Akron Law Review

Volume 55
Issue 3 *Cybersecurity Symposium Issue*

Article 2

2022

Ohio's Data Protection Act and/as a Process-Based Approach to "Reasonable" Security

Brian Ray

OHIO'S DATA PROTECTION ACT AND/AS A PROCESS-BASED APPROACH TO "REASONABLE" SECURITY

*Brian Ray**

I. INTRODUCTION

Cybersecurity is not uniformly regulated today. Where it exists, regulation is sectoral and inconsistent, making it difficult to improve cybersecurity on a wholesale basis. Until there is a national legal standard, or a national consensus on what that standard may be, we are in a period where organizations are left on their own to decide what constitutes "reasonable" information security practices.

State legislatures are exploring creative ways to address this critical gap. Without the authority to mandate uniform cybersecurity standards, an increasing number of states have pioneered ways to *incentivize* the voluntary adoption of cyber best practices. In 2018 Ohio started this trend with a first-of-its-kind law that, rather than prescribe specific obligations, establishes a legal defense from tort claims in private lawsuits for organizations that *voluntarily* adopt certain widely accepted industry standards like the NIST Cybersecurity Framework and the Center for Internet Security's Critical Security Controls and implement a written information security program.

In September 2016, Ohio's Attorney General created the CyberOhio initiative to help businesses and consumers fight back against data security threats.[1] Two years later, Ohio Governor Jon Kasich signed CyberOhio's first legislative proposal, the Ohio Data Protection Act (the ODPA), into law.[2] The ODPA pioneered a new approach to cybersecurity regulation. Rather than impose specific requirements on organizations covered by the law, the ODPA instead provides an incentive for organizations to voluntarily create and implement cybersecurity programs.

Specifically, the ODPA creates a statutory affirmative defense that an organization may assert against tort claims alleging that a failure to implement reasonable information security standards resulted in a data breach. For an organization to avail itself of the affirmative defense in litigation involving an alleged data breach, it must have implemented a cybersecurity program containing administrative, technical, and physical safeguards and that "reasonably conforms" with one of eleven specified cybersecurity frameworks.[3] Described as a "safe harbor," the Act is intended to give businesses an incentive to voluntarily "invest in strong cyber security controls" allowing consumers to be "confident that their personal information will be better protected."[4]

This essay, based on remarks delivered at the University of Akron Law Review's 2022 Symposium argues that the ODPA, which has become a model for similar laws and legislative proposals in several other states, in effect creates a process-based standard for cybersecurity. It does so by incorporating the risk-based approach used by the listed cybersecurity frameworks as the defacto standard for reasonable security for organizations seeking to qualify for the Act's affirmative defense.

I first summarize the ODPA and then explain the risk-based approach of the cybersecurity frameworks it incorporates. I conclude by arguing that this risk-based approach in effect establishes a process-based definition of reasonable security and explain why that process-based definition offers intriguing possibilities to provide more specific but still

*Leon M. and Gloria Plevin Professor of Law. I am grateful to Katherine Mills and the staff of the University of Akron Law Review for excellent editing assistance.1.Ohio Attorney General's Office, *Attorney General DeWine Launches CyberOhio Initiative to Assist Ohio Businesses*, Press Release, OAG (Sept. 29, 2016), www.ohioattorneygeneral.gov/Media/News-Releases/September-2016/Attorney-General-DeWine-Launches-CyberOhio-Initiat.

2. The Ohio Legislature, *Senate Bill 220, Committee Activity,* www.legislature.ohio.gov/legislation/legislation-committee-documents?id=GA132-SB-220.https://www.ohioattorneygeneral.gov/Business/CyberOhio/Data-Protection-Act

3. O.R.C. 1354 (2018).

4. Ohio Attorney General's Office, *Bill Launched by Attorney General's CyberOhio Initiative Signed Into Law,* (August 3, 2018), OAG, *https*://www.ohioattorneygeneral.gov/Media/News-Releases/August-2018/Bill-Launched-by-Attorney-General%E2%80%99s-CyberOhio-Init.

flexible guidance for organizations seeking to develop defensible cybersecurity programs.

