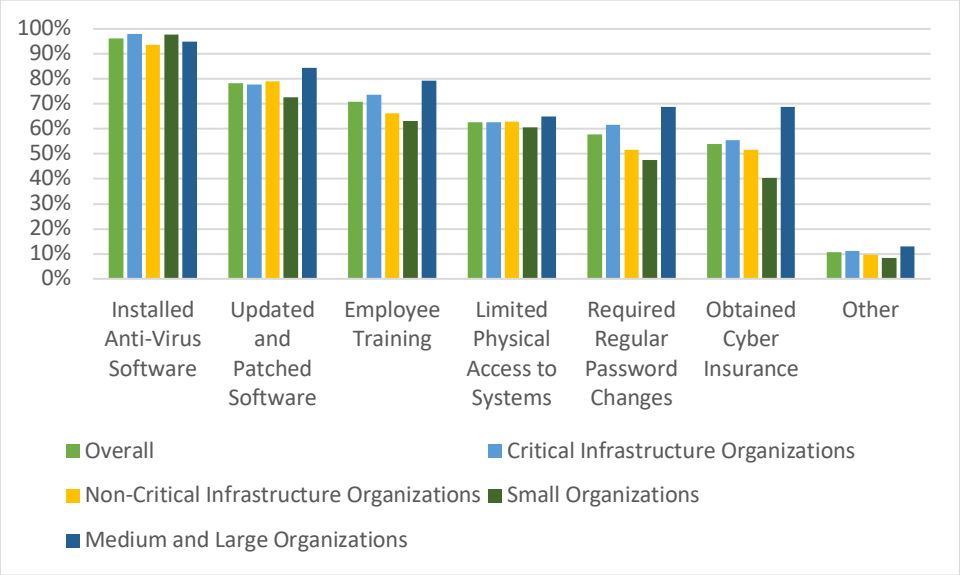


Figure 5: Reported Cyber Incident Prevention Practices

Mitigation planning is an essential complement to cyber incident prevention activities. About 68% of our survey respondents reported that their organization had taken steps to mitigate the impacts of a cyber incident; a figure that was fairly consistent across respondents from critical infrastructure organizations and non-critical infrastructure organizations. Fewer small organizations reported that their organization had undertaken mitigation steps, with about 56% of respondents from small organizations reporting that their organization engaged in cyber incident mitigation practices in comparison with about 87% of medium and large organizations. This echoes our previous finding on the frequency of cyber incident prevention practices.

Respondents who indicated that their organization had engaged in cyber incident mitigation practices were then asked about the specific practices used. On average, respondents reported that their organization engaged in 2.7 of the mitigation practices listed on the survey (counting the "other" category as a single practice). The average number of mitigation practices was very similar across critical infrastructure organizations (2.67 mitigation practices) and non-critical infrastructure practices (2.8 mitigation practices), as well as small organizations (2.42 mitigation practices) and medium/large organizations (2.98 mitigation practices). Figure 6 helps us understand more about the specific mitigation practices that respondents indicated they were engaged in through their organization, drawing mainly on automatic backup systems, followed by cloud computing and adoption of cyber risk insurance, to mitigate cyber risk.

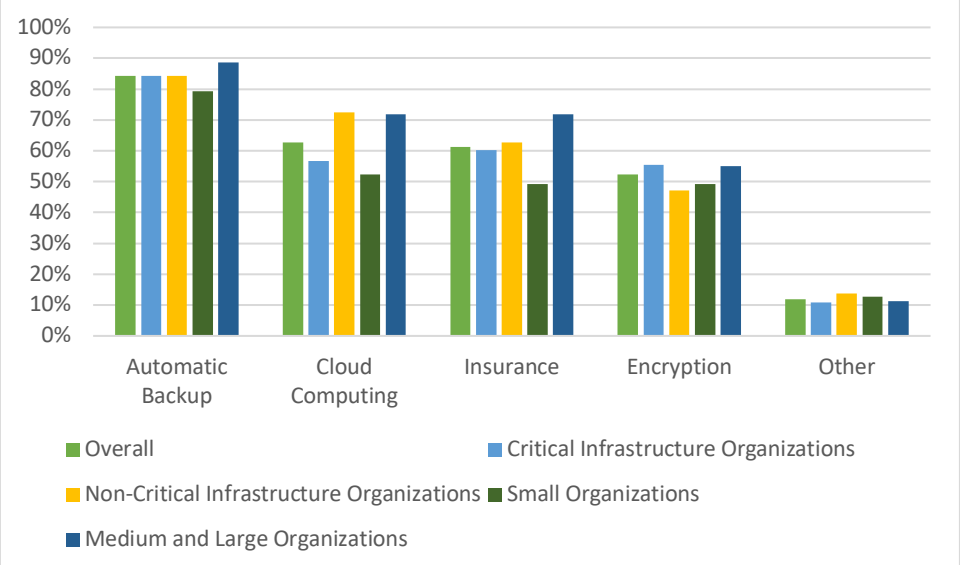


Figure 6: Reported Cyber Incident Mitigation Practices

In addition to being asked about their cyber incident prevention and mitigation practices, respondents were asked about their organization's cyber security practices in general. As is shown in Figure 7 below, the most common practices reported were automatic updating of operating systems and remote backups, followed by multi-factor authentication.

