wgs

The Sedona Conference

Commentary on a Reasonable Security Test

A Project of The Sedona Conference Working Group
on Data Security and Privacy Liability (WG11)

September 2020
Public Comment Version
Submit comments by November 18, 2020,
to comments@sedonaconference.org

The Sedona Conference Commentary on a Reasonable Security Test

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

SEPTEMBER 2020 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editor-in-Chief
William R. Sampson

Contributing Editors
David Thomas Cohen
Chris Cronin
Hon. Joseph C. Iannazzone
James Pizzirusso
Ruth Promislow
Samuel S. Rubin
Joseph W. Swanson
James Trilling
Hon. Thomas I. Vanaskie (Ret.)

Steering Committee Liaison
Douglas H. Meal

Staff Editors
David Lumia
Michael Pomarico

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the public comment version of The Sedona Conference *Commentary on a Reasonable Security Test* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief William R. Sampson for his leadership and commitment to the project. We also thank Contributing Editors David Cohen, Chris Cronin, Judge Joe Iannazzone, James Pizzirusso, Ruth Promislow, Sam Rubin, Joe Swanson, Jim Trilling, and Judge Tom Vanaskie for their efforts, and Doug Meal for his contributions as Steering Committee liaison to the project. We thank Alyssa Coon and Jim Shook for their contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Commentary* were the subject of the dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by November 18, 2020, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
September 2020

Table of Contents

INTRODUCTION

Objective

This *Commentary* addresses what "legal test" a court or other adjudicative body should apply in a situation where a party has, or is alleged to have, a legal obligation to provide "reasonable security" for personal information, and the issue is whether the party in question has met that legal obligation.

Roadmap

The *Commentary* begins with a brief summary of the importance of having a test, the reasoning behind a cost/benefit approach for the test, and what issues the test does not address. Part I sets out the proposed test and the explanation of how it is applied. Part II provides review and analysis of existing resources that offer guidance on how "reasonable security" has been defined and applied to date and explains how they bear upon the test. It includes a summary review of statutes and regulations that require organizations to provide reasonable security with respect to personal information, decisions of courts and other administrative tribunals with respect to the same, applicable industry standards, and marketplace information. Following this discussion, the *Commentary* identifies those items that are not included in the proposed test (also referenced in the Introduction section) and concludes with a discussion regarding the importance of flexibility.

The Importance of Having a Test

This *Commentary* proposes a reasonable security test. In the course of developing it, the drafters considered whether a "reasonable security" test is even needed.

The reasons are there, and they are important. First, there is no one-size-fits-all cybersecurity program. Different organizations face different data security risks and have different levels of resources available to address those risks.

While approaches such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework provide a helpful structure for identifying protections an organization may need to counter risks particular to its business, few frameworks set out a structure for determining what is "reasonable" in the circumstances—a necessary consideration when adapting such a framework to an organization.

Statutes and regulations require subject organizations to implement reasonable security with respect to the protection of personal information. But here, as well, most of these statutes and regulations require the organization to determine what is "reasonable" in the circumstances. Review of existing laws and regulations[1] found different requirements. Because fewer than half explicitly required a common component, the question of how to determine what is reasonable continues unanswered.

---

[1] Regulation (EU) 2016/679 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 Re-

Certain regulators have tried to address this situation by offering "guidance" to organizations on how to implement reasonable security.[2] Such guidance, however, is not legally binding.[3] Accordingly, organizations that follow (or fail to follow) the guidance would not necessarily be found to have implemented (or to have failed to implement) reasonable security.

Even if it were legally binding, the guidance provides limited instruction on the question of reasonableness. The Federal Trade Commission's (FTC) guidance, for example, provides high-level descriptions of security management programs and specific controls. These controls are by no means comprehensive and cannot account for the many factors that might be pertinent for any given organization.

California's guidance describes the measures specified in the Center for Internet Security's Critical Security Controls as furnishing the minimum security measures that the California Attorney General believed to be necessary ingredients of reasonable security.[4] Yet, because it is keyed to an identified set of 20 controls, the guidance is both cumbersome and static. In sum, regulatory guidance has not provided a test for determining reasonableness.

The importance of a reasonable security test is further underscored by the reported legal cases. Taken together, they indicate "unreasonable" security may be a necessary element of a data security claim; but they do not clearly define "reasonableness." This point is highlighted by the Pennsylvania Supreme Court decision in *Dittman v. UPMC,*[5] where the Court affirmed the pre-existing, 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 in-

---

pealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents; Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. Parts 160 and 164, Subpart C (2002); Federal Trade Commission Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314 (2002)*;* Children's Online Privacy Protection Act (COPPA) 15 U.S.C. §§ 6501–6506 (1998); Standards for the Protection of Personal information of Residents of the Commonwealth (Massachusetts data breach notification law), 201 MASS. CODE REGS. 17.00 (2010); California Consumer Privacy Act, CAL. CIV. CODE § 1798.150(a)(1) (2020); California Customer Records Act, CAL. CIV. CODE § 1798.81.5 (2000); New York SHIELD Act, N.Y. GEN. BUS. LAW § 899-bb; New York Department of Financial Services Regulation, N.Y. COMP. CODES R. & REGS. tit. 23 § 500 (2017); Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000 c. 5, (Can.); Ontario Personal Health Information Protection Act, SO 2004, c. 3; Alberta Personal Information Protection Act, SA 2003, c. P-6.5; British Columbia Personal Information Protection Act, SBC 2003, c. 63; New Brunswick Personal Health Information Privacy and Access Act, SNB 2009, c. P-7.05; Newfoundland Personal Health Information Act, SNL 2008 c. P-7.01; Nova Scotia Personal Health Information Act, SNS 2010 c.41.

2 *See, e.g.*, FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2016); FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015); KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT (2016).

3 *See, e.g.*, Wos v. E.M.A. *ex rel.* Johnson, 568 U.S. 627, 643 (2013).

4 HARRIS, *supra* note 2, at 30–32.

5 196 A.3d 1036 (Pa. 2018).

formation. The imposition of a negligence-based duty to safeguard personal information highlights the utility of a test to assess whether an organization has implemented reasonable security.

Cybersecurity "reasonableness" crosses both legal and technology issues. Reasonable security is a standard that both legal and technology professionals seek to apply. It can be difficult for information technology (IT) organizations to understand how to apply legal concepts to their organizations; it is similarly difficult for lawyers, compliance/risk professionals, and even judges to understand IT well enough to apply it to the legal concepts they know. A reasonableness test would help to bridge that divide.

Having said all of this, the proposed test is not intended to impose on organizations an affirmative legal duty to make one or another information security decision. Instead, the test determines the "reasonableness" of an organization's security measures based on the outcomes—measured by costs and benefits—that reasonably would be expected to flow from whatever information security measures the organization did or did not provide.

A Cost/Benefit Approach: How and Why

The statutes and regulations summarized in this *Commentary* commonly identify the following themes with respect to reasonable security:

- Sensitivity of information: Personal information should be protected by safeguards appropriate to the sensitivity of the information. More sensitive information should be safeguarded by a higher level of protection.

- Cost/benefit analysis: The analysis should include a consideration of the sensitivity of the information, the associated risk of harm arising either from unauthorized access to it or from the deprivation, loss or destruction of the information, the available controls to protect the information, and the cost of those measures to the organization.

The cost/benefit analysis that is embedded in some statutes and regulations weaves together the concept that reasonable security is informed by the sensitivity of information with a second concept: it is important to count the cost of implementing security to the organization relative to the cost of the potential harm of failing to do so. While a cost/benefit approach provides a useful, overall structure, further guidance is important when determining how the themes underlying the cost/benefit analysis should work together in defining reasonableness.

Costs and benefits may come in many forms, relevant both to organizations that are required to implement "reasonable" security measures and to others that are not. Organizations consider these costs and benefits as they design security controls; only later are adjudicators asked to consider the balance between them. The test should accommodate the variety of costs and benefits that should be considered in a cost/benefit analysis, including the utility or benefit of the risk, organizational costs (including financial and operational costs), and harm (including harms that alternative controls

may cause). The test should take these costs and benefits into account not only as to the organization and the claimant in question, but also as to all persons who would incur such costs and benefits, such as the data subjects whose information the organization elects to place at risk.

What the Test Does Not Address or Require

The test does not address other issues that may arise in cybersecurity litigation and regulatory enforcement proceedings, nor does the test require the presence of certain events or items. Those issues, events, and items include the following, all of which are outside the scope of this paper:[6]

1. The test does not mandate particular controls as part of a "reasonable" cybersecurity program.

2. The test does not define "personal information."

3. The test does not require a breach or similar incident to have occurred.

4. Causation in fact is not part of the test.

5. Similarly, proximate cause is irrelevant to application of the test.

6. Although the test addresses the issue of "harm," it does not address the issue of "damages."

7. The test does not address whether any particular information steward has an obligation to maintain "reasonable" security for personal information.

8. Legal fault and liability are not part of the test.

[6] These issues are discussed in more detail at pages 25-27, *infra*.

I. THE TEST

The proposed test for reasonable security is designed to be consistent with models for determining "reasonableness" that have been used in various other contexts by courts, in legislative and regulatory oversight, and in information security control frameworks. All of these regimes use a form of risk analysis to balance cost and benefit. The proposed test provides a practical method for expressing cost/benefit analysis that can be applied in data security regulatory actions, to litigation, and to information security practitioners using their current evaluation techniques. The *Commentary* also explains how the analysis should apply in the data security context. Because the test is rooted in commonly held principles, the drafters believe it offers methods for deriving reasonableness that are familiar to all interested parties. But it should be noted that depending on their text, individual laws or rules that require reasonable security might require use of a different analysis.

Since the organizations addressed in this paper are, by definition, those that have or are alleged to have an obligation to maintain reasonable security for personal information, this *Commentary* refers to them below as "information stewards."

As described below, two particular points warrant acknowledgement: (1) courts have often looked to industry customs to inform a reasonableness analysis;[7] and (2) in some instances, legislatures and regulatory agencies have already identified particular security measures or "controls" to be worth the cost of implementation and have required them.[8] In connection with these two points, this *Commentary*'s position is that evidence of an information steward's noncompliance with an "industry custom" that required a specific security control as to the personal information in question, in a way that increased the risk of a security breach, will be sufficient to establish that the information steward's information-security controls for that personal information were not reasonable. Unreasonableness would remain the conclusion unless the information steward adequately counters the effect of this evidence (1) by questioning the intelligence of the custom, (2) by showing that its operation poses different or less serious risks than those occasioned by others engaging in seemingly similar activities, (3) by showing that it has adopted an alternative method for reducing or controlling risks that is at least as effective as the customary method, or (4) by establishing, through application of the cost-benefit test, that implementation of the industry-custom-required controls in question would have burdened the information steward and others by at least as much as the implementation of the controls would have benefitted the claimant and others.

Evidence of an information steward's noncompliance with a statute, regulation, or ordinance that required implementation of the specific controls for the personal information in question will be sufficient to establish a presumption that the information steward's information security for that

---

7 *See, e.g.*, McDermott v. Connecticut*,* 113 A.3d 419, 428 (Conn. 2015); Brooks v. Beech Aircraft Corp., 902 P.2d 54, 63 (N.M. 1995); Schultz v. Consumers Power Co.*,* 506 N.W.2d 175, 180 (Mich. 1993); Pierce v. Platte Clay Elec. Coop., Inc.*,* 769 S.W.2d 769, 772 (Mo. 1989); and D.L. *ex rel.* Friederichs v. Huebner, 329 N.W.2d 890, 907 (Wis. 1983).

8 *E.g.*, 201 MASS. CODE REGS. 17.04; NEV. REV. STAT. ANN. § 603A.215.

personal information was not reasonable. The force of such a presumption will depend on the application of the governing substantive law, which might include the doctrine of negligence *per se* that many states in the United States have adopted in one form or another. If permitted by applicable law, such presumption could be rebutted if the information steward establishes, by applying the cost-benefit test, that implementation of the legally required controls would have burdened the information steward and others by at least as much as the implementation of the controls would have benefited the claimant and others.

Further, the test addresses the fact that information-security risks stemming from the absence of a control may affect more than just the claimant. The public may have its own risks; even the information steward may have some. The corollary also applies: controls that place burdens on information stewards can place the same or different burdens on the claimant and the public. To deal with this, the test compares the risks and burdens for all parties while protected by the control to the risks and burdens for all parties without the control.

A. Articulation of the Test

An information steward's information security controls for personal information are not reasonable when implementation of one or more additional or different controls would burden the information steward and others by less than the implementation of such controls would benefit the claimant and others.

The test may be expressed as a formula similar to the rule that Judge Learned Hand famously summarized in *United States v. Carroll Towing Co.*:[9]

$B_2 - B_1 < (P \times H)_1 - (P \times H)_2$

Where B represents the burden, P represents the probability of harm, H represents the magnitude of 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.