II. ODPA HISTORY AND SUMMARY[5]

A. *ODPA History*

Ohio Attorney General Mike DeWine launched CyberOhio on September 29, 2016, describing it as a collection of cybersecurity initiatives aimed at helping Ohio businesses fight back against data security threats. DeWine announced CyberOhio would focus on five initiatives, including creating an Advisory Board comprised of industry experts and business leaders to advise the Attorney General's office on cybersecurity initiatives and exploring draft legislation "to improve the legal cybersecurity environment in Ohio for businesses and consumers."[6]

The CyberOhio Advisory Board was chaired by Kirk Herath, Vice-President and Chief Privacy Officer at Nationwide Financial Services and included a mix of legal, business and technical experts.[7] The Advisory Board created a Legal Working Group to explore developing draft legislation. That group decided early in its discussions to attempt to craft legislation that would address these issues before a breach occurred, which included creating incentives for organizations of all sizes to proactively address cybersecurity risk.[8] Most organizations in Ohio

5. The history and summary of the ODPA in Section II is adapted from an earlier analysis that I co-authored. *See* Dennis Hirsch, Brian Ray and Keir Lamont, *Promoting Better Cybersecurity: An Analysis of the Ohio Data Protection Act* (Mar. 25, 2019), available at https://www.law.csuohio.edu/sites/default/files/shared/cybersecurity-whitepaper-32819f-1.pdf.

6. Ohio Attorney General's Office, *Attorney General DeWine Launches CyberOhio Initiative to Assist Ohio Businesses*, Press Release, OAG (Sept. 29, 2016), www.ohioattorneygeneral.gov/Media/News-Releases/September-2016/Attorney-General-DeWine-Launches-CyberOhio-Initiat.

7. *Id.* The other original members were: Karen Chamberlain, Chief Information Officer, Western and Southern Financial Group; Jason DeHaan, Chief Information Officer, Abercrombie & Fitch; Robert Giacalone, Senior VP of Regulatory Affairs, Cardinal Health; Candice Hoke, Co-Director, Center for Cyber Security and Privacy Protection, Cleveland State University College of Law; John Hrivnak, Director, Rev1 Labs; Kathy Jobes, Chief Information Security Officer, OhioHealth; Shawn Karasarides, VP-Corporate Counsel, The Wendy's Company; Bob Kozel, Chief Executive Officer, eInformatics; Waylon Krush, Chief Executive Officer, Lunarline; Helen Patton, Chief Information Security Officer, The Ohio State University; Allen Perk, Chief Executive Officer, XLN Systems; Stephen Polenski, Chief Information Security Officer, Battelle Memorial Institute; Harry Raduege, Chairman, Center for Network Innovation, Deloitte; Brian Ray, Co-Director, Center for Cyber Security and Privacy Protection, Cleveland State University College of Law.; Matt Wald, President, Columbus Collaboratory; David White, Chief Information Officer, Battelle Memorial institute; Spence Witten, Director of Federal Sales, Lunarline; Doug Young, System Administrator, United States Department of Energy.

8. I was (and am) a member of the CyberOhio Legal Working Group. This summary is based

already were subject to one or more cybersecurity and privacy-related laws and regulations, including Ohio's security breach notification law in which was enacted in 2006, and so the objective was to avoid simply adding another potentially conflicting regulatory obligation.[9]

The primary challenge was to identify sufficiently flexible but still meaningful criteria that a range of organizations could use to improve their cybersecurity posture without creating a minimum standard or a new regulatory requirement. The group ultimately settled on an approach that rested on three key decisions.

First, rather than attempt to draft a new cybersecurity standard, the legislation should leverage existing legal and regulatory frameworks requirements as well as more general standards on which many of those frameworks were based. This first would allow organizations (and ultimately courts) to draw on history of expertise and knowledge for applying implementing those frameworks. Second, it would avoid unnecessary duplication of effort for organizations already complying with one of these frameworks. The group recognized, however, that none of those standards was perfect or even clearly superior to the others and that several were specifically focused on particular industries and therefore not suitable on their own as a general cybersecurity standard. This would require both some general criteria and also necessarily leave open some significant questions that would ultimately have to be resolved through litigation.