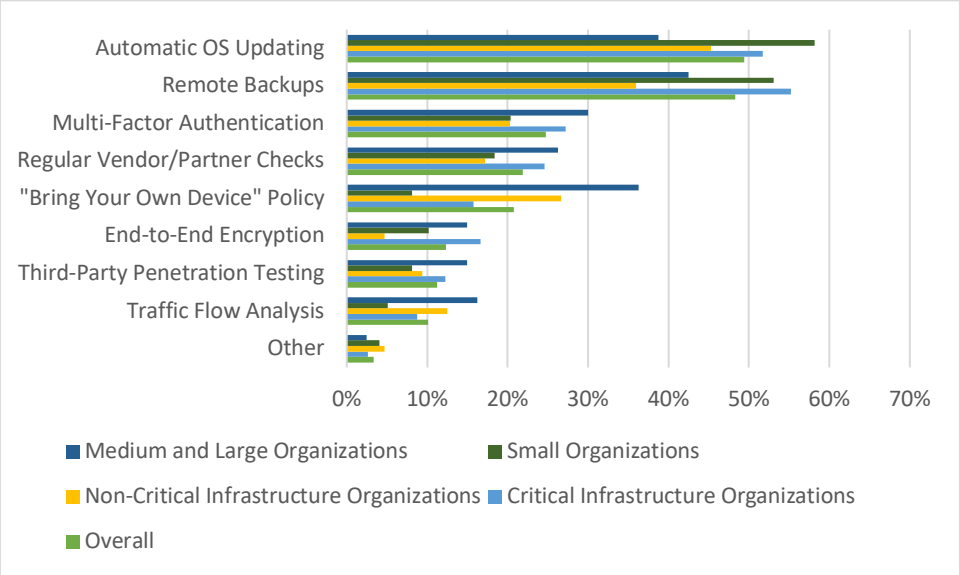


Figure 7: Cyber Security Practices

Employee training is a critical component of organizational cyber incident preparedness.[192] About 30% of respondents indicated that they had received cyber security training in a formal setting from their organization. This number was higher amongst respondents from critical infrastructure organizations (33%) than non-critical infrastructure organizations (24%), and was higher amongst respondents from medium/large organizations (35%) than small organizations (26%). About 75% of respondents who indicated that they received formal cybersecurity training from their organization described that training as occurring at least yearly. This number was higher amongst respondents from critical infrastructure organizations (77%) in comparison with non-critical infrastructure organizations (67%), and higher amongst respondents from medium/large organizations (86%) than small organizations (67%).

[192] See generally Nabin Chowdhury & Vasileios Gkioulos, Cyber Security Training for Critical Infrastructure Protection: A Literature Review, 40 COMP. SCI. REV. 100361 (2021).

D. Use of Proactive Tools and Externally-Developed Frameworks

Organizations have a number of tools and decision-making frameworks to help them proactively manage their cybersecurity needs. To explore how these resources are used, respondents were asked whether their organization used any of a provided list of tools to proactively manage cyber risk, as summarized in Figure 8 below. Overall, respondents most commonly indicated that their organization revised organizational governance to ensure that cyber threat information was getting where it was needed, with about 31% of respondents selecting that option, followed by consulting news reports (30% of respondents) and relying on government data (24%).