"Burden" to the information steward and others from implementation of one or more additional controls is the net burden on the information steward and others that likely would result from such implementation. The calculation is the product of the cost or value of such burden and the likelihood of such burden resulting from the implementation of the controls. The burden would include (1) the incremental cost to the information steward and others of implementing the controls in question, (2) the cost or value to the information steward and others of any other lost or diminished, or any gained or increased, utility by reason of the implementation of such controls, and (3) the cost of new threats that may be introduced by the controls.

---

[9] 159 F.2d 169, 173 (2nd Cir. 1947). The *Commentary* provides a detailed consideration of *Carroll Towing* at p. 17, *infra.*

"Benefit" to the claimant and others from implementation of one or more additional controls means the net benefit to the claimant and others that likely would result from such implementation. The calculation is the product of the cost or value of such benefit and the likelihood of such benefit resulting from the implementation of the controls. The benefit would include (1) the incremental value to the claimant and others resulting from the implementation of the controls in question as measured by the magnitude of the harm they would likely incur from unauthorized access to or disclosure or use of the information in question in the absence of the controls, and (2) the cost or value to the claimant and others of any lost or diminished, or any other gained or increased, utility by reason of the implementation of such controls.

An information steward is not responsible for failing to address risks that were neither known nor reasonably knowable at the time of the alleged violation of the duty to provide reasonable security.

B. Explanation of the Test:

1. Controls

The controls being evaluated include the known or reasonably knowable technical, physical, or administrative measures that secure or could secure the personal information in question.

2. Foresight Versus Hindsight

An information steward should not be responsible for failing to address risks that were neither known nor reasonably knowable at the time of the alleged violation of the duty to have in place reasonable security measures. In the analogous product liability context, for instance, courts frequently determine whether a defectively designed product was unreasonably dangerous by applying a risk-benefit analysis based on what was known or reasonably knowable at the time the product left the defendant's control, rather than what is known or reasonably knowable at the time of trial.[10] A similar approach should apply in the data security context.[11]

Accordingly, in assessing the costs and benefits under the proposed test, an adjudicator should look to what was known or reasonably knowable at whatever points in time the information steward al-

---

[10] DAVID G. OWEN & MARY J. DAVIS, OWEN AND DAVIS ON PRODUCTS LIABILITY § 5:33 (4th ed. 2019) ("Almost all courts focusing on the issue in recent years have agreed, rejecting the hindsight test and limiting a manufacturer's responsibility to risks that are foreseeable."); Aaron Twerski & James A. Henderson Jr., *Manufacturer's Liability for Defective Product Designs: The Triumph of Risk-Utility*, 74 BROOK. L. REV. 1061, 1065 (2009) ("most American courts do not hold product sellers responsible for information not available at time of sale"). For an examination of the policy rationales for and against a "time of trial" approach, *see* Guido Calabresi & Alvin K. Klevorick, *Four Tests for Liability in Torts*, 14 J. LEGAL STUD. 585 (1985). In the United States, the courts applying that approach are in the minority. OWEN & DAVIS, *supra*, § 5:33; Twerski & Henderson, *supra*, at 1065.

[11] *See, e.g., Remarks Before the Congressional Bipartisan Privacy Caucus* (statement of Fed. Trade Comm'r Maureen K. Ohlhausen), 2014 WL 585465, at *2 (Feb. 3, 2014) (noting that the FTC, in assessing whether a company's security was "reasonable," "examines factors such as whether the risks at issue were well known or reasonably foreseeable . . . .").

legedly failed to have reasonable security in place.[12] In a case stemming from a data breach, this would normally be the time of the breach.

3. Burden to the Information Steward and Others (Costs)

The "incremental cost to the information steward and others of implementing the controls in question" would include any of the following: the out-of-pocket costs to acquire or create such controls; the labor costs to identify, implement, maintain, and monitor such controls; and the interruption of normal business operations by reason of the foregoing actions. The "cost or value to the information steward and others of any other lost or diminished, or of any gained or increased, utility" would include but not necessarily be limited to the cost or value to the information steward and others of any loss or improvement of quality of service or products by reason of the implementation of the controls in question, the cost or value of any increased or decreased risk to the information steward and others by reason of such implementation, and the harm from unauthorized access to or disclosure or use of the information in question—all to the extent such costs and values have not separately been taken into account in applying the other components of the test.

4. Benefit to the Claimant and Others (Benefits)

The decrease, by reason of the implementation of the controls in question, in the likelihood and/or in the magnitude of the harm the claimant and others[13] would likely incur from unauthorized access to or disclosure or use of the information in question would be determined by taking into account any security risks that would have been reduced by the implementation or maintenance of the additional security controls in question as well as security risks that would have been introduced or increased by implementation of the same controls.[14] The task would be to develop a "net" change in the probability and/or magnitude of harm by reason of the implementation of such controls.

The "harm" to be taken into account here is the harm that is legally actionable under the law applicable to the claim being asserted. The law on what constitutes legally actionable "harm" in the data security context is evolving. Whether and when intangible harms such as emotional distress or inva-

---

[12] If the information steward previously conducted an assessment of its own data security risks, the product of that assessment may include evidence of whether a particular threat or harm was foreseeable.

[13] One might ask why benefits to "others" than the claimant should come into the unreasonableness equation, as doing so might enable a claimant to predicate an unreasonable security claim entirely on the harm that the information steward's information security practices caused or threatened to cause to persons *other than* the claimant. This concern, to the extent it is valid, can be addressed through the legal principles that govern a claimant's standing to make the claim in question and/or the required showing of injury and causation of injury in order to prevail on that claim (all of which are issues beyond the scope of this paper).

[14] A security control may reduce some risks while increasing others. For example, encrypting communications between two computers may safeguard sensitive data. But it may also obscure cyberattacks that are occurring between those computers. Controls that delay authorized users' access to sensitive data may encourage users to share data among themselves. Organizations commonly avoid implementing common safeguards because of other risks they may increase. Such technical and business considerations should be considered in the test.

sion of privacy are actionable, and how such harms would be quantified, are critical questions that are receiving different answers in different courts. The Commentary takes no position on them here. It simply notes that whatever harm is recognized as legally actionable under the law applicable to the claim in question should be considered in the "reasonableness" analysis, as those are the harms the legislatures or the courts have identified as warranting a legal remedy.

The "cost or value to the claimant and others of any lost or diminished, or of any other gained or increased, utility" would include the cost or value to the claimant and others of any loss or increase of quality of service and/or products by reason of the implementation of the controls in question, the cost or value of any increased or decreased risk to the claimant and others by reason of such implementation, and the harm from unauthorized access to or disclosure or use of the information in question.[15]

5. Industry Custom

"Industry custom" refers to a practice that is both generally followed within the relevant industry and sufficiently well known that the information steward may fairly be charged with knowledge of it.[16]

---

[15] While evaluating the risk of a breach—either at the time of the breach or in consideration of alternative or additive controls—an information steward may articulate the utility of its conduct so it may be included in its risk assessment, or presented to an adjudicator for its consideration as it exercises the test.

"Utility" may be understood as a benefit to the public or to an individual that results from the conduct that creates risk. Organizations presumably use personal information to provide a benefit other than their sole enrichment. For example, banks use their customer's personal information to provide beneficial services to their individual customers. These services, and the customer's financial goals, could not plausibly be met without the bank's processing customer personal information. Some personal information can be analyzed, aggregated, or otherwise used to provide a broader public good, such as by schools who educate children, epidemiologists who track and control pandemics, or health-application vendors who provide individual coaching to subscribers based on the outcomes of their large user base.

When an adjudicator applies the test, parties may present an estimation of risk to the utility along with other factors such as costs of controls and harm to others. Adjudicators may evaluate the applicability and use of utility factors based on several criteria, such as whether a plaintiff or the public directly benefited from the conduct that put them at risk, and whether equally available and affordable alternatives presented a lower risk to the plaintiff or the public and therefore reduced the necessity of the information steward's risky conduct.

An adjudicator may properly refuse to credit any forms of utility from the handling of personal information that society does not regard as appropriate, just as an adjudicator hearing an ordinary negligence action may refuse to recognize the feeling of excitement a motorist feels from racing a train towards a highway crossing. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL & EMOTIONAL HARM § 3 cmt. h (AM. LAW INST. 2010).

[16] Further discussion on how courts have defined industry custom in situations where it is used to decide what was "reasonable" is discussed at length at Section II.A.1., p. 15 and pp. 19–21, *infra.* (*See, e.g.,* Silverpop Sys., Inc. v. Leading Market Techs., Inc., 641 F. App'x 849, 852 (11th Cir. 2016)*;* McDermott v. Connecticut, 113 A.3d 419, 428 (Conn. 2015); Brooks v. Beech Aircraft Corp., 902 P.2d 54, 63 (N.M. 1995); Schultz v. Consumers Power Co., 506 N.W.2d 175, 180 (Mich. 1993); Pierce v. Platte-Clay Elec. Coop., Inc., 769 S.W.2d 769, 772 (Mo. 1989); ; D.L. *ex rel.* Friederichs v. Huebner, 329 N.W.2d 890, 907 (Wis. 1983); *In re* City of New York, 522 F.3d 279, 285 (2d Cir. 2008);

Courts have historically seen industry custom not as conclusive, but as a relevant factor in the "reasonableness" inquiry.[17] Industry custom is not merely an indication of whether a practice is cost-efficient; it is also evidence of acceptable, reasonable behavior. And this *Commentary* maintains evidence of it may be offered by either the claimant or the information steward in the reasonableness analysis. Courts often give industry custom significant weight. But a defendant may counter this evidence by questioning the intelligence of the custom, by showing its own operation poses risks that are less serious or altogether different than those posed by others in the same industry, or by showing it has adopted an alternative method for addressing risks that is at least as effective as the customary method.[18]

Evidence of industry custom should be relevant whether offered by the claimant or the information steward. Evidence offered by the claimant that the custom existed, that the custom called for implementation of the control, and that the information steward failed to adhere to the custom should be sufficient to shift the burden to the information steward to justify the lack of the control. Evidence offered by the information steward that an industry custom existed and that the steward adhered to it is likewise relevant. But, as discussed in Comment b to Section 13 of the Restatement (Third) of Torts: Liability for Physical & Emotional Harm, such evidence is not entitled to the same weight. As set out therein, it is conceivable the entire industry has lagged in the implementation of reasonable standards.

Private contractual requirements, such as the Payment Card Industry Data Security Standard or other private contractual standards, to the extent they meet the standard for "industry custom" set forth above, may create an industry custom.[19]

Sours v. Gen. Motors Corp., 717 F.2d 1511, 1517 (6th Cir. 1983); *cf.* U.S. Fid. & Guar. Co. v. Plovidba, 683 F.2d 1022, 1028–29 (7th Cir. 1982); Hoffman v. Enter. Leasing Co. of Minn., LLC, No. A16-869, 2017 WL 1210123, at *4 (Minn. Ct. App. June 20, 2017); *cf.* Friendship Heights Assocs. v. Koubek, 785 F.2d 1154, 1162 (4th Cir. 1986); and Beard v. Goodyear Tire & Rubber Co., 587 A.2d 195, 199 (D.C. 1991)).

17 *See, e.g., McDermott*, 113 A.3d at 428; *Brooks*, 902 P.2d at 63; *Schultz*, 506 N.W.2d at 180; *Pierce*, 769 S.W.2d at 772; *D.L. ex rel Friederichs*, 329 N.W.2d at 907.

18 RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, *supra* note 15, at § 13 cmt. c.

19 Because risk analysis is a common practice in cybersecurity management and is often required by regulations, statutes, and information security frameworks, organizations may have conducted a risk assessment prior to a breach. The results of such *ex ante* risk analysis may be used by those organizations to counter a *prima facie* claim by Complainant, or an expert risk analysis presented by Complainant (although the adjudicator of course will be free to question the accuracy of either party's analysis). In this regard, the cybersecurity community offers many risk-assessment methods that an organization may consider using to evaluate their risks and controls. As of this writing, methods such as the International Organization for Standardization's ISO/IEC 27005, NIST Special Publications 800-30, Center for Internet Security Risk Assessment Method (CIS RAM), Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE), Factor Analysis for Information Risk (FAIR), RISK IT, and Applied Information Economics (AIE) all estimate the likelihood and magnitude of harm and may be used to conduct analysis that is similar to the proposed test.

6. Effect of Violating a Statute, Regulation, or Ordinance

Evidence of an information steward's noncompliance with a statute, regulation, or ordinance that required the implementation of a specific control as to the personal information in question will be sufficient to establish a presumption that the information steward's security for that personal information was not reasonable.