Second, the group sought to ensure that the legislation would not meaningfully diminish consumers' ability to pursue legitimate claims against organizations that failed adequately to protect their information. Limiting the incentive to an affirmative defense would require an organization seeking the protection to bear the burden of producing evidence and proving that it implemented and complied with a reasonable cybersecurity program. Notably, this also could help address the information asymmetry problem that often makes pursuing data breach claims challenging for plaintiffs because it would require the defendant to disclose all relevant details regarding its security program. Equally important, it requires developing a fairly extensive factual record, making it unlikely that the defense would be dispositive at the motion to dismiss stage.

Finally, the draft limited the scope of the defense to tort claims for two reasons. First, it would not want to interfere with any existing

on my personal recollection and notes from these discussions.

9. Ohio Rev. Code Ann. § 1349.19 (LexisNexis 2006).

statutory claims. Second, including some of the contract-based theories that were already emerging as alternative claims in data breach litigation could inadvertently interfere with other contractual rights.

The Act was co-sponsored by Ohio Senators Bob Hackett and Kevin Bacon who introduced it in December 2017.[10] The Senate Government Oversight and Reform Committee held five hearings, and the House Government Accountability and Oversight Committee held three hearings. A total of 17 different witnesses testified at these hearings, 10 who favored passage and seven who opposed it.[11]

Opponents of the legislation raised several objections:

- The listed frameworks are overly flexible and compliance with them will not ensure adequate protection of private information;[12]
- Several of the frameworks are aimed at particular industries and/or not addressed specifically to cybersecurity;[13]
- The affirmative defense will increase litigation costs over what is required to conform with the listed frameworks and whether an organization meets that standard;[14]
- Courts will be required to become experts in data privacy and other technical topics at the motion to dismiss stage;[15]
- The affirmative defense will have a chilling effect on claims by small businesses and financial institutions harmed by a breach;[16]
- To better protect consumer privacy, the bill should include a private right of action for consumers affected by a data breach;[17]

10. Ohio Senate Bill 220, Committee Activity, https://www.legislature.ohio.gov/legislation/legislation-committee-documents?id=GA132-SB-220.

11. *Id*. Several of these witnesses testified at more than one hearing.

12. *See* Matthew Erickson, SpiderOak & The Digital Privacy Alliance, Testimony in Opposition to SB 220, before the Ohio Senate Government Oversight & Reform Committee (May 9, 2018) ("Erickson Testimony").

13. *See* Erickson Testimony, *supra* note 12.

14. *See* Mark Abramovitz, DiCello Levitt & Casey, *Testimony in Opposition to S.B. 220 Before the House Government Accountability & Oversight Committee* (June 26, 2018) ("Abramovitz Testimony"); Curtis Fifner, Ohio Ass'n for Justice, Testimony in Opposition to S.B. 220 Before the House Government Accountability & Oversight Committee (June 26, 2018) ("Fifner Testimony").

15. *See* Abramovitz Testimony, *Testimony in Opposition to S.B. 220 Before the House Government Accountability & Oversight Committee* (June 26, 2018).

16. *Id.*

17. Marc E. Dann, Dann Law, *Testimony in Opposition to S.B. 220 Before the House Government Accountability & Oversight Committee* (June 26, 2018).

- The "restricted information" definition is overly broad and requiring "reasonable conformity" with the specified frameworks sets an "artificially high bar" for organizations seeking the defense.[18]

Several changes were made to the bill as it moved through the legislative process.[19] First, in addition to protecting "personal information" the enacted version includes the category of "restricted information," which extends to any unencrypted information that could be combined "to distinguish or trace the individual's identity or that is linkable to an individual." This addition was made to ensure that organizations would be required to address a sufficiently broad range of sensitive information, including data that could be aggregated to identify individuals even if it did not qualify as "personal information" by itself.