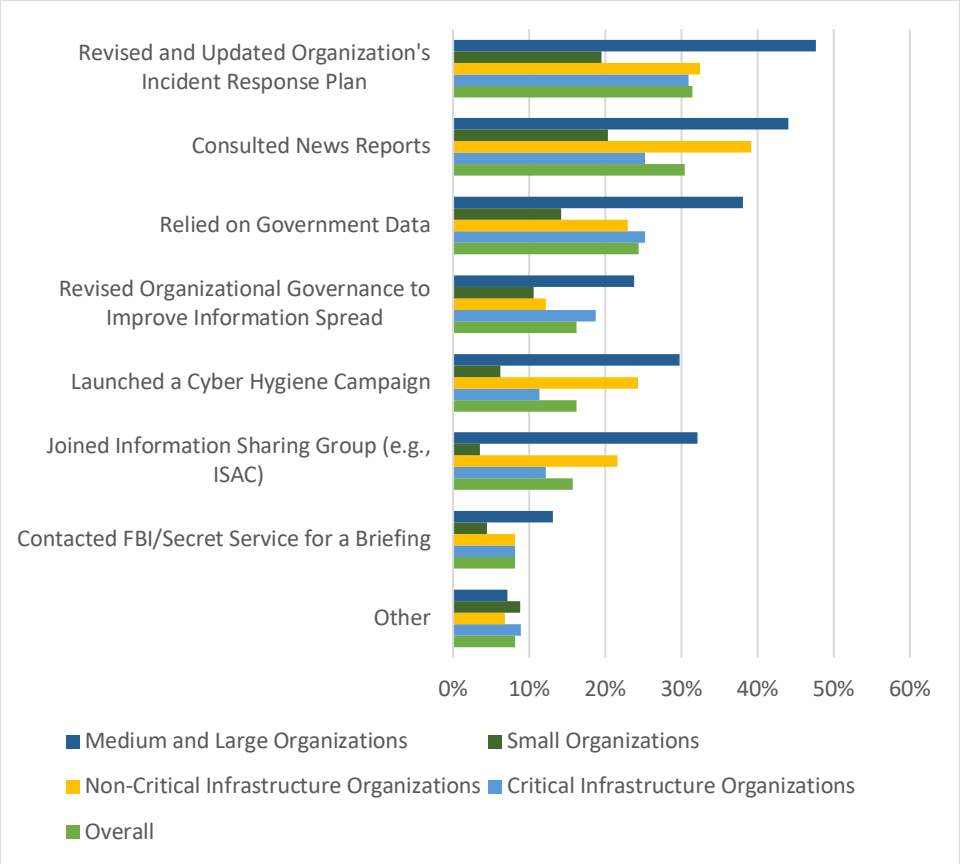


Figure 8: Tools Used to Proactively Manage Cyber Risk

In addition, organizations may use externally developed frameworks to guide their cybersecurity decision-making. In particular, there has been much interest on the impact of the NIST Cyber Security Framework on cybersecurity decision-making, as it

"has the potential to shape a standard of care for domestic critical infrastructure organizations . . . [and] help to harmonize global cybersecurity best practices for the private sector writ large."[193] About 30% of respondents indicated that their organization referred to externally developed tools in making cybersecurity decisions, although a large proportion (34%) were unsure. This number was very similar across both respondents from critical infrastructure (30%) and non-critical infrastructure (30%) organizations. However, respondents from medium/large organizations much more frequently indicated that their organization used an externally developed tool to make decisions (48%) when compared with small organizations (17%). The NIST CSF was the external decision-making framework most commonly adopted, with about 59% of respondents who indicated that their organization used an external framework further indicating that they used the NIST Cybersecurity Framework. This number was higher amongst critical infrastructure organizations (67%) than non-critical infrastructure organizations (45%), and higher amongst medium/large organizations (62%) than small organizations (53%).

E. Use of Cyber Risk Insurance

As insurance can be a crucial tool for both managing risk to an organization and promoting public welfare,[194] we elicited information about organizational use of cyber risk insurance from our respondents. Almost half of our respondents indicated that their organization had cyber risk insurance. The frequency of cyber risk insurance was similar across respondents from critical infrastructure organizations (51%) and non-critical infrastructure organizations (49%). Respondents from small organizations less frequently indicated that their organization had cyber risk insurance than respondents from medium/large organizations, with about 36% of small organization respondents indicating that their organization had cyber risk insurance in comparison with almost 70% of medium/large organizations.

---

[193] Scott J. Shackelford et al., Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices, 50 TEX. INT'L L.J. 305, 310 (2015).

[194] *See* Damla Kuru and Sema Bayraktar, *The Effect of Cyber-Risk Insurance to Social Welfare*, 24 J. FIN. CRIME 329 (2017); Robert S. Kaplan & Anette Mikes, *Managing Risks: A New Framework,* HARV. BUS. REV. (2012), https://hbr.org/2012/06/managing-risks-a-new-framework [https://perma.cc/M7GG-AFNM].

The scope of coverage provided by cyber risk insurance may vary greatly.[195] To explore the extensiveness of coverage, respondents who indicated that their organization had cyber risk insurance were then asked to indicate what first-party losses were covered by their insurance. Respondents on average indicated that their organization had coverage for 4.4 loss categories out of a provided list of 12 loss categories (including the "other" category as a single type). The scope of insurance coverage appeared to be similar across respondents from critical infrastructure organizations (who on average indicated that their insurance covered 4.5 loss categories) and non-critical infrastructure organizations (who on average indicated that their insurance covered 4.4 loss categories. However, the scope of insurance coverage did appear to vary across small and medium/large organizations. Respondents from small organizations on average indicated that their insurance covered 3.9 loss categories, while respondents from medium and large organization on average indicated that their insurance covered 4.8 loss categories. The frequency of respondents indicating that their insurance covered various loss categories is depicted in Figure 9 below.

