FOLEY

FOLEY & LARDNER LLP

September 2019 Midwest Cyber Security Alliance Meeting

Thursday, September 12, 2019

5:00 p.m. – 7:00 p.m. CT

MIDWEST CYBER SECURITY ALLIANCE

Visit **www.midwestcyber.org/sign-up** to join today and receive communications about other MCSA news and events, plus access to members-only content online

FOLEY

FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

State Data Breach Notification Laws

This chart should be used for informational purposes only because the recommended actions an entity should take if it experiences a security event, incident, or breach vary depending on the specific facts and circumstances. Further, data breach notification laws change frequently. The chart is a summary of basic state notification requirements that apply to entities who "own" data. This chart does not cover non-owners of data. If you do not own the data at issue, consult the applicable laws and contact legal counsel.

This chart also does not cover:

- Exceptions based on compliance with other laws, such as the Health Insurance Portability and Accountability Act (HIPAA) or Gramm-Leach-Bliley Act (GLBA).
- Exceptions regarding good faith acquisition of personally identifiable information (PII) by an employee or agent of an entity for a legitimate purpose of the entity, provided there is no further unauthorized use or disclosure of the PII.
- Exceptions regarding what constitutes PII, such as public, encrypted, redacted, unreadable, or unusable data. The chart indicates whether a safe harbor may be available for data that is considered public, encrypted, redacted, unreadable, or unusable, but the specific guidance will vary based on the circumstances. For example, some states have a safe harbor only for data that is encrypted, whereas other states may have a safe harbor for data that is encrypted or public.
- The manner in which an entity provides actual or substitute notification (e.g., via email, U.S. Mail, etc.).
- Requirements for the content of the notice.
- Any guidance materials issued by federal and state agencies.
- A comprehensive assessment of all laws applicable to breaches of information other than PII.

This Chart is Current as of July 1, 2019.

For more information about state data breach notification laws or other data security matters, please contact your Foley attorney or the following:

Chanley Howell
Partner, Jacksonville
904.359.8745
chowell@foley.com

Michael Overly
Partner, Los Angeles
213.972.4533
moverly@foley.com

Jennifer Rathburn
Partner, Milwaukee
414.297.5864
jrathburn@foley.com

Aaron Tantleff
Partner, Chicago
312.832.4367
atantleff@foley.com

Jennifer Hennessy
Senior Counsel, Madison
617.502.3211
jhennessy@foley.com

Steven Millendorf
Senior Counsel, San Diego
858.847.6737
smillendorf@foley.com

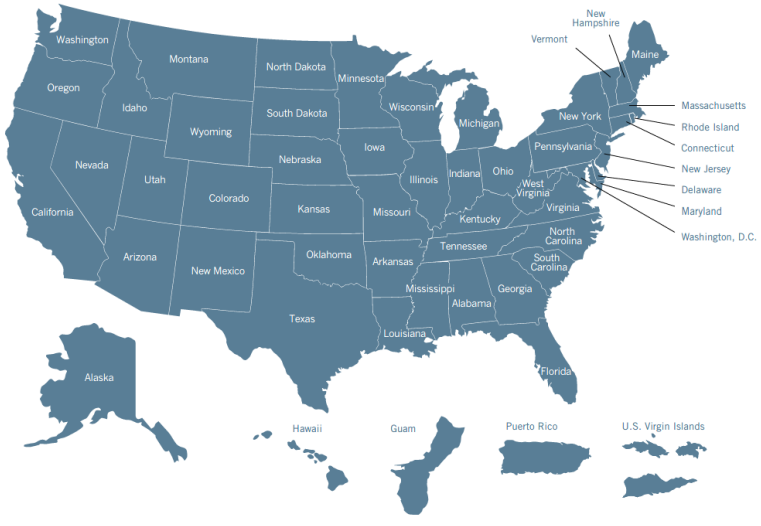
Thomas Chisena
Associate, Boston
617.502.3224
tchisena@foley.com

Samuel Goldstick
Associate, Chicago
312.832.4915
sgoldstick@foley.com

The chart does not constitute legal advice or opinions. The receipt and/or review of this chart do not create an attorney-client relationship.