Second, the original bill required "substantial compliance" with the specified frameworks. The enacted version requires an entity to "reasonably conform" to one of the listed frameworks. This was in part a technical correction reflecting the fact that it is not possible to "comply" with the general industry frameworks. The change from "substantial" to "reasonably" was made because the "reasonable" security is the most common standard applied under data protection laws in other states and also the industry standard under the specified frameworks.[20]

B. ODPA Summary

To assert the affirmative defense, an organization must "create, maintain and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards" for the protection of personal information or both personal information and restricted information and that "reasonably conforms to an industry recognized cybersecurity framework," defined in section 1354.02.

This provision requires an organization's cybersecurity program to meet two distinct sets of requirements: (1) the general list of "safeguards" and (2) the requirements of the specific industry framework to which the organization asserts it reasonably conforms. It is no accident that these

18. Jim Halpert, State Privacy and Security Coalition, *Oppose SB220, "Cybersecurity Safe Harbor" Legislation*, House Government Accountability and Oversight Committee (June 26, 2018).

19. Cody Weisbrodt, *Ohio Leg. Serv. Comm. Sub. Bill Comparative Synopsis: Sub. S.B. 220*, 132nd Gen. Assemb. *(House Gov't Accountability and Oversight Comm.)*, at https://www.legislature.ohio.gov/legislation/legislation-documents?id=GA132-SB-220.

20. *See generally*, National Conference on State Legislatures, *Data Security Laws: Private Sector* (Oct. 15, 2018), at http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

general safeguards mirror language contained in most of the specified frameworks, and so it is likely that these two sets of requirements will overlap. For example, the HIPAA Security Rule requires a covered entity to "maintain reasonable and appropriate administrative, technical, and physical safeguards" to protect electronic protected health information.[21] Nonetheless, it's not sufficient for an organization to demonstrate reasonable conformity with the listed frameworks. It also must consider what additional steps are necessary to ensure it has included all of these general safeguards.

Section 1354.02(B) further requires that the program must be designed to protect: (1) "the security and confidentiality of the relevant information"; (2) "against threats to the security or integrity of the information"; and (3) "against unauthorized acquisition of information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates." These requirements reinforce the possibility that an organization will need to analyze cybersecurity risks independently from the framework it selects. One of the concerns leveled at the statute is that some of the listed frameworks, such as GLBA and the portion of the CFR cited in relation to HITECH, are not specifically addressed to specific cybersecurity per se.[22] Even where an organization chooses to demonstrate reasonable conformity under one of those more specific frameworks, however, satisfying these requirements necessarily will involve a more comprehensive analysis of cybersecurity risk.

Finally, section 1354.02(C) states that the "scale and scope" of the program is "appropriate" if it is based on all of the following: the entity's size and complexity; the nature and scope of its activities; the sensitivity of the relevant information; the cost and availability of tools to protect the information; and the entity's available resources. This list reflects the flexibility contained in most of the specified frameworks and requires an organization to calibrate its cybersecurity program to its specific situation. In many situations it will permit smaller organizations with fewer resources to argue that it qualifies for the defense with a less extensive cybersecurity program. Conversely, it imposes a higher burden for larger, better resourced entities. The sensitivity of information and nature and scope of an organization's activities, however, may require a more extensive program irrespective of the size of the organization. The statute

21. 45 C.F.R. § 164.530 (2009).

22. *See* Erickson Testimony, *supra* note 12; Jason Wool, *Ohio Provides Breach Litigation Safe Harbor to Businesses*, ZWILLGENBLOG (October 5, 2020), https://www.zwillgen.com/litigation/ohio-provides-litigation-safe-harbor/

leaves open the question of how to balance these potentially competing factors.

The statute provides three separate options for demonstrating reasonable compliance with an industry framework. First, an organization may demonstrate that its program "reasonably conforms" to the current version of several general industry frameworks. The standards for each framework listed vary to some degree in complexity and specificity of requirements raising the question of why a business would choose to implement a more complex standard. Many organizations that do not already comply with another framework likely will seek to conform to one of the more flexible standards, including the ISO 27000 family and the CIS controls. The ISO 27000 family has the additional potential benefit of an associated certification process, which could make it easier to demonstrate reasonable conformity.