[195] Sasha Romanosky et al., Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?, 5 J. CYBERSECURITY 1, 5 (2019).

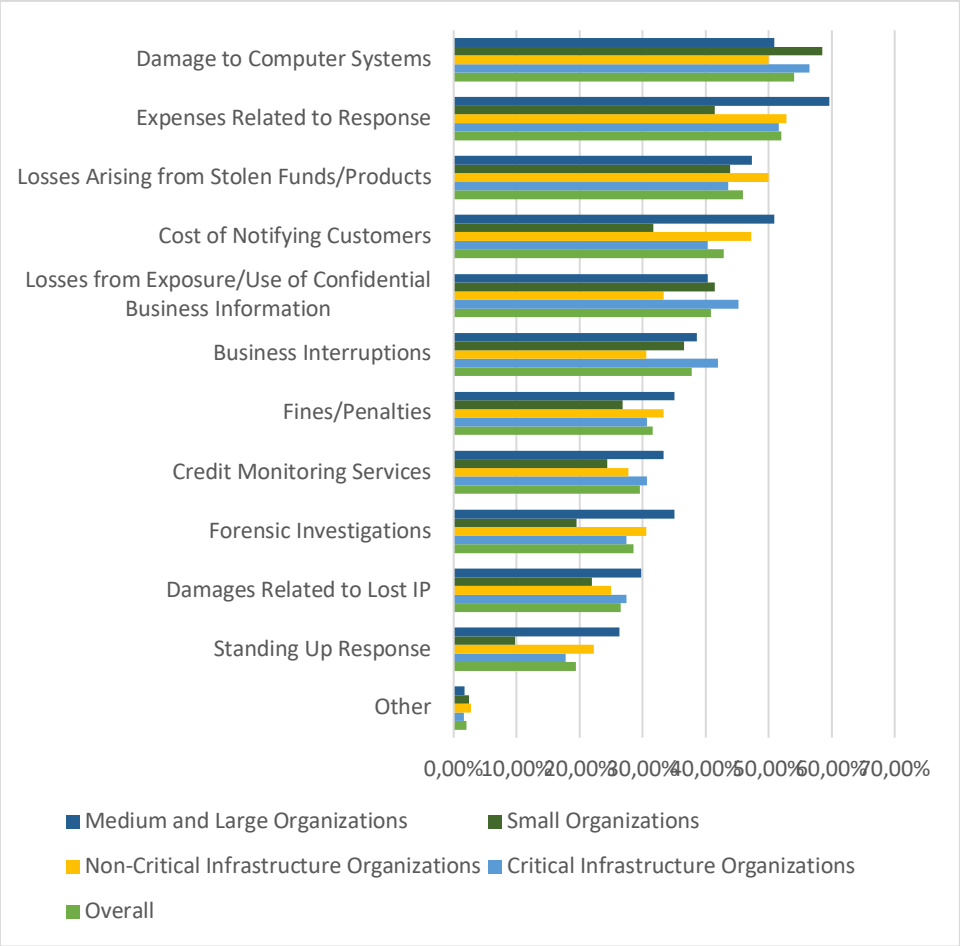


Figure 9: First Party Losses Covered Under Cyber Risk Insurance Policies

In addition to allowing organizations to manage risks associated with cyber incidents, cyber risk insurance can also change organizational cyber security behaviors by mandating certain security practices as a condition of coverage. About 48% of respondents who indicated that their organization had cyber risk insurance further indicated that their insurer required security measures as a condition of their policy. This number was slightly higher amongst critical infrastructure organizations (50%) than non-critical infrastructure organizations (44%), and slightly higher amongst medium/large organizations (49%) than small organizations (46%). Respondents who indicated that their insurer required security measures as a condition of their policy were then asked to describe which security measures were required. The most commonly indicated security requirement was employee training and cyber hygiene, with about 40% of relevant respondents indicating that these measures were required by their insurer,

followed by mandatory automatic patching, with about 34% of relevant respondents indicating that these measures were required by their insurer.

V. POLICY IMPLICATIONS

This final Part summarizes the results of the Indiana case study presented in Part 3, and then investigates the implications of these findings for policymakers and practitioners including the overarching discussion of defining "reasonable" cybersecurity.

A. Summary and Overview of Results

Table 1 below provides a qualitative overview of the results provided in Part 4, with particular focus on instances where the frequency of cybersecurity perceptions or practices varied across the critical/non-critical infrastructure or small/medium and large organizations in our respondent pool.