This position finds support in various sources related to the doctrine of negligence *per se*, which has been adopted in one form or another by many states in the United States.[20] Under this doctrine, statutes, regulations, or ordinances applicable to the conduct at issue set the applicable standard of care, and failure to comply is presumptively unreasonable.[21]

Applicable law may make this presumption irrebuttable; and in those situations the adjudicator must follow the law. Where applicable law does not impose that requirement, a rebuttable presumption is better suited to the data security context. Technology and business practices change rapidly.[22] A rebuttable presumption strikes a useful balance. It allows the information steward charged with a violation the opportunity to demonstrate that falling out of technical compliance was reasonable because the costs of achieving such technical compliance would have matched or exceeded the benefits of doing so.[23] If the law allows it, the presumption that arises here should be found rebutted if the information steward establishes, by applying the cost-benefit test, that implementation of the legally required controls would have burdened the information steward and others by at least as much as the implementation of the controls would have benefitted the claimant and others.

---

[20] *E.g.*, RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, *supra* note 15, at §§ 14–15; RESTATEMENT (SECOND) OF TORTS, §§ 286, 288A, 288B (AM. LAW INST. 1965). The California Evidence Code explicitly creates a presumption that may be rebutted with proof that "[t]he person violating the statute, ordinance, or regulation did what might reasonably be expected of a person of ordinary prudence, acting under similar circumstances, who desired to comply with the law[.]" CAL. EVID. CODE § 669.

[21] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS, *supra* note 20, at § 288B(1) ("The unexcused violation of a legislative enactment or an administrative regulation which is adopted by the court as defining the standard of conduct of a reasonable man, is negligence in itself."); Pratico v. Portland Terminal Co., 783 F.2d 255, 265 (1st Cir. 1985) (negligence *per se* "allows the presence of a statutory regulation to serve as irrefutable evidence that particular conduct is unreasonable.").

[22] *E.g.*, *In re* LabMD, slip op. at 14 (F.T.C. Jan. 16, 2014) ("The Commission has long recognized that information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve.").

[23] Negligence is a question ordinarily resolved by the trier of fact, and the strict liability concept of negligence *per se* is an exception. There is a difference among jurisdictions as to whether the presumption created by the violation of a statute or regulation is rebuttable or not. Some larger jurisdictions, such as California, New York, and Georgia, use a rebuttable presumption standard. Some recent literature suggests that negligence *per se* should be abandoned. Barry L. Johnson, *Why Negligence Per Se Should Be Abandoned*, 20 N.Y.U J. LEGIS. & PUB., 247 (2017). Based on these factors, a rebuttable presumption is favored.

We include statutes, regulations, and ordinances alike as potential sources for the presumption. All carry the force of law,[24] and the doctrine of negligence *per se* has recognized all three.[25]

7. Determining Likelihood of Burden and Benefit

A cynic would say that because there is no usable framework for determining probability, the fact finder applying the proposed test will achieve the desired result by plugging in the degree of likelihood necessary to achieve it. In fact, the information security community has broad experience with this. Likelihood of harm can be estimated, for example, using one of several techniques that are provided by the information security community. NIST Special Publications 800-30,[26] ISO 27005,[27] Center for Internet Security Risk Assessment Method,[28] Applied Information Economics,[29] and Factor Analysis for Information Risk[30] all provide guidance for estimation of likelihood or probability.

8. When to Apply the Test

The cost/benefit analysis should be applied as of the time the information steward is or was allegedly violating its obligation to maintain "reasonable" security, and not as of the time the adjudicator is conducting the cost/benefit analysis. In a breach case, that would typically be at the time of the breach. In a case involving an agency accusation of unreasonableness not tethered to a breach, it would be as of the time of the events on which the agency's accusation is based.[31]

---

[24] It is worth noting here that regulatory guidance, policy statements, opinion letters, and the like do not have the force of law. *See, e.g.*, Wos v. E.M.A. *ex rel.* Johnson, 568 U.S. 627, 643 (2013). As a result, violation of such regulatory pronouncements would not trigger the presumption.

[25] *E.g.*, RESTATEMENT (SECOND) OF TORTS, *supra* note 20, at § 288B ("legislative enactment or an administrative regulation"); CAL. EVID. CODE § 669 ("statute, ordinance, or regulation of a public entity").

[26] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST SPECIAL PUBLICATION 800-30 REVISION 1, GUIDE FOR CONDUCTING RISK ASSESSMENTS (2012).

[27] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO/IEC 27005:2018, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—INFORMATION SECURITY RISK MANAGEMENT (2018).

[28] CENTER FOR INTERNET SECURITY, RISK ASSESSMENT METHOD (CIS RAM) ver. 1.0 (2018).

[29] DOUGLAS W. HUBBARD & RICHARD SEIERSEN, HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK (1st ed. 2016).

[30] JACK FREUND & JACK JONES, MEASURING AND MANAGING INFORMATION RISK: A FAIR APPROACH (2014).

[31] In order to apply the test, the parties and the adjudicator will need to consider the question of over what period of time the burden and the benefit are to be measured. To the extent either the burdens or the benefits of the added security measure(s) in question would reasonably be incurred beyond the initial period (*e.g.*, "year one") into a subsequent period (*e.g.*, "out-year(s)"), those reasonably expected benefits and burdens would need to be included in the analysis. Having said that, the methodology by which the "out-year" burdens and benefits are to be factored into the analysis would be determined not by application of a pre-set formula but rather on a case-by-case basis, which would depend on the evidence presented as to the amount and duration of those burdens and benefits, the appropriateness of discounting them to present value, and, if appropriate, the manner of accomplishing such discounting.

9. Availability of Resources

While the test does not directly consider whether the information steward in question had the resources necessary to implement the additional controls that application of the test would require in order for that information steward's data security measures to be found reasonable, the availability of those resources may affect the results of the test indirectly. To explain, the "burdens" included in the test take into account the lost utility that would result from the additional controls. That being the case, if an information steward had insufficient resources to manage a high likelihood and high magnitude of harm, and if the benefit of engaging the risk were low, then the test could result in the additional controls being deemed necessary even where the information steward lacked the resources to implement them . . . and would go out of business trying to do so.

On the other hand, if a similarly under-resourced information steward provided a highly beneficial utility, then the test might demonstrate a commensurately high loss of benefit with the additional controls in place. And this could result in a finding that the information steward was not required to implement the additional controls in order to maintain reasonable security. In other words, it was reasonable to proceed without implementing the controls.

10. Poor Implementation of a Control

There may be instances where the information steward has determined a security control is necessary but has implemented it poorly, or not at all. Indeed, such a fact pattern may occur frequently. The question presented is how the adjudicator applying the proposed test should account for the poor implementation of the control. As an example, this could occur if the information steward had determined enhanced training was required for all individuals handling certain types of data but failed to identify everyone who handled it, leaving out individuals in a given location or business unit. As another example, the information steward may have assigned responsibility appropriately, but the individual charged with implementing the control failed to do it. Under the test, the adequacy of the design is not determinative. Even an excellent design will not protect the information steward where a consideration of the costs and benefits of the failed control shows its proper implementation would have been "worth it." The test satisfactorily addresses this issue.

11. Illustrations of the Application of the Test

To demonstrate the practical utility of the proposed test, three hypothetical illustrations are included in an Appendix. The exemplars do not represent any one case and do not name actual organizations. However, the facts, issues, and causes in each exemplar are common components of breaches in which members of Working Group 11 have been professionally involved.

The reader will note the third exemplar uses quantitative scoring based on the nonquantitative assessments of such things as potential utility, cost, and harm. An adjudicator should first look for quantitative information on both sides of the cost/benefit analysis and should endeavor to apply the reasonable security test using quantitative information. However, information stewards do sometimes resort to nonquantitative inputs in order to conduct a cost/benefit analysis. The *Commentary*

takes no position on how an adjudicator should apply the test in a situation where it does not have quantitative information available, or on whether the adjudicator should do so at all. The third exemplar is included only to illustrate how an adjudicator might apply the test where quantitative information was not available.

II. DISCUSSION

A. The Work That Led to the Test

Extensive, separate reviews of the treatment of reasonable security were conducted in three distinct areas: (1) judicial opinions; (2) statutes and regulations; and (3) the marketplace. A summary of that work follows.

1. Judicial Opinions

A review of judicial opinions in which courts considered the issue of reasonable security highlights the benefits of articulating a test to determine what it is.

In *LabMD v. Federal Trade Commission*, the Eleventh Circuit overturned a cease-and-desist order the FTC had entered requiring LabMD to implement "reasonable" data security.[32] The court held that the "reasonableness" requirement in the FTC's order, which did not specify what measures are "reasonable" or set forth a standard for "reasonableness," was so vague that being subject to penalties for violating it could violate due process: it subjected LabMD to the prospect of being found in violation of the order without having been given fair notice of what conduct is prohibited. The court added it would also be impossible for the FTC to enforce the order as a practical matter. Without a governing standard for "reasonableness," a court would have no way to determine whether LabMD violated the order.

Several earlier data security cases suggested a standard for "reasonable" data security, but only in discrete contexts. In *Federal Trade Commission v. Wyndham Worldwide Corp.*, the FTC asserted what Wyndham did was "unreasonable" and thus "unfair" under Section 5 of the FTC Act. Wyndham responded it lacked fair notice of what data security measures the FTC claimed were "reasonable." Here, the Third Circuit concluded the "unfairness" provision of Section 5 at issue in *Wyndham* provided sufficient notice as to what conduct would comply with its requirements for purposes of Wyndham's motion to dismiss: the text of Section 5 expressly cabins the FTC's authority to declare an act unfair to situations where the act or practice in question "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[33] Finding the statute "informs parties that the relevant inquiry here is a cost-benefit analysis that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity,"[34] the Third Circuit rejected Wyndham's position.

---

[32] No. 16-16270, 2018 WL 3056794, at *7–12 (11th Cir. June 6, 2018).

[33] 799 F.3d 236, 255–59 (3d Cir. 2015) (quoting the statute).

[34] *Id.* at 255.

In *Silverpop Systems, Inc. v. Leading Market Technologies, Inc.*, the Eleventh Circuit held in an unpublished opinion that plaintiff's negligence claim against its service provider, which suffered a cybersecurity breach, failed at the summary judgment stage because the plaintiff "failed to present evidence to establish the applicable standard of care."[35] 'Observing that "evidence of custom within a particular industry, group, or organization is admissible as bearing on the standard of care in determining negligence," the court noted plaintiff failed to identify any "standards that are ordinarily employed in [the defendant's] industry."[36] Accordingly, as the plaintiff "failed to present evidence establishing the standard of care," it could not "establish a breach of the standard of care."[37]

In *Razuki v. Caliber Home Loans, Inc.,* the court held "Razuki could have identified what made Caliber's security measures unreasonable by comparison to what other companies are doing.[38]

Additional decisions have likewise pointed to industry custom or standards as a potentially relevant consideration.[39]

In the context of an order that could subject a party to contempt sanctions for failing to have "reasonable" cybersecurity, *LabMD* suggests "reasonableness" currently has no enforceable meaning. *Wyndham* clarifies that "reasonableness" has meaning to the extent it is the standard for unfairness liability under Section 5 of the FTC Act, since Section 5 itself expressly sets forth a cost/benefit test. *Silverpop* and other private data-security litigation cases show industry standards and/or industry custom play a role in an analysis of "reasonable data security."

In *Dittman v. University of Pittsburgh Medical Center (UPMC)*,[40] the Pennsylvania Supreme Court recognized a negligence-based duty to safeguard personally identifiable information (PII) where the plaintiffs alleged the employer (UPMC) required its employees "to provide certain personal and financial information, which UPMC collected and stored on its internet-accessible computer system without use of adequate security measures, including proper encryption, adequate firewalls, and an adequate authentication protocol." [41]

---

35 641 F. App'x 849, 852 (11th Cir. 2016).

36 *Id.*

37 *Id.*

38 No. 17CV1718-LAB (WVG), 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018).

39 *See, e.g.,* Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 316CV00014GPCBLM, 2016 WL 6523428, at *10 (S.D. Cal. Nov. 3, 2016) (denying dismissal where plaintiffs alleged that defendants "failed to employ reasonable security measures to protect . . . PII, such as the utilization of industry-standard encryption"); *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 119 (D. Me. 2009) ("reasonable" security "might include meeting industry standards"), *aff'd in part, rev'd in part on other grounds sub nom.* Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011).

40 196 A.3d 1036 (Pa. 2018),

41 *Id.* at 16; *but see* Cooney v. Chicago Pub. Sch.*,* 943 N.E.2d 23, 28-29 (Ill. App. Ct. 2010) (no duty to safeguard personal information under Illinois law).

A trio of recent cases from the Northern District of Georgia embraced the view that federal statutes and regulations can provide an ascertainable standard of conduct for state-law claims of negligence *per se*.[42] These cases looked to both Section 5 of the FTC Act and, in one case, to the Safeguards Rule of the Gramm-Leach-Bliley Act as providing an applicable standard of conduct.[43] These cases also found a negligence-based duty under Georgia law to provide reasonable security.[44] An intervening Georgia Supreme Court case appears to negate such a duty but does not affect the Northern District's findings regarding negligence *per se*.[45]

A review of case law where a standard of reasonableness was applied outside the data security context showed two approaches: a cost/benefit test and a consideration of industry custom.