Second, organizations that are "regulated by the state, the federal government, or both" or are "otherwise subject to the requirements of any of the laws or regulations listed in section 1354.03(B)(1)" may demonstrate reasonable conformity with one of those laws or regulations. The Act does not specify what it means to be "regulated" but, as the catchall language "or is otherwise subject to" reinforces, the clear intent of this provision is to limit it only to organizations covered by one of the listed laws. Thus, it would be practically impossible for an organization that does not collect private health information to attempt to conform with HIPPA. As a practical matter that may be the simplest route for such organizations, but the general requirements in section 1354.03 combined with section 1354.03's permission to demonstrate reasonable conformity under any of the three routes suggest that a regulated organization instead could choose to demonstrate conformity with one of the general frameworks.

The third path requires compliance with the current version of the PCI standard and conformity with one of the general cybersecurity frameworks listed in section 1354.04(A). Complying with the PCI standard is a fairly specific process and the Act thus requires strict compliance with that standard. A reasonable reading of this provision is that it will apply where a breach involves PCI-related information requiring an organization seeking to assert the defense to demonstrate compliance with PCI and conformity with another framework to qualify for it.

Certification. Several of the listed frameworks, including the ISO 27000 family, have a third-party certification process available. The Act does not explicitly require certification to demonstrate reasonable conformity with those frameworks, but there are clear benefits to doing so. While obtaining third-party certification will not be sufficient in itself to demonstrate reasonable conformity, at a minimum, it would lay a substantial foundation by providing an objective assessment that an organization's program meets the requirements of the framework. By the same token, failing to seek certification where it's available implicitly would raise doubts regarding whether the program would have met the framework's requirements.

For the frameworks that do not have a standard certification process, demonstrating reasonable conformity is more complicated. Most of these standards provide relatively specific guidance for conducting assessments, but they do not set a definitive standard for compliance. For example, NIST 800-53 emphasizes that compliance requires "using all appropriate information as part of an organization-wide risk management program" and the effective use of "the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations."[23] Implementing these standards thus requires considerable expertise and may require outside assistance.

The Act also does not specify a process for demonstrating that an organization has included the general safeguards and protections listed in section 1354.02 or for certifying that the scale and scope is appropriate. The substantial overlap between these general requirements and the requirements under most of the listed frameworks strengthens the potential value of engaging an independent expert to conduct an assessment and provide an attestation that the program meets both sets of requirements.

Create, Maintain and Comply. Drafting a policy that meets these requirements is only the first step. The organization also must "maintain and comply" with the program. At a minimum, this means that the organization will need to show that it regularly updated the policy in response to changes in its own circumstances as well as changes to the framework it has selected. More importantly, the organization also will need to ensure that the policy is implemented throughout its operations, including third-parties that have access to protected information.

One of the key issues in litigation will almost certainly be whether the alleged breach was a result of an organization's failure to maintain and

23. Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53 (Rev. 5),* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,*)* (Sept. 2020), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

comply with its cybersecurity program. The reasonable conformity standard provides flexibility and recognizes that perfect security is an impossible standard. Thus, even where an alleged breach resulted from the temporary failure of a specific control or requirement under the selected framework, an organization still should be able to argue that it reasonably conformed in the aggregate to the selected framework and/or that the specific failure was not reasonably avoidable. Whether that argument succeeds will turn on the specific facts in each case and how strictly the trier of fact applies the Act's requirements.

This requirement also makes it unlikely that obtaining certification under a specific framework will be dispositive of whether an organization reasonably conformed to it. Some frameworks offer different types of certifications.[24] Certifications that are limited to the program design and do not address implementation clearly will be insufficient to meet this requirement. Even where the certification covers implementation of the policy, however, it will at most reflect the state of the organization at a given point in time. A plaintiff therefore could introduce evidence that the organization failed to maintain continuous compliance following the certification resulting in the alleged breach.

Litigation Issues. The Act structures this protection as an affirmative defense to ensure that the organization asserting it has a qualifying cybersecurity program that bears the burden of providing evidence and proving that the program meets the Act's requirements. Under both the Federal Rules of Civil Procedure and Ohio's Civil Rules, a defendant must assert an affirmative defense in either a pre-answer motion or in a responsive pleading (or an amendment to that pleading).[25]

The option to assert the defense in a pre-answer motion leaves open the possibility that a defendant could seek dismissal of an action on the basis of the defense. Qualifying for the defense, however, will inevitably raise a range of complex factual and legal questions. Resolving these factual issues will require at least some discovery, and so it's unlikely that a court would dismiss a case on this basis.