Full chart available for download at: www.foley.com/state-data-breach-notification-laws

FOLEY
FOLEY & LARDNER LLP



FOLEY
FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

State of Residence	Wisconsin
Statute	Wis. Stat. § 134.98
Definition of "Personal Information"	Individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted or altered in a manner that renders the element unreadable: (1) Social Security number; (2) driver's license number or state ID number; (3) the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (4) the individual's deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a); or (5) individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
Definition of "Breach"	(1) If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. (2) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information.
Analysis of Risk of Harm	Notice is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice shall be made within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required for any period of time and the notification process required shall begin at the end of that time period. If an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.
Notifications to Regulators[2]	Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to 1,000 or more individuals.
Enforcement/Private Cause of Action/ Penalties[3]	Failure to comply is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

Thank You to Our Co-Sponsor

HALOCK®
Purpose Driven Security

halock.com

FOLEY
FOLEY & LARDNER LLP

The California Consumer Privacy Act (CCPA)

Applicability, Requirements, and Practical Tips on Compliance

Presenters

MODERATOR:

Jennifer Rathburn
Partner
Foley & Lardner LLP

Jennifer Hennessy
Senior Counsel
Foley & Lardner LLP

Terry Kurzynski
Senior Partner
HALOCK

Agenda

- Overview
- Scope of the CCPA
- Consumer Rights
- "**Reasonable** Security"
- Pending CCPA Amendments
- Penalties/Potential for Litigation
- Summary: How to Prepare for CCPA

FOLEY
FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

Overview

California Consumer Privacy Act (CCPA)

- Passed on June 28, 2018
- Gives "consumers" (i.e., CA residents) broad rights to access and control of their personal information
- Similar to the EU GDPR, including a new and very broad definition of what is included in protected personal information
  - However, there are also some key differences from the GDPR

Key Points

Effective: 1/1/20
Enforced: 7/1/20

More amendments expected before January

California Attorney General will issue implementing regulations

High Level Requirements

- Implement reasonable security measures
- Privacy notice requirements
- Consumer right to access data
- Consumer right to deletion
- Consumer right to opt-out of sale of personal information
- Prohibition on discrimination against consumers who exercise their rights
- Contractual requirements with service providers

FOLEY
FOLEY & LARDNER LLP

Scope of the CCPA

FOLEY
FOLEY & LARDNER LLP

Who Does the CCPA Apply To?

For-profit businesses that **do business** in CA, collect **consumers' personal information**, and determine the purposes and means of processing (alone or jointly)

50,000
Buys or sells personal information of 50,000+ California consumers, households, or devices per year

$25 million
Annual gross revenues in excess of $ 25 million (worldwide)

50% or more
50% or more of annual revenues derived from selling California consumers' personal information

Definition of Personal Information (PI)

Broadly defined as any information that relates to, describes, is capable of being associated with, or could reasonably be linked to a particular consumer or household. It includes, without limitation:

Real name, alias, postal address

Email address, IP address, browsing history, search history, interaction with website, application, or advertisement

Commercial information: records of personal property, products, or services purchased, or considered, or other purchasing/consuming history

Geo-location data

SSN, drivers license number, passport number

Professional or employment-related information

FOLEY
FOLEY & LARDNER LLP

Exemptions from the CCPA

Exempt Entities

- Non-profit entities that are neither controlled by, nor share common branding with, a business to which the CCPA does apply
- A provider of health care governed by California's Confidentiality of Medical Information Act ("CMIA") or a covered entity governed by HIPAA *to the extent the provider or covered entity maintains patient information in the same manner as medical information or PHI, respectively*

Excluded Data

The following types of data are excluded from CCPA, but an organization may still be subject to CCPA obligations for activities related to other types of data it collects, processes, sells or discloses

- PHI collected by a HIPAA covered entity or business associate
- Medical information governed by the CMIA
- Clinical trial data
- Information collected, processed, sold, or disclosed pursuant to the GLBA, CFIPA, or DPPA
- Information that is deidentified or part of aggregate consumer information
- Sale of PI to or from a consumer reporting agency in certain circumstances

FOLEY
FOLEY & LARDNER LLP

15

Definition of a Service Provider

For-profit legal entity that processes PI on behalf of a business and to which the business discloses a consumer's PI for a business purpose pursuant to a written contract, which:

- Prohibits the recipient from: (1) selling the PI and (2) retaining, using or disclosing the PI outside of its direct relationship with the business and for any purpose other than that of performing the services provided for by the contract
- Includes a certification that the recipient understands these restrictions and will comply with them.

Definition of a Third Party

- A third party is any individual or entity that is not a business or a service provider but still receives PI from a business.
  - Third parties cannot sell PI about a consumer sold to it by a business unless the consumer has received explicit notice and is provided an opportunity to opt-out of the sale.

Service Providers vs. Third Parties

- Situations in which a business is using a "third party," not a "service provider":
  - No written contract exists between the business and the vendor.
  - A contract exists, but it allows the vendor to (1) retain, use, or disclose PI outside the direct business relationship between the business and service provider (i.e., to provide the services specified in the contract) or (2) sell PI.