Judge Learned Hand famously summarized the test for reasonableness with his algebraic expression in *United States v. Carroll Towing Co*.[46] *Carroll Towing* considered whether the owner of a barge should be held liable when the barge broke away from its moorings while the bargee was absent. Recognizing there would be occasions when a barge breaks away from its moorings, the potential liability of the barge owner involved the assessment of (1) the probability of the barge breaking away, referred to as "P," (2) the gravity of the loss if the barge did break away, referred to as "L," and (3) the burden of adequate precautions, referred to as "B." Liability would seem to be warranted when B (the cost of adequate precautions) is less than the product of P multiplied by L.

The test in *Carroll Towing* is keyed to applying safeguards that are no more burdensome than the risks they protect against. Thus, the burden of the safeguards must not be greater than the probability and liability of the harmful event. And while the harm from a barge that escapes its moorings is almost always more determinable than the harm from sensitive, personal information that escapes its server, there is nevertheless good reason to believe that the Learned Hand Formula can be usefully applied to both.[47]

---

42 *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019); *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F.Supp.3d 1150 (N.D. Ga. 2019); *In re* Arby's Rest. Grp. Inc. Litig., No. 1:17-CV-0514-AT, 2018 WL 2128441, at *5 (N.D. Ga. Mar. 5, 2018).

43 *In re Equifax*, 362 F. Supp. 3d at 1327; *In re Equifax*, 371 F.Supp.3d, 1173–76; *In re Arby's*, 2018 WL 2128441, at *8; *but see, e.g., In re* Supervalu, Inc., 925 F.3d 955, 963 (8th Cir. 2019) (violation of Federal Trade Commission Act (FTCA) could not establish breach of duty for negligence claim in data breach case part because "Congress empowered the Commission—and the Commission alone—to enforce the FTCA. Implying a cause of action would be inconsistent with Congress's anticipated enforcement scheme.").

44 *E.g., In re Arby's*, 2018 WL 2128441, at *5.

45 Dep't of Labor v. McConnell, 305 Ga. 812, 815–16, 828 S.E.2d 352, 358 (2019).

46 159 F.2d 169, 173 (2nd Cir. 1947)

47 In other cases, Judge Hand questioned, or even rejected, the quantitative test outlined in *Carroll Towing* as being unworkable. *See, e.g., Conway v. O'Brien*, 111 F.2d 611, 612 (2d Cir. 1940), rev'd on other grounds, 312 U.S. 492 (1941). In *Moisan v. Loftus*, 178 F.2d 148, 149–50 (2d Cir. 1949), for example, authored by Judge Hand after *Carroll Towing*, he recognized the "inherent uncertainties . . . in applying such a formula" to an "incommensurable subject matter."

Product liability cases were examined as well. At least one court has rejected the adoption of a strict liability test in the data breach context.[48] Nonetheless, the case law and scholarship associated with product liability cases is useful in supporting a "reasonable security" test resting on a cost/benefit analysis.[49] For example, Section 2 of the Restatement (Third) of Torts: Products Liability provides that a product is defective in design where the foreseeable risks of harm could have been reduced or avoided with a reasonable alternative design.[50] That section, the Restatement continues,

> adopts a reasonableness ("risk-utility balancing") test as the standard for judging the defectiveness of product designs. More specifically, the test is whether a reasonable alternative design would, at reasonable cost, have reduced the foreseeable risks of harm posed by the product and, if so, whether the omission of the alternative design by the seller or a predecessor in the distributive chain rendered the product not reasonably safe.[51]

The case law outside the data security context also recognizes a defendant's compliance with or departure from industry custom is evidence either of due care or negligence but is not dispositive.[52]

This view of industry custom has been adopted by the leading commentators.[53]

But even then, in *Moisan*, he supported the *Carroll Towing* test and observed that, if nothing else, the test is helpful in identifying which of those factor(s) will be determinative in any given case. *Id.* at 149.

This *Commentary* and its proposed test draw inspiration from *Carroll Towing* while noting the difficulties that may arise in a strictly quantitative application of the test. In that regard, the Restatement (Third) of Torts section 3(e), and the accompanying Reporters' Note for section 3(d), use *Carroll Towing*, *Moisan*, and *Conway* as examples of courts' applying the Restatement's proposed cost/benefit approach to negligence determinations. Such authority provides further support for the approach proposed in this *Commentary*.

48 *See In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 119, 125 (D. Me. 2009).

49 *See* Mark A. Geistfeld, *Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability*, 66 DEPAUL L. REV. 385, 399–401 (2016).

50 RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (AM. LAW INST. 2012).

51 *Id.* at cmt. d.

52 *See, e.g.*, McDermott v. Connecticut, 113 A.3d 419, 428 (Conn. 2015) ("The trier of fact is not bound by the industry standard, but rather should consider it in light of the totality of the evidence presented in the case."); *Brooks v. Beech Aircraft Corp.*, 902 P.2d 54, 63 (N.M. 1995) ("We adhere to the principle that evidence of industry custom or usage, and evidence of compliance with applicable regulations, is relevant to whether the manufacturer was negligent or whether the product poses an unreasonable risk of injury, but that such evidence should not conclusively demonstrate whether the manufacturer was negligent or the product was defective."); Schultz v. Consumers Power Co., 506 N.W.2d 175, 180 (Mich. 1993) ("While it may be evidence of due care, conformity with industry standards is not conclusive on the question of negligence where a reasonable person engaged in the industry would have taken additional precautions under the circumstances."); Pierce v. Platte-Clay Elec. Coop., Inc., 769 S.W.2d 769, 772 (Mo. 1989) ("[E]vidence of industry standards is generally admissible as proof of whether or not a duty of care was breached. However, compliance with an industry's own safety standards is never a complete defense in a case of negligence."); D.L. *ex rel* Friederichs v. Huebner, 329 N.W.2d 890, 907 (Wis. 1983) ("Customary practice is not ordinary care but is evidence of ordinary care.").

The Restatement (Third) of Torts: Physical & Emotional Harm states "there is no minority rule," and modern decisions frequently cite Justice Holmes's opinion in *Texas & Pacific Railway Co. v. Behymer*, and Judge Hand's opinion in *The T.J. Hooper*.[54]

While industry custom is not conclusive on the issue of reasonableness, it often has "significant weight."[55] However, a "party who has departed from custom can counter the effect of this evidence by questioning the intelligence of the custom, by showing that its operation poses different or less serious risks than those occasioned by others engaging in seemingly similar activities, or by showing that it has adopted an alternative method for reducing or controlling risks that is at least as effective as the customary method."[56]

In general, industry custom relates to the feasibility and acceptance of alternative measures and whether the defendant was, or should have been, aware of those measures.[57] In addition, if the defendant complied with industry custom, this fact cautions the jury that its ruling on the particular actor's negligence has implications for large numbers of other parties. A companion caution is that the industry "may have been pursing self-interest in a way that has encouraged the neglect of a reasonable precaution."[58]

Industry custom is an important factor the adjudicator would take into account in determining whether the defendant exercised reasonable care. But industry standards are not dispositive.[59]

---

53 *See* RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM, *supra* note 15, at § 13 ("An actor's compliance with the custom of the community . . . is evidence that the actor's conduct is not negligent but does not preclude a finding of negligence. An actor's departure from the custom of the community . . . in a way that increases risk is evidence of the actor's negligence but does not require a finding of negligence."); 57A AMERICAN JURISPRUDENCE 2d, Negligence § 165 (2019) ("[C]ompliance or noncompliance with customary or industry practices is not dispositive of the issue of due care, but constitutes only some evidence thereof."); WILLIAM LLOYD PROSSER & W. PAGE KEETON, PROSSER & KEETON ON TORTS § 33 (5th ed. 1984) ("Much the better view, therefore, is that of the great majority of cases, that every custom is not conclusive merely because it is a custom, that must meet the challenge of learned reason, and be given only the evidentiary weight which the situation deserves. . . . But, as a general rule, the fact that a thing is done in an unusual manner is merely evidence to be considered in determining negligence and is not in itself conclusive.").

54 RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM, *supra* note 14, at § 13 Reporter's Note cmt. b; *see also* Texas & Pacific Ry. Co. vs. Behymer, 189 U.S. 468, 470 ("What usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not."); The T.J. Hooper, 60 F.2d 737, 740 ("Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages.").

55 RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM, *supra* note 15, at § 13 Reporter's Note cmt. c.

56 *Id.*

57 *Id.*, cmts. b & c.

58 *Id.,* cmt. b.

59 *See In re* City of New York, 522 F.3d 279, 285 (2d Cir. 2008) ("Fortunately, we need not reason from a blank slate in applying the Hand formula; we can look to guideposts like industry custom and government regulations in deter-

In the context of contractual relationships, merchants bargain against the backdrop of industry custom, and those customs will be implied in a contract unless the agreement indicates a specific intent to depart from them.[60] Even in tort cases, the existence of a contractual or other special relationship between the plaintiff and the defendant can affect the weight given to industry standards: "The prospect of unreasonable conduct by all potential defendants who engage in a line of activity is especially great when potential victims do not enter into contractual or other consensual relationships with those defendants. By contrast, when potential victims are the patrons of defendants who engage in a particular line of commercial activity, the customs that those defendants accept might be expected to give considerable weight to their patrons' desires."[61] Likewise, in professional malpractice cases, the standard of care is largely defined by professional standards and customs, although industry custom would be given less weight in a products liability case.[62]

The case law also explains what industry practices constitute an "industry custom" for this purpose. William Lloyd Prosser and W. Page Keeton state in Prosser & Keeton on Torts: "A custom, to be relevant, must be reasonably brought home to the actor's locality, and must be so general, or so well known, that the actor may be charged with knowledge of it or with negligent ignorance."[63] That a few members of the industry may use a particular safety measure is not sufficient to show a custom.[64] An industry standard that is not generally followed or that is merely aspirational will not establish industry custom.[65] But neither do industry standards require 100 percent adherence by the industry members in order to become recognized as industry custom.[66]

---

mining the standard of care . . . ."); Sours v. Gen. Motors Corp., 717 F.2d 1511, 1517 (6th Cir. 1983) ("GM's alleged compliance with FMVSS 216, along with its other evidence of adherence to industry customs and standards, was properly left to the jurors to factor into the calculus that comprises reasonable design in a case of strict products liability."); *cf.* U.S. Fid. & Guar. Co. v. Plovidba, 683 F.2d 1022, 1028–29 (7th Cir. 1982) (Posner, J.) (observing that, at least under a no-fault liability regime, industry practice should reflect efficient risk allocation).

60 *See* RESTATEMENT (SECOND) OF CONTRACTS, *supra* note 20, at § 220 cmt. f & § 222.

61 RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM, *supra* note 15, at § 13 cmt. b.

62 *See id.*

63 PROSSER & KEETON, *supra* note 53, at § 33.

64 *See In re City of N.Y.*, 522 F.3d at 285 ("And while the precautions taken by the one ferry operator with ships comparable to the Staten Island Ferry may be prudent, those practices have not become universal enough to suggest an industry custom."); The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) (Hand, J.) ("[H]ere there was no custom at all as to receiving sets; some had them, some did not; the most that can be urged is that they had not yet become general.").

65 *See* Hoffman v. Enter. Leasing Co. of Minn., LLC, No. A16-869, 2017 WL 1210123, at *4 (Minn. Ct. App. June 20, 2017) (unpublished) (expert failed to demonstrate that industry recommendations rose "any higher than best practices" or were "relied on or followed in the rental-car or tire-repair industry").

66 *Cf.* Friendship Heights Assocs. v. Koubek, 785 F.2d 1154, 1162 (4th Cir. 1986) (the standard of care could be shown "through testimony describing steps ordinarily taken" by members of the profession); Beard v. Goodyear Tire & Rubber Co., 587 A.2d 195, 199 (D.C. 1991) (evidence that the merchants' own "procedures conform to those generally used by members of their industry, or at least by many of them" was relevant to the standard of care).

2. Statutes and Regulations

A broad set of U.S., Canadian, Australian, and European privacy legislation was reviewed to identify themes employed there. The review focused in particular on requirements for the protection of personal information that were common across the several statutory regimes.

Here are key findings:

(a) Sensitivity of information: Personal information should be protected by safeguards appropriate to the sensitivity of the information. More sensitive information is expected to be safeguarded by a higher level of protection.

(b) Availability of resources: The size, sophistication, and availability of resources of an information steward can be relevant to what is required in given circumstances.

(c) Cost/benefit analysis: Reasonable security entails consideration of the sensitivity of the information, the associated risk of harm arising from unauthorized access to it or from the deprivation, loss or destruction of the information, the available measures to protect the information, and the cost of those measures to the information steward.