Either party could move for summary judgment on the question of whether the defense applies. Certification and/or an independent attestation of compliance with the Act's requirements could play a significant role at this stage if a court deems it sufficient to meet a defendant's initial burden of production. This would require the plaintiff

24. *See* Brian P. Bartish and Craig A. Hoffman, *Ohio Law Offers Safe Harbor to Companies Meeting Cyber Standards*, BAKERHOSTETLER, (Aug. 13, 2018), https://www.bakerdatacounsel.com/data-breaches/ohio-law-offers-safe-harbor-to-companies-meeting-cyber-standards/

25. *See* Ohio Civ. R. 8(c), 12; Fed. R. Civ. P. 8(c) and 12.

to identify admissible evidence in the record that the trier of fact could rely on to decide that the organization failed to meet the Act's requirements in spite of that certification/attestation.

As an initial matter, there's a strong argument that a court should require a defendant to provide more than independent certification or attestation of compliance to meet its initial burden because the Act requires continuing maintenance and compliance. It also should not be overly difficult where an alleged breach has occurred for a plaintiff to identify evidence that would demonstrate that there is a genuine issue over facts material to the defense. This makes it likely in most cases that the defense will not dispose of the case at the summary judgment stage.

In theory the defense establishes an alternative path for a defendant to demonstrate that it is not legally liable for the damages caused by the alleged breach. In addition to rebutting the evidence that the plaintiff puts forward to show it violated a reasonable duty of care, the defense allows the defendant to affirmatively demonstrate that its actions met an even higher standard. It may be difficult in practice, however, to effectively distinguish between those two standards given the significant subjective dimension to both and the substantial overlap in the factual issues they implicate.

The technical nature of the factual issues the Act raises almost certainly will require expert testimony on both sides. One of the concerns raised during hearings on the Act and in subsequent commentary is that this will result in increased litigation costs.[26] Data breach litigation typically involves expert testimony regarding many of the same factual questions that the defense raises, including forensic analysis of the incident itself and the extent to which the organization had taken reasonable steps to prevent, resolve and mitigate it.

A related concern is that the availability of the defense under Ohio law and in Ohio courts may create an incentive for both sides to forum shop and lead to increased litigation over choice-of-law and other procedural questions. The defense does not by itself establish a basis either for establishing personal jurisdiction in Ohio or for the application of Ohio law under conflict of laws principles. Thus, while the defense may create a new incentive to litigate where they already are present, it does not create new opportunities to contest those issues.

26. *See* Abramovitz Testimony, *supra* note 14; Fifner Testimony, *supra* note 14.

III. CONCLUSION: ODPA AND PROCESS-BASED REASONABLE SECURITY

A. A Risk Approach to Cybersecurity

Most of the uncertainties identified above are not unique to the Act but rather reflect issues that are inherent in the nature of any cybersecurity risk management process. The practical process of preparing an organization to potentially assert the defense in the event of breach-related litigation is not fundamentally different from the process it should undertake to manage cybersecurity risk from a business perspective.

It is important to emphasize that, while these frameworks differ in scope, complexity and the extent to which they prescribe specific requirements, most are based on the NIST Cybersecurity Framework (NIST CSF).[27] Indeed, most of these frameworks (and NIST itself) provide explicit guidance on how the requirements map to the NIST CSF.[28] Under each of these frameworks an organization applies a list of factors similar to the general ones included in the Act to determine the acceptable level of risk, which then determines the extent and nature of the controls it will implement. While each of the frameworks differ in important ways , the starting point for each is a risk analysis.[29]

The NIST CSF notes that it "is not a one-size-fits-all approach to managing cybersecurity risk," and emphasizes that each organization has "unique risks—different threats, different vulnerabilities, *different risk tolerances*" that will dictate how the implement the Framework.[30] Identifying both an organization's risk tolerance and the measures its cybersecurity program should include to operate within that tolerance requires undertaking some version of a cybersecurity risk assessment. That process first evaluates the security requirements of an organization based on the risk tolerance it identifies and then identifies a range of security controls that the organization could implement to manage that risk in a manner acceptable to the organization. Frameworks like ISO

27. *See* National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure* Version 1.1. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (.