Table 1: Overview and Summary of Results

Perception/ Practice	Overall Description	Differences by Critical Infra. Status	Differences by Organization Size
Perceptions and Experience with Cyber Incidents			
Risk of Incident	95% somewhat or very concerned	More critical infrastructure organizations very concerned	Many more medium/large organizations very concerned
Likelihood of Incident	Likelihood of cyber incident much higher than likelihood of loss due to fire or lawsuit from workplace injury		Medium/large organizations much more concerned on average
Harm from Incident	If cyber incident occurs, harm about same as harm of a fire or natural disaster		Medium/large organizations expect less harm
Past Cyber Incidents	19% of organizations had successful cyber incident in last 3 years	Fewer critical infrastructure organizations reported incidents	Many more medium/large organizations reported incidents
General Prevention and Mitigation Practices			

Adopted Prevention Practices	82% had taken steps to prevent cyber incidents		Many more medium/large organizations reported prevention practices
N Prevention Practices	Reported 4.3 prevention practices on average		
Adopted Mitigation Practices	68% had taken steps to mitigate damage if incident occurred		Many more medium/large organizations reported mitigation practices
N Mitigation Practices	Reported 2.7 mitigation practices on average		
General Security Practices	Automated updating of OS most common		
Employee Training	30% of respondents reported formal training	Slightly more respondents from critical infrastructure organizations reported training	Slightly more respondents from medium/large organizations reported training
Use of Proactive Tools and Externally-Developed Frameworks			
Use of Proactive Tools	Revised and updated incident response plan most common		
Use of External Frameworks	30% report use of externally developed framework		Many more medium/large organizations reported use of external framework
Use of NIST CSF	59% who used framework used NIST CSF	Many more critical infrastructure organizations who used framework used NIST CSF	More medium/large organizations who used framework used NIST CSF
Use of Cyber Risk Insurance			
Insurance Adoption	50% adopted cyber risk insurance		Many more medium/large organizations adopted cyber risk insurance

Covered Losses	Reported 4.4 types of first party losses covered on average		Medium/large organizations reported more loss types covered
Insurance Mandated Security	48% with insurance reported security measured required by policy	Slightly more critical infrastructure companies reported security measures required	

Taken as a whole, these results suggest that there were some systematic differences in the cybersecurity practices of the critical infrastructure organizations and the non-critical infrastructure organizations represented by the respondents in our sample. Where there were differences between these two types of organizations, respondents from critical infrastructure organizations reported "stronger" practices as measured by the number and breadth of cybersecurity best practices they have deployed. These differences are most pronounced with regards to adoption of the NIST CSF, which is expected given that the original intent of the NIST CSF was to guide decision-making amongst critical infrastructure organizations.

Our results also suggest that there were more pronounced differences in the cybersecurity practices of the medium/large organizations and the small organizations represented by the respondents in our sample, with stronger practices always being reported by representatives from medium/large organizations. These differences appear to be quite substantial in some cases; for example, almost twice as many respondents from medium/large organizations reported that their organization had cyber risk insurance than respondents from small organizations.

Among other things, it might be expected that the observed differences in cybersecurity practices across different types of organizations could be driven by differences in risk perceptions across organization type. While our survey results do not necessarily imply causality between perception and prevention practices, this would be a fruitful area for future research. The type of organizations that reported higher perceived risk also reported more comprehensive cybersecurity practices. This is particularly pronounced when considering the differences between medium/large organizations and small organizations, as medium/large organizations reported higher perceived risk of an incident, likelihood of an incident, and potential harm from an incident — and also described stronger cybersecurity practices across more than half of the cybersecurity practice dimensions

considered in this study. Interestingly, this relationship is not clearly seen when considering whether the type of organizations that report experiencing cyber incidents are also the types of organizations that report strong cybersecurity practices. Future research could help expand the evidence base in this area by incorporating experimental components into surveys on organizational cybersecurity practices that attempt to vary perceived risk in order to explore its effects on cybersecurity practice adoption.

B. Implications for Defining Reasonability

As Loren Selznick and Carolyn LaMacchia note with regards to how courts are weighing whether "reasonable" data security was demonstrated: "Courts generally take into account the financial resources of the business in determining what is reasonable[, but] [t]he law should also take into account the technological expertise and education of the small business owner."[196] Based on the results of our survey, this observation seems particularly apt. Rather than focusing on the divide between critical and non-critical infrastructure providers, which while important given the number of sector-specific laws and requirements discussed in Parts 1 and 2, a more significant factor in cybersecurity readiness appears to be firm size and related risk perceptions. The implications for this finding, and recalling the extent to which it should be considered in context given the limitations of this survey discussed in Part 3, underscore the need for stepped up efforts to distill complex cybersecurity standards and frameworks down to a series of understandable action items that small business owners can appreciate, and afford to adopt. NIST's efforts at developing a 'Small Business Cybersecurity Corner" are a useful step in this direction, but as seen in the survey there remains significant confusion about what proactive steps small businesses need to take even when they are aware of the cyber risks they face.[197]

Small and medium-sized businesses are rightly confused about what constitutes "reasonable" cybersecurity given the confusion of state-level laws and industry norms discussed in Parts 1 and 2. Globally, this is also an area of concern since both California's CCPA[198] and the EU's General Data Protection

[196] Selznick & LaMacchia, *supra* note 88, at 253.