Service Providers vs Third Parties (cont.)

Absent a written CCPA-compliant contract, a vendor will be treated as a "**third party**" for purposes of disclosures and other obligations

↓

Consumers may not opt-out of disclosures of their PI to service providers (only third parties)

↓

A business must direct its service providers to delete a consumer's PI from their records upon receipt of a verifiable request from the consumer

↓

Businesses *generally* insulated from liability for violations of the CCPA committed by their service providers (but not necessarily third parties)

FOLEY
FOLEY & LARDNER LLP

Consumer Rights under CCPA

Consumer Rights - Overview

- Right to be Informed
- Right to Access and Portability
- Right to Deletion
- Right to Object to the Sale of PI
- Right to Opt-In to Sales of Minors' PI
- Right to Non-Discrimination

Right to be Informed: Required Disclosures

Privacy notices must be updated at least every 12 months and disclose the following information:

- List(s) of the categories of PI collected, sold, and disclosed for a business purpose in the past 12 months—or a statement by the business that it has not sold or disclosed PI in the preceding 12 months (where applicable)
- Sources of each category of PI
- Categories of third parties with whom PI is shared
- Purposes for using each category of collected PI
- Description of consumers' rights and how to exercise them
- Two or more designated methods for submitting requests, including, at a minimum, a toll-free number and, if the business maintains a website, a web address
- A link, titled "Do Not Sell My Personal Information," to an opt-out page on the business's website (if applicable)
- Any financial incentive for providing data or not exercising rights

Right to be Informed: Required Disclosures (con't)

- Additional notice is required to:
  - Collect additional categories of PI
  - Use or disclose collected PI for any new or unrelated purposes

Responding to Consumer Requests

Verification Requirement

- A business must "reasonably verify" the identity of the consumer making the access, portability, or deletion request (known as a "verifiable consumer request")
- AG to issue regulations

Time to Respond

- Respond within 45 days of receipt of the request, potentially extendable for another 90 days where necessary, "taking into account the complexity and number of requests"
- Inform consumer of any extension and the reasons for delay within 45 days of receipt of the request

Responding to Consumer Requests (cont.)

Cost to Respond

- Requests must be handled free of charge, unless the request is manifestly unfounded/excessive (e.g., repetitive)
- Business bears burden to demonstrate the request's character
- If this criteria is met, a business may charge a "reasonable fee" reflecting administrative costs involved ***or*** refuse to respond to the request and notify the consumer of the reason

Right to Access and Portability

Upon a verified consumer request, a business must provide the following information to the requesting consumer on an individualized basis (i.e., specific to his or her data):

- The **categories of PI** collected about that consumer
- The **categories of sources** from which the PI was collected
- The **business or commercial purposes** for collecting or selling the PI
- The **categories of third parties** with whom the business shares PI
- The **specific pieces of PI** collected about that consumer
- Separate list containing the **categories of PI sold** about that consumer and the categories of third parties to whom the PI was sold (*if applicable)
- Separate list containing the categories of PI **disclosed for a business purpose** (*if applicable)

Right to Access and Portability –Format

Information provided in response to a request for disclosure may be delivered by mail or electronically

If information is delivered electronically, it must be sent in a portable and, if technically feasible, readily usable format that allows the consumer to transfer his/her data to another entity without hindrance

Right to Access and Portability - Limitations

- Right limited to 2x/year
- Information disclosed to the consumer need only cover the 12-month period prior to the verifiable consumer request
- Does not apply to PI collected for a single, one-time transaction if not sold or retained by the business

Right to Deletion

- Consumers can request deletion of any of their PI from a business and its service providers
- Opens the door for partial deletion requests
- Subject to many exceptions…

Exceptions to the Right to Deletion

No obligation to delete if the PI is necessary to:
Complete a transaction requested by data subject or to perform a contract
Detect a security incident
Protect against deceptive, fraudulent or illegal activity
Identify and repair errors
Promote free speech
Comply with California Electronic Communications Privacy Act
Engage in scientific, historical, or statistical research in the public interest
Enable solely internal uses that are reasonably aligned with consumer's expectations
Comply with a legal obligation
Otherwise used internally in a manner compatible with the context of the collection