(d) Industry standards: Industry standards may be considered to determine what is reasonable in a particular context.

Examples of legislative requirements that appear throughout the sources include the following:

- Comprehensive, written, information-security program/policies;
- Commitment to protect information through "reasonable" security measures;
- Designation of responsible person(s);
- Performance of risk assessment;
- Restrictions on physical access to personal information;

Courts appear to use terms like "industry custom," "industry standard," and the like interchangeably, or as equivalents. *See, e.g., In re City of N.Y.*, 522 F.3d at 285 (referring to "[c]ustom or standard practice in the industry"); Tzilianos v. N.Y. City Transit Auth., 936 N.Y.S.2d 159, 161 (N.Y. App. Div. 2012) (referring to "an industry standard or a generally accepted safety practice"). For the purposes of this *Commentary*, the term "industry custom" is preferable because it tracks the language used by the Restatement (Third) of Torts: Physical & Emotional Harm. Terms like "industry standard" may imply a formal standard, which is not necessary to establish industry custom, and may not be sufficient to do so. *See* RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM, *supra* note 15, § 13; *see also Hoffman*, 2017 WL 1210123, at *4. Terms like "common practice" are vague and could cover situations in which the practice has been adopted by only a minority of industry members. *See The T.J. Hooper*, 60 F.2d at 740.

- Encryption of sensitive personal information;
- Incident response planning;
- Limiting access privileges to those with a need to know;
- Employee training and compliance monitoring;
- Evaluating and improving the means for detecting and preventing security system failures;
- Disciplinary measures for violations;
- Oversight of the data security practices of third parties, subcontractors, vendors, and the like; and
- Secure user-authentication protocols.

Even where the statutes/regulations set out specific requirements for the protection of personal information, a determination of what is reasonable in a particular circumstance is always required. A "check-here-and-you're-done" form does not exist.

The Ohio Data Protection Act is of great interest. In Ohio, an information steward can claim a "safe harbor" against tort claims if it has "reasonably conformed" with a specified, industry-recognized cybersecurity framework. However, the Ohio Data Protection Act relies on the same factors found in other statutes/regulations. In particular, the Act provides that the scale and scope of a covered information steward's cybersecurity program is appropriate if it is based on all of the following factors:

- Size and complexity of the covered information steward;
- Nature and scope of the activities of the covered information steward;
- Sensitivity of the information to be protected;
- Cost and availability of tools to improve information security and reduce vulnerabilities; and
- The resources available to the covered information steward.

It's important to note that the Ohio Data Protection Act does not specify how these factors are to be prioritized when determining whether the information steward has "reasonably conformed" to the industry-recognized cybersecurity framework. For example, if an information steward has highly

sensitive personal information but limited resources, will it be afforded a safe harbor if it does not implement the entire industry-recognized framework?

Overall, the themes embedded in the statutes and regulations provided useful guidance for assessing reasonable security, but they did not make clear how the several principles should be weighed against each other.

3. Marketplace

Marketplace standards of reasonable conduct in cybersecurity preparedness included the following approaches: (a) mandated minimum controls; (b) prescriptive but flexible controls; (c) standards/frameworks and; (d) open requirements. Here are examples of each:

a. Mandated Minimum Controls:

- The Payment Card Industry Data Security Standard requires specific technical controls for information stewards that handle payment card information.

- The National Institute of Standards and Technology Special Publication 800-171 is a list of required controls that federal contractors must apply when safeguarding "Sensitive but Unclassified" data. These controls are a subset of NIST SP 800-53 and apply to what NIST believes are the most common causes of security concerns federal agencies encounter with their contractors.

b. Prescriptive But Flexible Controls:

- A familiar example is the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which requires covered information stewards to ensure the confidentiality, integrity, and availability of electronic Protected Health Information. But the Rule allows "flexibility of approach" in how that data protection is achieved, based on the information steward's size, complexity, and other factors such as risk.

- The Center for Internet Security Controls (CIS Controls) lays out no fewer than 20 high-level controls, each of which contains subordinate implementation guidance.

c. Standards/ Frameworks:

- Some information security standards provide listings and descriptions of controls. For example, the NIST Cybersecurity Framework (NIST CSF) includes high-level control groupings (Identify, Protect, Detect, Respond, Recover) but does not require specific, technical controls. Instead, NIST CSF subcategories reference specific controls from *other* standards, such as the CIS Controls, ISO 27001, and NIST SP-800-53.

- Other information security standards describe how to analyze information security risks so that controls can be implemented in a way that is reasonable or acceptable for each environment. NIST SP 800-30 and ISO 27005 provide guidance for evaluating controls for their risk acceptability, while the CIS Risk Assessment Method provides guidance for evaluating controls for their reasonableness. Some methods such as Factor Analysis for Information Risk and Applied Information Economics help quantify information security risks.

- The Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (CAT) identifies controls that should be found in commercial and retail banks and organizes them in five different maturity levels. The CAT classifies banks by size, complexity, and volume of business, then indicates the maturity of controls that banks in those classifications should achieve.

d. Open Requirements:

- An excellent example is the European Union's General Data Protection Regulation (GDPR), whose language notes that, "considering the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

- The Australian Essential Eight Maturity Model was developed by the Australian Signals Directorate. The idea of the Essential Eight is to implement a "baseline" of eight cyber-threat mitigation strategies that can be deployed against common threats in a cost-effective way. These include application whitelisting, patching, and restricting administrative privileges. The Essential Eight is a one-size-fits-all approach, which has the benefits of simplicity and broad applicability.

- The U.S. Department of Health and Human Services has published guidance documents ("HHS Guidance") on best practices for health-care information stewards to reduce cybersecurity risks. The HHS Guidance outlines prevalent threats to the health-care industry and identifies best practices to mitigate these threats. The HHS Guidance identifies the following ten specific practices to be considered by an information steward according to its size, complexity and type:

  1. e-mail protection systems

  2. endpoint protection systems

  3. access management

  4. data protection and loss protection

5. asset management

6. network management

7. vulnerability management

8. incident response

9. medical device security

10. cybersecurity policies

The HHS Guidance includes a discussion of specific examples of steps a health-care information steward may take in the context of each of the ten practices but does not identify any framework for assessing what comprises "reasonable security."

B. All the Things "Ruled Out"

As the drafters reviewed and discussed their sources and moved on to developing the proposed test, some things were ruled out. Included were:

1. Specific Controls

This project began and ended with the belief there is not and should not be a one-size-fits-all cybersecurity program. Because application of the proposed test will necessarily depend on the particular circumstances faced by the information steward, mandating particular controls would be inconsistent with a cost/benefit approach.

2. Definition of Personal Information

The proposed test does not seek to define personal information but is intended to be flexible enough to apply to any definition of "personal information."

3. Breach Requirement

Consideration was given to whether a reasonableness test should apply only when a breach or incident has actually occurred. But there are many instances where a determination of reasonableness is important regardless of whether a breach has occurred. In addition, the proposed cost/benefit test does not focus on, nor is it limited to, the occurrence of a breach. Rather, the test focuses on the probability and magnitude of the costs and benefits that would reasonably have been expected to flow from the adoption and implementation of the additional or different security measures under consideration.

4. Causation in Fact

Just as the proposed test does not depend on the presence of a breach, the operation of the cost/benefit analysis is separate from the issue of causation in fact. The cost/benefit analysis addresses reasonably expected costs and benefits with an eye toward the potential for a breach, rather than looking for and focusing on what caused the breach. Indeed, since the test can be applied whether or not there is a breach, it can be applied whether or not causation in fact is an issue that needs resolution.

That causation in fact is not a necessary part of the test becomes concrete where the presence or absence of a particular control is blamed for an incident. Post-incident analyses invariably conclude that implementation of one or more controls could have prevented the incident. But a breach can take any one of many paths. That a brilliant attacker found a new door to walk through should not in and of itself mean the information steward failed to implement reasonable security. Under the test, then, the question is never whether absence of a particular control is to blame for an incident. Instead, the test is always whether, at the time of the incident, the reasonably anticipatable benefits of the control in question outweighed its reasonably expected costs.

Because it was concluded that causation in fact is not necessary to an inquiry into whether the security was reasonable, it was not incorporated as part of the proposed test. Still, in saying that, it is recognized that in many cases the claimant will need to prove the information steward's unreasonable security controls were a but-for cause of the injury on which the claimant's claim is based.

5. Proximate Cause

Consideration of proximate cause was excluded because, like causation in fact, it is irrelevant to application of the cost/benefit test. Again, it is acknowledged that in many cases the claimant will need to prove the information steward's unreasonable security controls were the proximate cause of the injury on which the claimant's claim is based.

6. Damages

The issue of "damages" is not addressed as a component of the test, but "harm" is included. The concepts are related, but different. While proof of actual damages (or for that matter actual harm or injury) is not necessary to application of the cost/benefit test, in many cases the claimant may be able to use such proof. It could establish the magnitude of reasonably foreseeable harm to the claimant and others that was potentially avoidable by implementation of the additional controls in question; and it could establish that the information steward's unreasonable security caused the injury and damages to the claimant.

7. Existence of Obligation to Have "Reasonable" Security

The *Commentary* takes no position as to whether any particular information steward is, in fact, under an obligation to maintain "reasonable" security for personal information. While it is indisputable that some are under such an obligation, that is not clear for all information stewards.

8. Fault/Liability

If the application of the test results in a finding that the information steward did not maintain reasonable security, it does not necessarily follow that the information steward is "at fault" and liable to the claimant, or subject to some adverse finding and penalty by a regulator or court. Legal fault, and any liability that may flow from it, will be determined according to the law applicable to the claim in question. In order for there to be liability under the applicable law, a claimant may need to show fault or other culpability on the part of the information steward in addition to a showing that the information steward's security for personal information was unreasonable. For example, if the information steward acted in response to advice from experienced third-party consultants and attorneys, that "advice of counsel" might provide a complete defense. The *Commentary* takes no position on whether a showing of fault or other culpability on the part of the information steward is required to impose liability on an information steward for failure to have reasonable security for personal information.[67]

C. The Importance of Flexibility

If one accepts there is no one-size-fits-all cybersecurity program, it follows that a reasonableness test must be flexible.

Some of the flexibility factors that were identified include:

1. The Data to Be Protected

As the loss or compromise of different types of data presents different kinds of harm, different levels of protection are appropriate. The source or owner of the data should also be considered. An information steward holding data about others, particularly personal data, must consider the value of that data to the owners and to itself. Maybe the information steward should not hold the infor-

---

[67] On a related but different note, just as the test would not require an information steward to implement a particular control where the burden of doing so is greater than or equal to the benefit to be derived from it, one could argue the steward should still have responsibility in this setting. Under this line of thinking, where the costs of employing a control are $100,000 and the probability-adjusted costs to others from not employing it are $100,000, and the information steward who declines the control is found to have reasonable security . . . but will also have saved $100,000, individuals who are impacted by the absence of the control should be compensated up to the limit of the savings. In response, another could argue that such position would make the information steward a guarantor against some degree of loss, no matter how reasonable its security. While it is not the position of this *Commentary* that the information steward should always have responsibility to a claimant, irrespective of the reasonableness of its security; the *Commentary* acknowledges that such an argument exists.

mation in the first place. If it does hold the information, and if the information is sensitive enough, the information steward may not only be obligated to employ the very highest level of protection but may also have to pay damages no matter how or why the information was compromised—the so-called "plutonium covenant." Conversely, if the data held belongs to the information steward—such as intellectual property—then absent law, regulation, industry standard, or fiduciary obligation to shareholders, the information steward should have considerable flexibility in how to protect it.

2. Threats and Risks

Bad actors have varying levels of sophistication and resources. Protecting against a sophisticated team operating at the nation-state level may well be impossible. Still, as nation states do not threaten the majority of information stewards, threat identification can be an important component of evaluating reasonableness, as it will inform the analysis of what threats were reasonably knowable at the time of the claimed violation, and what threats were not. Such an analysis is important to the application of the proposed cost/benefit test.

CONCLUSION

In the data security space, the reasonableness of a protection has a kind of half-life, and probably a short one. Even regulators concede the point. As set out in the Cybersecurity Requirements for Financial Services Companies:[68]

> Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risk in a robust fashion. [Emphasis added.]

While there is some guidance for assessing reasonable security in the existing judicial opinions, in statutes and regulations, and in the marketplace, the guidance is not uniform and is not always helpful. Further clarity will help custodians of personal information determine whether they have complied with their obligations; and it will assist the courts when they are asked to rule on the efforts to do so. The clarity can be achieved in the form of a test; one keyed to a rigorous analysis of risk.

Risk analysis is particularly appropriate to a consideration of the threats to and the responsibility for data security. Here, the expectations of protection are high and are increasingly endorsed by statute; here, the threats to privacy are real, constant, serious, and rapidly changing; here, the cost of providing the protections can be daunting. Just as how to identify and assess these considerations is important, the actual assessment can be difficult.