[197] *See Small Business Cybersecurity Corner*, NIST, https://www.nist.gov/itl/smallbusinesscyber [https://perma.cc/6CSL-Z2JP] (last visited Sept. 3, 2021).

[198] California Consumer Privacy Protection Act of 2018, Cal. Civ. Code § 1798.100 (West 2022).

Regulation (GDPR)[199] call for "reasonable" cybersecurity.[200] Certain European nations, such as Norway, have similar long-standing and well-defined commitments to requiring reasonable cybersecurity practices. For example, Norway's 2019 Security Act requires "that any sensitive objects, infrastructure information and information systems shall have a 'reasonable' level of security."[201] This marks a departure from previous specific to functional requirements for Norwegian firms, with reasonability being a "dynamic concept that will be in constant change based on technological development, innovations and new threats."[202] As with other jurisdictions including China, though, Norway's classification/grading system will help in this regard with more critical and higher-level threats receiving more stringent security requirements.[203]

Reasonability, then, is clearly a moving target given technological and regulatory trends, as well as the knowledge level of the business in question. For example, in *Patco Construction Co. v. People's United Bank*, for example, the First Circuit found that the cybersecurity protections in place were unreasonable under the circumstances because the bank's leadership were aware of ongoing fraud using keyloggers—malware that records and transmits the victim's keystrokes—but did not have activity-based monitoring in place to detect such nefarious activity.[204] Thus, bank executives had breached their duty to their customers.[205] Other examples of unreasonable cybersecurity practices according to the FTC, which was discussed in Part 1, are offered in Figure 10.

---

[199] Regulation 2016/679, art. 88, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/2RZ3-KZKT].

[200] *See* Abraham Kang, *What Is "Reasonable Security"? And How to Meet the Requirement*, CSO ONLINE (Apr. 23, 2019), https://www.csoonline.com/article/3390150/what-is-reasonable-security-and-how-to-meet-the-requirement.html [https://perma.cc/9HMJ-K66M].

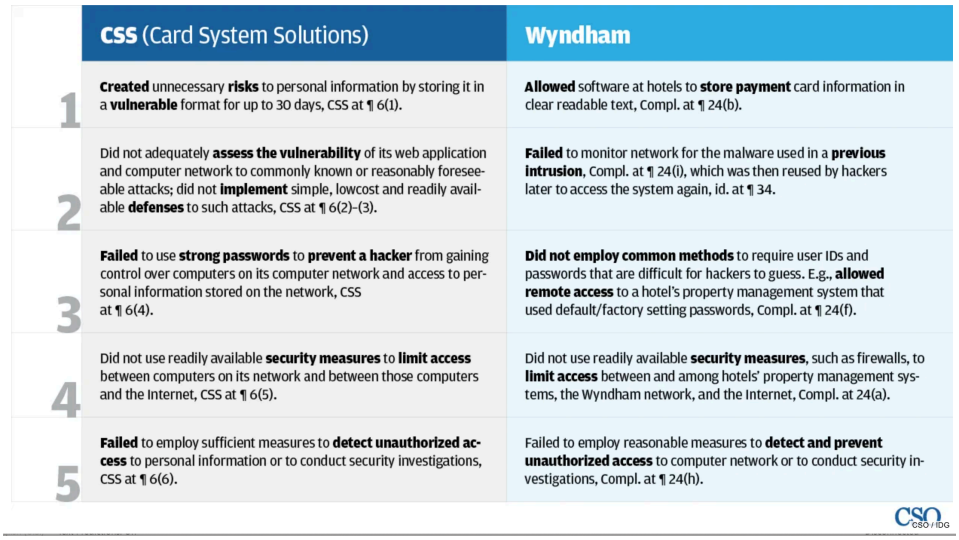
[201] Jeppe Songe-Møller, Erlend W. Holstrøm, & Tore Fjørtoft, *The New Security Act*, SCHJØDT (Aug. 30, 2019), https://www.schjodt.no/news--events/nyhetsbrev/the-new-security-act [https://perma.cc/V5WE-D9D6].

[202] Kang, *supra* note 200.

[203] Møller, *supra* note 201.

[204] Kang, *supra* note 200; *Patco Const. Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012).

[205] Kang, *supra* note 200.