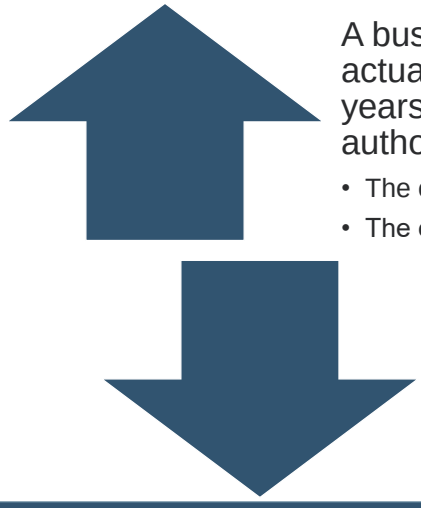
Right to Opt-Out of the Sale of PI

A consumer shall have the right, at any time, to direct a business that sells PI about the consumer to 3rd parties not to sell his or her PI

If a consumer has opted out, a business cannot request authorization to sell that consumer's PI for at least 12 months

Must include a "Do Not Sell My Personal Information" link in a clear and conspicuous location on a website homepage, a privacy policy, and in any California-specific description of consumers' privacy rights

Right to Opt-In to the Sale of Minors' PI



A business may not sell PI of a consumer if it has actual knowledge that the consumer is under 16 years of age, unless the sale was affirmatively authorized by:

- The consumer (if 13-15 years old); or
- The consumer's parent or guardian, if the consumer is under 13.

Willful disregard of the consumer's age is deemed actual knowledge of it.

FOLEY
FOLEY & LARDNER LLP

32

Right to Nondiscrimination

Right to Nondiscrimination

- In response to consumers who exercise their rights under the CCPA, a business may not:
  - Deny them goods or services.
  - Charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
  - Provide a different level or quality of goods or services to the consumer.
  - Suggest that they will do any of the above.

Carve-Outs

- May charge different prices, or provide different levels of goods/services, if the difference is reasonably related to the value provided to the consumer by his or her data.
- May offer financial incentives for the collection, sale or deletion of PI if:
  - The business notified the consumer of the material terms of the incentive and obtained opt-in consent (revocable at any time) prior to enrollment; and
  - The financial incentives are not unjust, unreasonable, coercive or usurious.

FOLEY
FOLEY & LARDNER LLP

33

Action Steps to Prepare for Consumer Rights Requests

In General

- Provide at least 2 methods for consumers to make requests for access (portability), deletion, and opting out
- Draft template initial and detailed responses to each of these requests
- Review mechanisms for gaining assistance from service providers

Right to Access and Portability

- Confirm ability to comply with 45-day timeline
- Confirm technical capabilities to deliver information pursuant to an access request in a portable and readily usable format that allows the consumer to transmit this information without hindrance

Action Steps to Prepare for Consumer Rights Requests

Right to Delete

- Confirm that you can comply with 45-day timeline
- Confirm technical abilities to remove an individual record without corrupting database

Right to Object (or Opt-In) to Sales

- Confirm technical capabilities to allow opt-out of the sale of PI for adults
- Confirm technical capabilities to get opt-in from children between 13-16 years old
- Confirm technical capabilities to get opt-in from parents or guardians of children under 13 years old

FOLEY
FOLEY & LARDNER LLP

Reasonable Security under CCPA

20 Instances of "Reasonable" or "Reasonably"

1798.150. (a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain *reasonable* security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

Implementing Reasonable Security

- Businesses have a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PI.
- Organizations can adopt a **Duty of Care Risk Analysis** to demonstrate they meet "reasonable."
- Can use the same framework to justify actions in meeting the intent of the statute and its burden.

FOLEY
FOLEY & LARDNER LLP

Penalties/Potential for Litigation

Risks of Non-Compliance

Regulatory Fines: Up to $7,500 regulatory fine for each intentional violation ($2,500 for unintentional violations)

Private Right of Action: Statutory damages between $100 - $750 per consumer per incident or actual damages (whichever is greater)

Reputational Harm

Additional Relief by Courts: Courts have authority to impose "any other relief the court deems proper"

FOLEY
FOLEY & LARDNER LLP

Note on Private Right of Action

- Consumers can bring a private civil action against a business that violates its duty to implement reasonable security procedures and practices ***if…***that failure results in an consumer's personal information being subject to unauthorized access and exfiltration, theft, or disclosure **AND** the consumer provides the business with written notice of specific CCPA provisions the consumer alleges have been violated and a 30 day cure period (if cure is possible)

FOLEY
FOLEY & LARDNER LLP

41

Considerations Regarding Litigation

- Like GDPR, we expect data subject access requests and claims of violation to begin almost immediately upon the CCPA taking affect on January 1, 2020.
- 30-day cure period is limited to violations that can be cured.
- Whether an organization has used ”reasonable” security measures may be left to the discretion of a judge/jury.
- Potential for litigation not only for how an organization uses data, but also if it fails to maintain it properly – concerned with unauthorized access, exfiltration, theft, or disclosure. A showing of harm may not be required.
- California State AG will issue additional regulations, which may increase potential liability.