For questions of reasonableness concerning the handling of personal information, a test keyed to risk analysis is most likely to yield the right answers, and it is in that context that this test is offered for consideration.

---

[68] N.Y. COMP. CODES R. & REGS. tit. 23 § 500 (2017).

APPENDIX A – Exemplar Cases

The test was applied using the three exemplars below. The scenarios they present do not reflect any one case, and they do not name actual organizations. However, the facts, issues, and causes in each scenario are common components of breaches that the drafters have been professionally involved in.

These scenarios were developed with the intention that they fit the following criteria:

- The breach scenarios should involve facts (controls and causes) that are commonly found in breaches of personal information.
- Each hypothetical information steward's identifying features should not match any organization that any of the drafters worked with relevant to a breach.
- Each scenario should present facts that call for application of each factor of the test.
- Cybersecurity attacks, analysis, vulnerabilities, and alternatives are complex and would be difficult to treat in their full complexity in these exemplar cases. Each exemplar uses facts, descriptions of controls, and descriptions of control alternatives that have been simplified in order to demonstrate the application of the test within a limited space. For the same reason, the exemplars simplify the analysis of harm from a breach. As well, the exemplar cases simplify the litigation process, such as by treating as undisputed inputs that, in a real lawsuit, would be vigorously disputed.
- The estimations, values, and decisions presented in the exemplar cases are not intended to represent actual or normative evaluations or expected outcomes. They are presented for illustrative purposes only.
- The exemplar cases evaluate only the cost/benefit analysis that would be considered in a data breach case and do not address violations of industry custom, regulations, statutes, or ordinances.
- The test is stated as a formula, and there are many approaches an adjudicator could use to arrive at the inputs to be inserted into that formula. That the first two of these exemplars use quantitative information while the third uses nonquantitative information is an acknowledgement only that organizations use both. As the *Commentary* states, an adjudicator should endeavor to use quantitative information if it is available.
- Solely in an effort to illustrate how these varying analysis methods can operate, the test was applied using the Applied Information Economics, Factor Analysis for Information Risk, and Center for Information Security's Risk Assessment Method.

Whether any of these methods, or a different method, should be used is beyond the scope of this *Commentary*.

- Some of the exemplars include risk assessments that were performed *ex ante* by information stewards to determine, as part of their normal security management program, whether their controls were suitable for the risks posed by their information technology environment.

- Although the exemplars provide both quantitative and nonquantitative risk analysis to demonstrate the varieties of risk assessment that may be presented by parties as they advocate for how the test should be applied, the exemplars were carefully created based on risk assessment actually used in the field. The exemplars also assume that the risk assessment was conducted by qualified professionals, with appropriate and available evidence to substantiate their estimates.

- Depictions of *ex ante* risk assessments are not intended to be approved applications of the test. Instead, they illustrate how industry has, in practice, assessed what risk may be prior to or at the time of a breach. Adjudicators in the exemplars reference the *ex ante* risk assessments as evidence of what was reasonably foreseeable at the time of the breach.

- The risk assessment methods employed in the exemplars all have strengths and limitations, and all require an element of subjective estimation and modeling by experts. Yet they have attained legitimacy among practitioners by producing measurable and predictable results. Stated simply, the methods shown in the exemplars have been adopted by government agencies and information security practice organizations because they have proved useful.

- Quantitative risk analysis is useful when all factors are expressible numerically and can be compared to each other in a numerical form. As stated previously, quantitative risk analysis should be used whenever quantitative inputs are available.

- Qualitative (nonquantitative) risk analysis should not come into play unless some factors cannot readily be expressed numerically or cannot be compared to each other when in numerical form. Qualitative risk analysis will be impractical to apply to the test when qualitative inputs are expressed in terms that are not measurable, are arbitrary, are vague, or are not comparable to other inputs.

- These limitations and capabilities are explored by the adjudicators in these exemplars.

- The *Commentary* does not take a position on whether one risk assessment method is better than others. The goal of the exemplars is to illustrate how adjudicators may use different methods as they apply the test.

SCENARIO I: A Vulnerable API at STS

Company: Small Tech Startup, Inc. (STS)

Number of employees: 22.
Revenue: $0 (Venture Capital funded).
Industry: Tech/real estate.
Products/Services: Aggregation of consumer home-loan mortgage data.
Sensitive customer information: Residential home-loan mortgage packages, including detailed and extensive PII for approximately 20 million U.S.-based borrowers.
Network environment: Google Cloud and Amazon Web Services (AWS).

Background:

STS has been in business for 1.5 years. The company collects and aggregates residential mortgage loan data from the major national lenders, which includes full loan packages for tens of millions of borrowers. It sells analysis and a feed of this data, which is purchased by large financial services firms and hedge funds, across a subscription-based Application Programming Interface (API).

Security Posture:

- While tech-savvy and generally aware of information security best practices, the company has no formal information security program. Because of its distributed work force and heavy reliance on cloud-based services, STS's security posture is loosely based on the "zero trust" model, where all access from inside or outside is untrusted until properly authenticated.

- The Chief Technology Officer is responsible for security. She delegates various security operational responsibilities, including patch management and network security, to engineers who are otherwise overworked building the company's products.

- The company has taken steps to secure its AWS environment, including adding controls to prevent unauthorized remote access to the AWS infrastructure.

- STS also encrypts sensitive loan data at rest in its AWS databases; that data is decrypted as needed in response to authenticated requests from the API. API responses are also TLS (Transport Layer Security) encrypted (i.e., encrypted in transit).

- In Q2 2019, the company retained a third-party cybersecurity company to perform a network and application vulnerability scan and penetration test. The findings of that engagement identified a web application vulnerability in the company's main API product.

- The company considered the web application vulnerability to be low priority because it was thought to be exploitable only in rare circumstances that would not occur in a normal production environment. Nonetheless, STS created a plan to remediate the web vulnerabilities after six months' time, when the API was scheduled to be overhauled.

- Besides the technical vulnerability assessment, the company has not otherwise conducted an information security risk assessment.

- Because of pressure from clients and data suppliers, STS has a longer-term plan to formalize its security program to earn an independently verified certification, but that process isn't scheduled to start until next quarter.

The Incident:

On December 3, 2019, an STS employee received an email message from a purported "security researcher" who, in broken English, claimed to have identified and exploited an SQL injection vulnerability in the STS API. The researcher/attacker included a link to a Twitter account that contained screenshots of database tables containing STS's data with the sensitive customer loan information. For a "consulting fee" of 72 Bitcoin (~$250,000) the researcher offered to reveal the API vulnerability to STS and to delete the obtained copy of data.

STS decided to ignore the threat.

Two weeks later, the attacker uploaded a 10-gigabyte dump of STS's sensitive customer information to the website "Pastebin." Security bloggers found the data, and within weeks the breach was making national headlines.

A plaintiffs' class action lawsuit followed. Included in the claims was the allegation that STS failed to properly protect plaintiffs' sensitive personal information that was contained in the loan documents.

The Dispute:

Did STS employ "reasonable security" to protect the personal information it maintained?

The plaintiff argued that although the data was encrypted in storage and in transit, it was presented to the web application as clear text through the API that had a known vulnerability for many months. Further, STS knew that the data was in the hands of hackers who expressed an intent to breach that data if certain demands were not met. STS should have repaired the API immediately when it discovered it was vulnerable during its vulnerability scan.

STS argued it allowed the API vulnerability to continue because it understood the vulnerability was difficult to exploit. As a start-up it had too few resources to address all vulnerabilities, so it scheduled a fix for July 2020 during the API's normal maintenance routine. As for the timing of its re-

sponse to the breach, STS argued that it was investigating the breach to verify that the data came from STS and was discussing with its attorneys whether to pay the ransom, which could have increased incentives for hackers to continue hacking the company and others. The hackers did not give STS deadlines, and STS did not have any means of knowing when or whether any exposure would happen.

The Risk Assessment Method:

In this exemplar, the plaintiff's expert conducts a risk assessment using quantitative, probabilistic methods known as Applied Information Economics (AIE). AIE helps organizations estimate probabilities of harm stated in quantities such as financials, time, populations, degrees of harm, or as binaries. AIE offers multiple, evidence-based methods for experts to express probability using subjective judgment and the data available to them.

As a probabilistic method, AIE may provide results in the form of beta distributions, power law distributions, histograms, scattergrams, or even single values, depending on the question being asked and the availability of data.

Application of the Test:

The adjudicator applies the test by evaluating the claims and evidence.

1. The adjudicator is unable to determine that a time period within which to resolve known vulnerabilities has been established as an industry custom. The adjudicator therefore allows STS and the plaintiff each to present a cost-benefit analysis of the utility of repairing the vulnerability on an emergency basis.

2. The plaintiff's expert conducts a risk assessment of breach, estimating the probability of harm with and without the API repair in place.

    (a) The expert uses information provided by STS to estimate the likelihood of the API being breached and the likelihood and impact of personal information being abused, both when the API's vulnerability is present and when it is not present.

    (b) The plaintiff's expert estimates a probability of a breach and misuse of personal information (meaning that information will be breached and will be used in a manner that harms others) through exploitation of the vulnerable API at 12.2 percent during the period between discovery of and the scheduled fix to the vulnerability (the "at-risk period"). Due to the wide variation of publicly available data about the out-of-pocket expenses that result from a data breach, the expert develops a range of possible breach outcomes and assigns probabilities to those outcomes. In this case, they estimate a likely range of the financial impact to the plaintiff and others from such a breach to be

between $740,000 and $12,225,000.[69] Applying the probability of a breach and misuse occurring (12.2 percent) to the expected range of likely costs to the plaintiff and others from a breach, the expert estimates a probability-adjusted benefit of repairing the vulnerability immediately, rather than in July 2020, as a range from $90,280 to $1,491,450.

(c) The expert next estimates that a probability of a breach and misuse of personal information through the repaired API to be at 1.7 percent during the at-risk period. The estimated likely range of financial impact from such misuse remained between $740,000 and $12,225,000 in the repaired API scenario.

(d) The expert then applies the 10.5 percent (i.e., 12.2 percent minus 1.7 percent) net reduced probability of a breach and misuse occurring if the vulnerability had been repaired immediately to the expected range of likely costs to others of such a breach to estimate a probability adjusted benefit of immediately repairing the vulnerability of from $77,700 and $1,283,625.

(e) The expert then applies the burden side of the test by concluding that STS would have incurred $5,000 of one-time additional burden to repair the API's vulnerability immediately rather than during its normal maintenance period.

(f) Because the $5,000 of burden would thereby have generated a benefit to others of between $77,700 and $1,283,625[70], the plaintiff's expert concludes that STS's security for personal information was rendered unreasonable by API's failure to repair the vulnerability immediately.

3. STS rejects the plaintiff's expert's analysis. STS asserts that had it stopped developing its application long enough to repair the vulnerability out-of-cycle (as an emergency change), it would have risked disruption of functionality of the API for days, which would have reduced the value of STS's clients' use of the API during that time. The utility of the application to STS's financial service provider customers would have suffered.

---

[69] The possibility of disparity in such expert estimates is supported by publications such as Verizon's Data Breach Investigations Report, NetDiligence's Claims Study, and the Ponemon Institute's Cyber Crime Study. Each provides an annual analysis on the costs of cyber breaches, and their estimates vary between $0.58/record to $200/record cost, or higher.

[70] The probable harm without the control was between 12.2 percent x $740,000 and 12.2 percent x $12,225,000, or between $90,280 and $1,491,450. The probable harm with the control was between 1.7 percent x $740,000 and 1.7 percent x $12,225,000, or between $12,580 and $207,825. That yields a benefit between $77,700 and $1,283,625.

(a) STS produces information about daily dollar value of use of the application's features. It estimates $35,000 per day of value enjoyed by its clients.

(b) STS's expert estimates the likelihood of the API being unavailable to STS's clients if it were to have repaired the API as an emergency change. The experts estimate a 59 percent likelihood that the API would have gone down had the repair been attempted; and had that happened, the API would have been down for two days on average (i.e., a 25 percent chance of a one-day outage, a 50 percent chance of a two-day outage, and a 25 percent chance of a three-day outage). Because the API creates $35,000 per day in value to STS's clients, the STS expert calculates $41,300 in expected loss of utility (i.e., $35K x .59 x 2 = $41.3K) because of an emergency repair.

(c) STS agrees that the repair itself would have involved a one-time incremental cost of $5,000 if done on an emergency basis, without consideration of the potential loss in utility of the API if the upgrade failed. STS also does not dispute the plaintiff's estimate that the repaired vulnerability would have produced a 10.5 percent net reduced probability of a breach and misuse occurring during the at-risk period.

(d) STS states that the reduced utility of the API if it failed during an emergency repair ($41,300) should be added to the burden associated with repairing the vulnerability on an emergency basis in applying the test.