	CSS (Card System Solutions)	Wyndham
1	**Created** unnecessary **risks** to personal information by storing it in a **vulnerable** format for up to 30 days, CSS at ¶ 6(1).	**Allowed** software at hotels to **store payment** card information in clear readable text, Compl. at ¶ 24(b).
2	Did not adequately **assess the vulnerability** of its web application and computer network to commonly known or reasonably foreseeable attacks; did not **implement** simple, lowcost and readily available **defenses** to such attacks, CSS at ¶ 6(2)-(3).	**Failed** to monitor network for the malware used in a **previous intrusion**, Compl. at ¶ 24(i), which was then reused by hackers later to access the system again, id. at ¶ 34.
3	**Failed** to use **strong passwords** to **prevent a hacker** from gaining control over computers on its computer network and access to personal information stored on the network, CSS at ¶ 6(4).	**Did not employ common methods** to require user IDs and passwords that are difficult for hackers to guess. E.g., **allowed remote access** to a hotel's property management system that used default/factory setting passwords, Compl. at ¶ 24(f).
4	Did not use readily available **security measures** to **limit access** between computers on its network and between those computers and the Internet, CSS at ¶ 6(5).	Did not use readily available **security measures**, such as firewalls, to **limit access** between and among hotels' property management systems, the Wyndham network, and the Internet, Compl. at 24(a).
5	**Failed** to employ sufficient measures to **detect unauthorized access** to personal information or to conduct security investigations, CSS at ¶ 6(6).	Failed to employ reasonable measures to **detect and prevent unauthorized access** to computer network or to conduct security investigations, Compl. at ¶ 24(h).

CSO / IDG

Figure 10: FTC's Examples of Unreasonable Cybersecurity[206]

Relatedly, it is important to note that professionals that hold themselves out as having "specialized skills related to executing a job successfully."[207] Cybersecurity professionals, then, would in many cases likely be included under a broad professional standard of care.[208] Further, there is a strong ethical case to be made that business leaders and lawyers should likewise hold themselves up to a higher standard of care given the trust placed in them by their clients and shareholders. This could include an ethical obligation to create a reasonable "security-aware culture, as was discussed above.

A universal baseline standard of "reasonable" cybersecurity, then, is impossible to state for all circumstances, but should be thought of as a sliding scale but with certain universal precautions that all businesses, regardless of their size or sophistication, should arguably be taking that takes into account (1) the sensitivity of the information in question, and (2) utilizes cost/benefit analysis. With those caveats, it seems clear that given the wide array of cybersecurity frameworks and standards on offer, a safe harbor law such as Ohio's has distinct advantages given that it offers businesses a menu of options. Indiana's 2020 attempt fell short, in part, due to a rigidity in only permitting the NIST CSF. While the data presented in Part 3 demonstrates that the NIST CSF is the dominant cybersecurity framework used by most small and medium-sized businesses, many prefer the CIS Top 20, NIST SP 800-53, or other approaches discussed in Part 2 as well as the newer Cybersecurity

[206] *Id.*
[207] *Id.*
[208] *Id.*

Maturity Model Certification (CMMC).[209] More can certainly be done to help small business owners by not just developing small business cybersecurity guides for particular frameworks, but highlighting areas of overlap, such as been done by the Center for Applied Cybersecurity Research with their Information Security Practice Principles.[210]

The Sedona Conference similarly has made effort in developing a cybersecurity reasonability test to help guide businesses, regulators, and judges.[211] The organizers recognize what has been discussed throughout this Article, that is that while frameworks such as NIST CSF are useful, they are static and divorced from context, and there is relatively little overlap between diverse approaches— fewer than half of the laws Sedona reviewed, for example, had a common cybersecurity component.[212] Moreover, the guidance that has been offered to help firms interpret these often conflicting and ambiguous definitions is often non-binding, and even where it does have legal force such as with regards to the FTC, oftentimes high-level controls are favored over clear instructions.[213] Without clear guidance, courts are left to determine reasonability, which has been shown to be increasingly essential in data security claims such as was seen in *Dittman v. University of Pittsburgh Medical Center*, when the Pennsylvania Supreme Court "affirmed the preexisting, negligence-based duty to safeguard personal information where an employer had required employees to provide personal information and then stored it in a manner that permitted an undetected breach of that information."[214] As such, the Sedona organizers argue for a test for "reasonable" cybersecurity that does not mandate security controls, define "personal information," require that a breach have happened to be actionable, establish causation, or legal fault.[215] Instead, they opt for an adaptation of the test that Judge Learned Hand famously articulated in *United States v. Carroll Towing Co*., which states that B2 — B1 < (P x H)1 — (P x H)2.[216]

---

[209] *Cybersecurity Maturity Model Certification*, U.S. DEP'T OF DEF., https://dodcio.defense.gov/CMMC [https://perma.cc/6MQS-H956] (last visited Dec. 11, 2022).

[210] *See* Information Security Practice Principles, CACR, https://cacr.iu.edu/principles/index.html [https://perma.cc/9EXY-GFU7] (last visited Sept. 3, 2021).