28. *See*, *e.g.*, Center for Internet Security, *CIS Controls Version 8: CIS Controls v8 Mapping to NIST CSF*, https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf; HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework (2016), https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf; National Institute of Standards and Technology, *NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001* (date).

29. NIST Special Publication 800-30, Rev. 1, *Guide for Conducting Risk Assessments* (Sept. 2012) ("NIST 800-30").

30. NIST CSF, *supra* note 29, at vi.

27001 further define processes for implementing and testing the effectiveness of the selected controls as well as to ensure ongoing compliance.[31]

Properly implemented cybersecurity risk analyses will carefully document an organization's rationale throughout the process. This starts with the information used in identifying the organization's risk tolerance and the reasons justifying that tolerance. It also includes analyses of the risks an organization has prioritized and the controls it selects. A complete assessment extends to identifying a consistent process for documenting efforts to implement and comply with the program on an ongoing basis and for updating the program in response to changes in operations and the risk environment.[32]

B. Process-Based Reasonable Security

The ODPA expressly states that it does not create a private right of action and thus does not establish an enforceable cybersecurity standard in Ohio.[33] Nonetheless, the risk-based approach that it incorporates for an organization to qualify for the affirmative defense arguably provides the basis for identifying what is best described as a process-based standard for reasonable security.

A process-based standard for cybersecurity grounded in the risk-based approach these frameworks describe is fundamentally different from both the prevailing maturity model approach and the prescriptive, rules-based approach that some have argued would be more effective in improving the cybersecurity posture of organizations in critical sectors.[34] The maturity model approach to managing cybersecurity risk identifies a generic set of maturity levels, often specific to an industry, typically defined primarily by the range of capabilities an organization has developed.[35] Rather than tailoring the program to each organization's

---

31. ISO 27001.
32. NIST 800-30.
33. Ohio Rev. Code Ann. § 1354.04 (LexisNexis 2018).
34. JIM BOEHM ET AL, *The Risk-Based Approach to Cybersecurity*, MCKINSEY & COMPANY, (October 8, 2019), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-risk-based-approach-to-cybers ecurity distinguishing risk-based approaches from the maturity model); Alexander Dill, *Prescriptive, "Rules-Based" Regulation Is Key to Enhancing Cybersecurity in Financial Institutions*, CHICAGO-KENT FACULTY BLOG (Mar. 10, 2017), http://blogs.kentlaw.iit.edu/faculty/2017/03/10/prescriptive-rules-based-regulation-key-to-enhancing-financial-institution-cybersecurity/ (arguing for rules-based cybersecurity regulations for the financial industry).
35. *See, e.g.,* OSAMAH, M.M. AL-MATARI, et al., *Adopting security maturity model to the organizations' capability model*, 22 EGYPTIAN INFORMATICS JOURNAL 193, 193 (2021).

specific risk profile, this model implies that every organization should work towards achieving the highest maturity level over time and therefore incorporate a similar range of capabilities.

Rules-based approaches to cybersecurity risk likewise rely on a relatively detailed set of specific controls required for compliance. In contrast to the maturity approach, which leaves some room for organizations to self-identify an appropriate maturity level based on their existing risk profile, a pure rules-based approach requires strict adherence to the prescribed measures.[36] Both approaches risk incentivizing overinvestment in a pre-determined set of general controls at the expense of prioritizing identifying and mitigating evolving critical threats specific to an organization.

By contrast, the risk approach embedded in a process-based security standard shifts responsibility from the regulatory authority to individual organizations themselves to identify and prioritize the risks they face and to implement a program designed to mitigate those risks to a level that meets the organization's own desired risk tolerance. This approach defines "reasonable" security not as an externally verifiable set of mitigation measures but instead through the risk assessment process that each organization must use to define for themselves what measures are reasonable in light of their own risk profile and tolerance.