4. The adjudicator employs STS's and the plaintiff's experts' analyses in applying the test.

(a) The adjudicator determines that a benefit of between $77,700 and $1,283,625 would have been realized from repairing the API on an emergency basis, with a $5,000 additional cost burden.

(b) The adjudicator also adds to STS's cost burden of repairing the vulnerability immediately the reduced utility of $41,300 associated with doing the repair on an emergency basis, bringing STS's total calculated burden of immediately repairing the vulnerability to $46,300.

(c) ***The adjudicator determines that the one-time added cost burden of $46,300 would have provided a benefit of between $77,700 and $1,283,625, and therefore that STS's failure to repair the API vulnerabil-***

ity immediately rendered its security for personal information unreasonable.[71]

[71] While utility, cost, and benefit can often be quantified, organizations may find it difficult *ex ante*, and adjudicators may find it difficult *ex post*, to evaluate some factors using quantitative information. Factors such as the education of students, the care of patients, development of health science, and the promotion of safety are not as obviously associated with quantitative information as are budgets. Further, court cases such as *Grimshaw v Ford Motor Co* (119 Cal.App.3d 757) and social science research (W. Kip Viscusi, "*Jurors, Judges, and the Mistreatment of Risk by the Courts*, 30 J. OF LEGAL STUD. 107 (2001))" demonstrate negative juror and jurist reactions to a purely quantitative risk analysis. In circumstances where organizations or adjudicators consider quantitative methods to be impracticable, they may feel inclined to consider the possibility of opting for other methods. The third exemplar sets forth a methodology by which a nonquantitative analysis might be done. Alternatively, in circumstances where a quantitative analysis is considered to be impracticable, organizations and adjudicators may conclude the test is unworkable and look instead to industry custom and/or statutory requirements to evaluate the reasonableness of the information steward's data security. The question of whether and to what extent a nonquantitative analysis may be used in such circumstances is beyond the scope of this paper.

SCENARIO II: Advanced Persistent Threat Attack at MMT Labs, Inc.

Company: Medium Medical Testing Labs, Inc. (MMT)

Number of employees: 500.
Revenue: $120 million.
Industry: Health care.
Products/Services: Medical testing services for hospitals and doctors' offices.
Sensitive customer information: Drug testing and other patient health test results going back five years.

Background:

Founded in 2003, MMT operates clinical labs in five states, offering health testing services to hospitals and other health-care providers. It maintains its test results in databases in its secure network environment.

Security Posture:

- MMT has worked hard to improve its security posture over time, formalizing its policies and procedures and implementing controls to achieve and stay in compliance with professional and regulatory requirements.

- MMT maintains a risk-based cybersecurity program that includes regular audits, penetration tests, and corrective actions where noncompliant controls or vulnerable controls were identified.

- Lab test results are maintained in encrypted form in Microsoft SQL Server databases. After five years, records are purged from the databases.

- MMT has a team of eight full time IT personnel, with one person in charge of network security.

- MMT has conducted annual risk assessments using Factor Analysis for Information Risk (FAIR) analysis methods. While many risks were identified, not all information assets or threats had been analyzed. As is common practice, MMT's risk analysis evaluated harm to themselves, including loss of reputation, incurred costs, and regulatory fines that could result from breaches.

The Risk Assessment Method:

MMT has conducted annual risk assessments using Factor Analysis for Information Risk (FAIR) analysis methods. FAIR uses subjective estimates by experts to estimate component factors that

comprise risk, such as the commonality and strength of attacks, the robustness of controls, the diligence of attackers, and multiple factors that contribute to post-incident costs.

The Incident:

On December 24, 2019 a system administrator noticed a large compressed file on the database server called "EXPORT.RAR." The administrator opened the file and found a dump of the database tables in decrypted format.

Further investigation revealed that similar export files had been created on the other database servers, and company firewall logs established that the data had been exfiltrated from the network and were therefore stolen.

Forensic investigators found a database administrator's account had been used to log into the database servers and export the data. They did not discover how the attackers obtained the database administrator's credentials.

The investigators determined that the attackers got into the network via a phishing attack that occurred seven months prior. A billing manager opened an email attachment with a weaponized Excel file that installed hybrid trojan malware on his computer. The malware opened up a port-forwarding back door using PowerShell, allowing the attackers to remotely control his computer, even through the firewall.

From there, the attackers found and cracked the credentials for a domain administrator who had previously logged onto the billing manager's computer; and they used that account to move laterally across the network environment.

Based on the tactics, tools, and procedures used by the attacker, the forensic team believed that MMT had been victimized by a sophisticated Advanced Persistent Threat actor.

MMT reported the breach to the State Attorney General (AG) in each of the five states the identified patients resided in and notified each of the 2.5 million affected patients.

The Dispute:

State Attorneys General allege MMT did not employ "reasonable security" in protecting the patient medical data in its care.

State AGs argued that the unsafe configuration of the billing manager's computer and the cached domain administrator's credentials on that machine permitted the hack to occur. Additionally, MMT's technical audits and penetration tests found these vulnerabilities, yet MMT accepted the risk and left the vulnerabilities in place.

MMT argued that its security program that includes phishing tests, encryption, continuously improved policies, Microsoft Advanced Threat Protection, patch management, etc. demonstrated due diligence. It further argued the billing manager's computer was configured in a weaker state than the others because the billing manager did not access sensitive data, and the computer needed to run a client health network's billing software application, which required a less-secure configuration in order to operate. MMT presented its *ex ante* FAIR risk analysis as evidence during discovery.

Application of the Test:

The adjudicator applies the test by evaluating the claims and evidence.

1. The adjudicator reviews MMT's *ex ante* risk assessment and sees that MMT evaluated the risk posed by the billing manager's less-secure computer. The adjudicator also sees that MMT accepted the risk. While not providing explicit criteria for accepting the risk, MMT explains the computer needed to be in the less-secure state in order to operate a critical billing application.

2. State AGs submit their risk analysis to the adjudicator to estimate the probability of harm with and without the standard protections on the billing manager's computer. State AGs' expert uses FAIR in accordance with MMT's risk assessment methods.

    (a) State AGs' expert estimates the likelihood of the hacker's successful attack and subsequent harm to states' residents as it would have been estimated at the time of the breach and with the billing manager's computer configured in its nonsecured state. Given the known vulnerabilities introduced by the billing software, the State AGs' expert estimates the Loss Event Frequency[72] at 29.2 percent per annum and the Loss Event Magnitude[73] to the states' residents as ranging between $10,500,000 and $60,000,000 at the time of the breach.

    (b) State AGs' expert then estimates the likelihood of the hacker's successful attack and consequent harm had the billing manager's computer been configured as securely as his colleagues' computers. The State AGs' expert estimates the Loss Event Frequency at 1 percent per annum (meaning that enhancing the security on the billing manager's computer would have decreased the probability of harmful abuse of personal information from 29.2 percent to 1 percent, or 28.2 percent, per annum).

---

[72] "Loss Event Frequency" is FAIR's term for per-annum probability of loss when paired with a "Loss Event Magnitude," the amount of the probable loss.

[73] "Loss Event Magnitude is FAIR's term for the sum of losses experienced during a loss event when paired with a "Loss Event Frequency." In essence, it is developed by considering a financial range of possible breach outcomes, and assigning probabilities to those outcomes, in order to create a probability-weighted amount of losses to be caused by an event if the event in fact occurs.

(c) State AGs assert that had MMT made a one-time $1,000 investment to secure the billing manager's computer, that investment would have generated a year-one benefit to their states' residents of somewhere between 28.2 percent x $10,500,000 and 28.2 percent x $60,000,000 (i.e., somewhere between $2,961,000 and $16,920,000).

3. The adjudicator solicits MMT's evaluation of risk at the time of the breach, and the risk had the billing manager's computer been configured similarly to MMT's other systems.

(a) MMT argues that the test should be applied by including the burden that would have resulted had the billing manager not run the health network client's invoicing software. MMT's largest client would only have done business with MMT had MMT used the client's billing software, which could only operate on a computer configured with moderate security controls. Because the billing manager's computer was the only one that was atypically unsecured, MMT agrees with AG's assumption that $1,000 is an appropriate estimate for the one-time cost of applying controls to that one system, including the added labor for doing so.

(b) Additionally, MMT believes that the evidence supporting the risk assessment it conducted prior to the breach should be considered for purposes of determining what the reasonably foreseeable likelihood and magnitude of a breach was at the time of the breach. MMT provides the annual billings from their largest client that it would not have earned had it secured the billing manager's computer and not used the client's billing software. The net profits from these billings average $1,800,000 per year.

(c) MMT produces analysis from its *ex ante* risk assessment showing that (i) enhancement of the billing manager's computer security would reasonably be expected to result in only a 2.7 percent decrease in the per annum probability of a breach that resulted in harm (from 13.2 percent to 10.5 percent) and (ii) such a breach would lead to $10,000,000 in damages to MMT alone (without consideration of harm to others).

(d) MMT presents analysis of risk at the time of the breach by multiplying (i) its 2.7 percent estimate of the per annum decreased likelihood of a breach resulting in harm after enhancing the billing manager's computer security by (ii) the State AGs' estimate that a breach would have resulted in costs to others ranging between $10,500,000 and $60,000,000, to arrive at an estimated year-one benefit from enhancing the billing manager's computer security of between $283,500 and $1,620,000.

(e) MMT then compares its estimated $1.8 million of year-one lost profits from implementing the enhancement to the reasonably expected $283,500-$1,620,000 year-one benefit of implementing the enhancement. It argues that the reasonably expected burden of the enhancement outweighed its reasonably expected benefit, as both would reasonably have been understood prior to the breach.

(f) MMT acknowledges that its prior risk assessment estimated only costs to MMT from a breach that resulted in harm and did not separately estimate the potential costs of a breach to others, including the patients whose PHI was stored by MMT, even though such costs to others were reasonably foreseeable at the time of the estimate and the breach.

(g) MMT also attempts to introduce its utility of producing accurate and fast test results but fails to produce a coherent financial model for that utility. State AGs respond that MMT has competitors who also provide fast and accurate results, so its customers could have used safer alternatives while enjoying the same benefits, rendering the utility claim moot.

4. The adjudicator applies MMT's and State AGs' analysis to the test.

(a) The adjudicator notes that MMT and State AGs agree that, at the time of the breach, the likely harm to the states' residents from such a breach ranged between $10,500,000 and $60,000,000 without consideration of the likelihood of such a breach occurring.

(b) The adjudicator notes that the State AGs and MMT agree that MMT's burden in securing the billing manager's computer in the manner advocated by the State AGs would have been the loss of $1.8 million in net profits in year one.

(c) The adjudicator notes that MMT and States' AGs disagree on the net decreased likelihood of a breach of this sort occurring had the billing manager's computer been secured in the manner advocated by the State AGs.

(d) If the adjudicator finds State AGs' expert's likelihood-of-breach estimates persuasive (perhaps the billing application's vulnerabilities being widely known to the hacking community is a deciding factor) it would apply the test as follows:

(i) The adjudicator would calculate the net year-one benefit of applying additional security to the billing manager's computer by multiplying the range of expected harm from such a breach by the State AG's estimates of the per annum probability of such a breach occurring with,

and without, the billing manager's computer secured in the manner advocated by the State AGs. The adjudicator would therefore conduct multiple calculations.

1) Risk at the time of the breach: 29.2 percent annual likelihood x $10,500,000 = $3,066,000; and 29.2 percent annual likelihood x $60,000,000 = $17,520,000.

2) Risk of a secured billing manager's computer: 1 percent likelihood x $10,500,000 = $105,000; and 1 percent likelihood x $60,000,000 = $600,000.

3) Net year-one benefit from additional security measure advocated by State AGs = from $2,961,000 (i.e., $3,066,000 minus $105,000) to $16,920,000 (i.e., $17,520,000 minus $600,000).

(ii) The adjudicator would compare the year-one benefit range of between $2,961,000 and $16,920,000 to the year-one burden of $1,800,000. ***Based on that comparison, and in the absence of any evidence that the benefit would not exceed the burden after year one, the adjudicator would find that the failure to secure the billing manager's computer in the manner advocated by the State AGs rendered MMT's security for personal information unreasonable.***

(e) If instead the adjudicator finds MMT's likelihood-of-breach estimates persuasive (perhaps MMT's history of penetration tests and audits make a convincing case of MMT's estimate), the adjudicator would apply the test as follows:

(i) The adjudicator would calculate the net year-one benefit of applying additional security to the billing manager's computer by multiplying the range of expected harm from such a breach by MMT's estimates of the per annum probability of such a breach occurring with, and without, the billing manager's computer secured in the manner advocated by the State AGs. The adjudicator would therefore conduct multiple calculations.

1) Risk at the time of the breach: 13.2 percent annual likelihood x $10,500,000 = $1,386,000; and 13.2 percent annual likelihood x $60,000,000 = $7,920,000.