[211] The Sedona Conference Commentary on a Reasonable Security Test, 22 SEDONA CONF. J. 345 (2021).

[212] *Id*. at 352-53.

[213] *Id*.

[214] *Id*. at 354 (citing 196 A.3d 1036 (Pa. 2018)).

[215] *Id*. at 356-57.

[216] *Id*. at 360 (citing 159 F.2d 169, 173 (2d Cir. 1947)) ("Where B represents the burden, P represents the probability of harm, H represents the magnitude of

Although the Sedona test is laudable for its utility, reliance on precedent along with industry best practices, and desire to not be either too prescriptive or vague in its terms, there is a concern that the average adjudicator or small business owner—when faced with such a formula—could become even more confused than when reading the list of Top 20 CIS Security Controls. Further, it requires the ability to access quantitative data to fill in values for these variables, which is often not available. This complexity is compounded by the fact that cybersecurity professionals, or software engineers, are not able to implement all of these security controls on their own, but instead require an organization-wide effort to include developers, facilities managers, and senior leadership to make and keep cybersecurity fundamental to a firm's operations. Only then could a decision-maker be able to defend that they crafted "a security program that a reasonably prudent security professional would have implemented."[217]

No single checklist or framework will protect at-risk organizations from the wide variety of cyber threats they face. Rather, each decision should be tailored to the particular cybersecurity needs of a given organization, including its functions, footprint, assets, and customer base.[218] Yet the closer we can get to treating cybersecurity as a commodity, and enhancing certainty over reasonableness, the more we can engender economies of scale and drive down costs. Of course, defining "reasonable" cybersecurity for a given organization is just the first step. A potentially even more daunting problem is demonstrating compliance with that framework or standard, such as in the event of an audit or government investigation, as well as enforcing compliance, and levying penalties when necessary.

C. Implications for Designing Interventions to Improve General Cybersecurity Due Diligence

In addition to their implications for designing reasonableness standards, our results also have some important implications for cybersecurity policymaking in general. Our findings suggest that—to the extent that cyber security decision-makers intend policymaking efforts to build upon existing variation in practices—it may be more useful for them to distinguish between small and medium/large organizations than critical and non-critical infrastructure organizations. While our results did find some

harm, subscript 1 represents the controls (or lack thereof) at the time the information steward allegedly had unreasonable security in place, and subscript 2 represents the alternative or supplementary control.").

[217] Kang, *supra* note 200.

[218] *Id*.

differences across critical and non-critical infrastructure organizations, the differences across small and medium/large organizations were much more pronounced. Going forward, policy-makers may want to consider accounting for the categories when making policy.

Future policy efforts to improve organizational cyber security decision-making may also want to focus on cybersecurity practices by small businesses in particular. Small businesses present a dual problem in cybersecurity: while they have been at the center of several significant cyber incidents, the available data suggests that they engage in less comprehensive cybersecurity practices.[219]

Recent reports have found that 28%[220] of organizations that suffered data breaches were small and medium businesses, but our results echo previous findings that small organizations "have been adopting a very limited approach to cyber security."[221] While our respondents from small organizations reported a lower rate of successful cyber incidents, this may be due in part to not identifying events when they occur. Moving forward, policymakers may want expand current efforts to improve cyber security practices amongst small organizations. Additionally, as small businesses may have further to go towards adopting strong cyber security practices, policymakers may want to include support and incentives for these organizations to avoid unintended consequences, including potential anti-competitive effects should required security practices increase the barriers to starting a small business. For example, the Small Business Administration could support and incentivize small businesses looking to acquire training and financing to improve their digital infrastructure.

VI. CONCLUSION

This Article has investigated attempts at the federal and state levels to define, and enforce, "reasonable" cybersecurity. Drawing on new data in partnership with the state government of Indiana, the paper presents results from a cybersecurity survey to inform how "reasonable" cybersecurity should be interpreted, showing that small and medium-sized businesses were particularly at risk, and confused, as to what cybersecurity best practices to put into place relative to large organizations. This highlights the need for coordinated federal, state, academic, and civil society outreach to

---

[219] *See* Jane Chen, *Cyber Security: Bull's-Eye on Small Businesses*, 16 J. INT'L BUS. & L. 97, 97 (2016).

[220] GABRIEL BASSETT ET AL., VERIZON 2020 DATA BREACH AND INVESTIGATIONS REPORT, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf [https://perma.cc/HE3P-E7FD] (2020).

[221] National Cyber Summit (NCS) Research Track 2021, 49 (Kim-Kwang Raymond Choo et al., eds., 2022).

leaders of small and medium-sized businesses to both educate them about the cyber threats facing their organizations, and equip them with distilled tools they need to defend themselves.