The flexibility of this process-based standard raises the obvious concern that it functionally establishes no standard at all because organizations can set a high risk tolerance and use that to justify adopting a minimalist cybersecurity program. That concern mischaracterizes the nature of risk analysis. Under a process-based standard, organizations aren't free to randomly set their risk tolerance. To satisfy the process-based standard an organization must undertake a comprehensive analysis of its risk environment and justify the risk tolerance it adopts. That justification can be evaluated both pre-breach as part of an external audit and also post-breach to determine whether the organization's analysis appropriately considered and prioritized the threat that resulted in a breach. Rather than simply demonstrating that it implemented certain mitigation measures, under this standard each organization bears the burden of demonstrating that the decisions it made throughout the process were reasonable.

36. *See* FABIO MASSACCI, ET AL., *Economic Impacts of Rules- versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers*, IEEE ECONOMICS OF CYBERSECURITY, Part 2, at 52 (2016).

There's nothing new about risk-based cybersecurity. But the ODPA's affirmative defense changes the mix of incentives under a risk-based approach. The defense shifts the focus from avoiding sanctions to qualifying for a benefit. Anecdotally, discussions with multiple in-house and outside counsel suggest that the ODPA's incentive-based approach helpfully reframes the cybersecurity discussion in a positive way that could help drive resources by providing a perceived benefit to an organization rather than imposing a regulatory cost.

No one has attempted to study the effects of the ODPA, and so we lack hard data about the extent to which this incentive is actually working to incentivize voluntary adoption of cybersecurity programs. The voluntary nature of the ODPA risks organizations simply choosing not to undertake this process altogether. There still is no reported decision where a party asserted the ODPA's defense. This may be due in part to the relatively small number of data breach cases brought in Ohio courts and the fact that many data breach cases settle. Regardless of the reason, the lack of reported decisions suggests that the ODPA's effects likely are modest at best.

The process-based standard the ODPA creates easily could be incorporated into legislation requiring some organizations to develop qualifying cybersecurity programs. While such a law would incorporate aspects of a rules-based approach, it could largely preserve the flexibility inherent in these frameworks for organizations to independently establish their risk tolerance and to develop a program tailored to their specific situations. This approach could offer a more effective mix of risk-based and rules-based approaches to regulating cybersecurity. At least one empirical study suggests that such mixed approach is more likely to lead to more effective cybersecurity programs.[37]

The consumer privacy laws that several states have passed or considered provide useful models. To start, it would make sense to limit the mandatory aspects of a law to larger organizations and/or those in high-risk sectors. Likewise, giving state attorneys general enforcement authority would necessarily limit the scope of enforcement. Legislators could calibrate such a law in various ways that tack towards stronger or weaker enforcement. For example, mandating only reporting with minor or no fines for failure would largely preserve the voluntary nature of the ODPA. Adding audit authority but still limiting sanctions would move further towards a rules-based approach. Both prospective audits and post-breach enforcement would entail precisely the same analysis described

37. *See* Massacci et al., *supra* note 36.

above. Rather than examining whether an organization implemented a pre-determined set of controls, it would be required to defend the decisions made and documented during the process of the cybersecurity risk analysis.

Two other states have adopted laws similar to Ohio's with key differences in each case.[38] Utah's law adds an additional framework and extends the defense to non-tort claims while also excluding it for risks of which an organization had actual notice.[39] Connecticut's legislature chose to limit the affirmative defense to punitive damages claims out of concern that a broad-based defense might provide too much protection to organizations in the case of a data breach.[40] Several other states have introduced similar legislation or are considering doing so. It's thus possible that we may see one or more states experiment with some of the modifications described above. Regardless, if this trend continues and more states adopt some version of the ODPA, we should begin to get more hard data that will enable us to better evaluate whether and how the process-based model of reasonable security works to incentivize more effective cybersecurity.

38. *See* Kayne McGladry, *Three US state laws are providing safe harbor against breaches*, CYBERSECURITY HUB (Sept. 8, 2021), https://www.cshub.com/security-strategy/articles/three-us-state-laws-are-providing-safe-harbor-against-breaches

39. *Id.*

40. *Id.*