2) Risk of a secured billing manager's computer: 10.5 percent annual likelihood x $10,500,000 = $1,102,500; and 10.5 percent annual likelihood x $60,000,000 = $6,300,000.

3) Net year-one benefit from additional security measure advocated by State AGs = from $283,500 (i.e., $1,386,000 minus $1,102,500) to $1,620,000 (i.e., $7,920,000 minus $6,300,000).

(ii) The adjudicator would compare the year-one benefit range of between $283,500 and $1,620,000 to the year-one burden of $1,800,000. ***Based on that comparison, and in the absence of any evidence that the burden would not exceed the benefit after year one, the adjudicator would find that the failure to secure the billing manager's computer in the manner advocated by the State AGs did not render MMT's security for personal information unreasonable.***

SCENARIO III: Lost Mobile Device at a Research University Hospital

Company: Research University Hospital (RUH)

Number of employees: 4,000.
Revenue: $3.2 billion patient revenue; $350 million research grants.
Industry: Academic medical center.
Products/Services: Patient care, clinical education, medical science research, clinical studies.
Sensitive customer information: Patients' protected health information (PHI).

Background: Founded in 1957, RUH serves its community through direct patient care, supports its affiliated university through clinical education of its medical students, and advances medical knowledge through hard science research and clinical trials.

Security Posture:

- RUH funds its security program comparably to other research universities of similar size. It collaborates with other hospitals, security experts, and regulators to determine, communicate, and improve best practices for securing PHI.

- RUH operates an information security program that conforms to the HIPAA Security Rule. The hospital's risk management program has defined when controls are "reasonable and appropriate" in alignment with the rule. RUH tests and improves its controls and maintains a record of their risks, vulnerabilities, and needs for improvement.

- RUH operates a set of secured mobile devices (tablets) to be used in its public outreach programs. Clinicians regularly visit underserved, remote communities to provide free checkups, examinations, and primary care to patients who cannot afford them. To prepare for these remote visits, clinicians download patient records from the Electronic Health Record (EHR) to a set of tablets, enabling fast, easy access to local patients' records. Access to these records does not require multifactor authentication, but a four-digit password is required to access the tablet's interface. RUH accepted the risks involved in this configuration because access to the EHR and multifactor authentication systems from remote locations is unreliable, and timely access to accurate patient charts is critical for providing safe, effective care.

The Risk Assessment Method:

In compliance with the HIPAA Security Rule, RUH evaluated its risk of potential breaches using a risk assessment. RUH used the Center for Information Security's Risk Assessment Method (CIS RAM), a nonquantitative risk assessment method, to model and prioritize its risks. CIS RAM evaluates risk in terms of an organization's duty of care by evaluating the likelihood and impact of harm

to themselves and others, by delineating between acceptable and unacceptable harm, and by determining whether additional controls are more burdensome than the risks they reduce.

RUH evaluated risk to five factors: its three utilities of patient health outcomes, educating clinicians, and advancing medical science; its objectives to balance its budget; and its obligation to protect the privacy of patients. As it evaluated these risks, it estimated the likelihood of harm in plain-language terms using associated integers (1 through 5) for the likelihood scores and impact scores.

Likelihood scores 1 through 5 used plain-language terms to describe the estimated plausibility and commonality of breaches. Impact scores 1 through 5 indicated degrees of measurable harm that would result from the breaches. Scores of 1 and 2 indicated harms that in its judgment would not require correction or remedy by any party. Score 3 indicated harms that would require some correction or remedy. Score 4 indicated harms that would be potentially severe but recoverable. Score 5 indicated unrecoverable harms such as death, or the hospital's inability to provide the care in question.

RUH's risk assessment determined that multifactor authentication on the tablets would have created a greater risk to the delivery of patient care than any potential harm to patient privacy if the tablets were lost or stolen.

The Incident:

In August 2019, a physician left his tablet behind at a school building where he and a medical outreach team were running a three-day remote clinic. Records for approximately 20,000 patients were stored on the tablet in case any patients from the region attended the clinic. The records were encrypted while stored in the EHR application but were viewable on a one-record-at-a-time basis.

The four-digit passcodes used to access the tablets could have been viewed by patients due to the clinic's public setting.

Once the tablets were accessed, no further credentials were required to access patient records on the local EHR application. This was meant to avoid clinicians being delayed while accessing patient records in critical situations or preventing lockouts when multiple attempts at tapping in complex passwords failed.

Once the physician realized he left his tablet behind, he immediately alerted his IT team and requested that they remotely wipe the device while a member of his staff drove back to the school to retrieve the tablet. But the staff member was not able to locate the tablet when he arrived at the school, the IT team could not confirm the tablet was remotely wiped, and the tablet did not contain a cellular network chip to assist in the recovery or wipe. Rather, it required only a local wi-fi network to connect to the internet.

RUH appears to have complied with the HIPAA Breach Notification Rule. It notified the Department of Health and Human Services Office for Civil Rights (OCR) the day after the tablet was left

behind. Further, RUH informed the patients whose data was on the tablet and provided them with identity theft protection services.

The Center for Medicare and Medicaid Services noted several recent and apparently fraudulent Medicare claims had been made in the names of patients whose PHI was on the outreach clinic tablets.

The Dispute:

The OCR claimed RUH should have used multifactor authentication as a "reasonable and appropriate safeguard" to protect the patients' PHI.

OCR argued multifactor authentication was used to provide access to patient records in all other uses of the EHR, and the tablets were at higher risk of breach due to their mobility.

RUH argued the risk to patients would have been higher had the tablets used multifactor authentication and enforced passwords. The remote location of the clinics and the user interface provided by tablets made it difficult to assure access to PHI if normal access controls were used.

The Test:

The adjudicator applies the test by evaluating the claims and evidence.

1. The adjudicator agrees with OCR's position that multifactor authentication to access patient health records on the tablets would have been industry custom, and that in fact RUH had used multifactor authentication to access the records on other systems, so the technology was known and available to them. The adjudicator therefore determines that OCR has presented evidence sufficient to support a finding that RUH's failure to use multifactor authentication on the tablets rendered its security for personal information unreasonable.

2. The adjudicator then allows RUH to seek to rebut OCR's evidence case by demonstrating that failing to use multifactor authentication on the tablets was reasonable under the test.

3. In an effort to describe the risk of breach from the nonuse of multifactor authentication for the tablets as it was known at the time of the breach, RUH presents its pre-breach risk assessment.

4. The adjudicator determines that RUH's pre-breach risk assessment was not quantitative and asks why RUH used a nonquantitative method to determine the risk of breach.

    (a) RUH states that their multiple utilities—patient health outcomes, educating clinicians, and advancing medical science—were very difficult to quantify in

financial terms, and to do so in a way that retained the meaning of those utilities. Moreover, hospital management was concerned that comparing budgetary impacts to financial representations of the benefits resulting from educated clinicians and advanced medical knowledge would have sent the wrong message to its staff and the community about its multiple missions.

5. RUH offers the adjudicator results from RUH's risk assessment that RUH argues the adjudicator can use to apply the test.

   (a) RUH first presents its analysis of the budgetary costs at the time of the breach of using multifactor authentication on the tablets.

      (i) RUH's experts calculated in their risk assessment that without the multifactor authentication control the risk to RUH's budget was 5 out of 25. This calculation reflected RUH's assessment that not adopting multifactor authentication would certainly (likelihood 5) have had a negligible impact (impact 1) to its budget; the 5 score was the result of multiplying the likelihood score by the impact score (i.e., 5 x 1 = 5).

      (ii) RUH's experts then estimated that with multifactor authentication controls in place, the risk to RUH's budget would have been the same: 5 out of 25 and for the same reasons.

      (iii) With the two scores being the same, RUH's experts concluded that the incremental cost to RUH's budget of employing multifactor authentication on the tablets would have been zero (i.e., 5 minus 5 = 0) at the time of the breach and thus should have no impact on application of the test.

   (b) RUH next presents analysis of the risk of patient privacy harm at the time of the breach, first without and then with multifactor authentication being employed on the tablets.

      (i) RUH's experts calculated in their risk assessment that without the multifactor authentication control, the risk of privacy harm to patients was 8 out of 25. This calculation reflected RUH's assessment that not adopting such authentication would plausibly (likelihood 2) have had redressable privacy impact to thousands of patients (impact 4) whose information may have been exposed one record at a time in the encrypted application. The 8 score was the result of multiplying the likelihood score by the impact score (i.e., 2 x 4 = 8).

(ii) RUH's experts then estimated that with multifactor authentication controls in place, the risk of privacy harm to patients would have been 4 out of 25. This calculation reflected RUH's assessment that, even though upon adopting multifactor authentication a lost or stolen tablet would not be accessible, the patients would still plausibly (likelihood 2) be concerned about their unexploitable privacy, although they would not suffer a particularized or concrete harm (impact 2). The 4 score was the result of multiplying the likelihood score by the impact score (i.e., 2 x 2 = 4).

(iii) Based on this analysis, RUH argues that the net benefit of employing multifactor authentication on the tablets was 4 (i.e., 8 minus 4 = 4) at the time of the breach.

(c) RUH next presents analysis of the risk to patient health outcomes at the time of the breach, first without and then with multifactor authentication being employed on the tablets.

(i) RUH's experts calculated in their risk assessment that without the multifactor authentication control in place on the tablets, the risk to patient health outcomes would have been 5 out of 25. This calculation reflects RUH's assessment that not adopting multifactor authentication would certainly (likelihood 5) have had a negligible impact (impact 1) to patient health outcomes; the 5 score was the result of multiplying the likelihood score by the impact score (i.e., 5 x 1 = 5).

(ii) RUH's experts then estimated that with multifactor authentication controls in place, the risk to patient care outcomes would have been 12 out of 25. This calculation reflects RUH's assessment that in rural environments where internet connectivity is not reliable, multifactor authentication communications would not be reliable either, with the result being that physicians would occasionally (likelihood 3) not gain access to patient records and would misdiagnose or erroneously provide harmful treatments to patients that worsen health outcomes short of permanent damage or death (impact 4). The 12 score was the result of multiplying the likelihood score by the impact score (i.e., 3 x 4 = 12).

(iii) Based on this analysis, RUH argues that at the time of the breach the net burden of employing multifactor authentication on the tablets was '7' (i.e., 12 minus 5 = 7) in terms of patient health-care outcomes and 0 in terms of its impact on RUH's budget, for a total burden of 7.

(d) RUH then argues that its failure to employ multifactor authentication on the tablets did not render its security for personal information unreasonable under the test because 7 is greater than 4.

(e) OCR challenges RUH's proposed application of the test on the following grounds: (i) RUH's methodology for calculating the net benefit of employing multifactor authentication on the tablets does not provide a reliable estimate of that net benefit, as it is entirely the product of RUH's own subjective qualitative value judgments and RUH's arbitrary formulas for quantifying and comparing those judgments; (ii) RUH's methodology for calculating the net burden of employing multifactor authentication on the tablets does not provide a reliable estimate of that net burden, as it too is entirely the product of RUH's own subjective qualitative value judgments and RUH's arbitrary formulas for quantifying and comparing those judgments; and (iii) even if they did yield reliable estimates of net benefit and net burden, RUH's methodologies for determining net benefit and net burden differ from one another so fundamentally in regard to the subjective qualitative value judgments and the formulas on which they are based that the output of one methodology (here '4') cannot be compared to the output of the other methodology (here '7') for purposes of comparing the benefits and the burdens of an additional security measure.

6. If the adjudicator rejects OCR's challenges to RUH's application of the test, and instead concludes that RUH's methodologies for calculating the net benefit and net burden of employing multifactor authentication on the tablets provide a reliable estimate of that net benefit and net burden that are themselves reliable and may reliably be compared to one another for purposes of applying the test, the adjudicator would apply the test as follows:

(i) The adjudicator would first determine the incremental benefit of employing multifactor authentication on the tablets from the reduction of privacy harm to patients achieved by the use of such authentication. The risk score for harm without multifactor authentication was 8, while the risk score for harm with multifactor authentication was 4. The incremental benefit, therefore, would be $8 – 4 = 4$.

(ii) The adjudicator then would determine the incremental burden of employing multifactor authentication on the tablets from the impact on RUH's budget of adopting such authentication and increased risk to patient care outcomes caused by its use. The budgetary impact score was 5 both with and without multifactor authentication, so the incremental budgetary impact of adopting it for the tablets would be $5 – 5 = 0$. The risk score for patient care outcomes with multifactor

authentication was 12, whereas the risk score for patient care outcomes without it was 5, so the incremental burden to patient care outcomes caused by the use of multifactor authentication, therefore, was 12 – 5 = 7.

(iii) Because the use of multifactor authentication on the tablets has greater incremental burden (7) than it has incremental benefit (4), the adjudicator therefore concludes that RUH's failure to use multifactor authentication on the tablets did not render its security for personal information unreasonable.