FOLEY
FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

Pending CCPA Amendments

Pending CCPA Amendments

AB 25
(Employee information)

- Exempts, until January 1, 2021, employee information collected and used in the employment context from all provisions of the CCPA, except the private right of action for breaches and the obligation to inform the employee as to the categories of PI to be collected.

AB 1564
(Methods for consumers to exercise rights)

- Businesses are required to maintain at least two designated methods for consumers to submit requests (must include a toll-free telephone number).
- However, businesses that operate exclusively online AND maintain a direct relationship with California consumers are only required to provide an email address for CCPA requests.

AB 846
(Reward programs)

- Allows businesses to offer a different price, rate, level, or quality of goods or services to a consumer if the offering is (1) in connection with the consumer's voluntary participation in a loyalty or rewards program or (2) for a specific good or service with a functionality that is directly related to the collection, use or sale of the consumer's data.
- Businesses are prohibited from selling PI they collect in connection with these programs.

FOLEY
FOLEY & LARDNER LLP

Pending CCPA Amendments (cont.)

AB 1146
(Vehicle information)

- Excludes from the "opt out" right vehicle information or ownership information – i.e., VIN, make, model, year, odometer reading and the name and contact information of the registered owner(s) – retained or shared between a new motor vehicle dealer and the vehicle's manufacturer, if shared for warranty repair or recall purposes.

AB 874
(Definition of PI)

- Redefines "personal information" to exclude information from government records.

AB 1355
(Disclosure obligations)

- Narrows the disclosure requirement to categories of third parties to which information was sold, rather than requiring disclosure on a specific third-party-by-third party basis.

FOLEY
FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

Summary: How to Prepare for CCPA

Preparing for CCPA

- Conduct a data mapping exercise to determine scope of PI collection, use, and disclosure given CCPA's broad definition.
- Review and revise existing privacy notices to comply with new requirements.
- Develop procedures for submitting access requests, right to deletion, and rights to opt-out, including for authenticating individuals making requests. Develop a "playbook" for handling requests, and train employees on handling access requests.
- Implement technical capabilities to process consumer requests within the required deadlines.

Preparing for CCPA (cont.)

- Implement opt-in and parental consent requirements for children under 16.
- Review policies and practices for any discrimination against consumers who exercise their rights under CCPA, including denying goods and services, charging a different price, imposing penalties, different level/quality of service, or suggesting that the consumer will receive any of these for exercising their rights.
- Review agreements with service providers for CCPA-required contractual limitations.

Implement Risk Management

- Adopt a risk management framework and perform on-going analysis to determine risks to all PI.
  - Include all types of information from the definition of CCPA
  - Consider adopting a known industry risk assessment, such as NIST 800-30,ISO 27005, DoCRA (CIS RAM)
- Update controls that are reasonable.
- Immediately and periodically thereafter, review and revise the organization's security policies and procedures, considering security requirements for new types of PI, and draft or revise a written information security policy.

How We Evaluate Controls in the Age of Risk

- Think through the likelihood and impact of threats
- Reduce unacceptably high risks …
- … using controls that are no more burdensome than the risks

Our Security Objectives in the Age of Risk

WE LOOK OUT FOR YOU

YOU LOOK OUT FOR US

How Do We Accomplish That?

PROTECT OTHERS FROM FORESEEABLE HARM

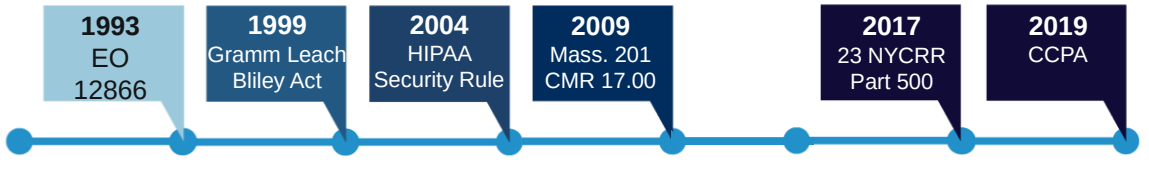
BUT WE **DON'T HARM OURSELVES** MORE IN THE PROCESS

FOLEY
FOLEY & LARDNER LLP

52

Regulations Are Business Friendly … Seriously

- Ever since 1993, **Executive Order 12866** required the regulations ***balance cost and benefit***.
- Controls must not cost more than the risk to others.
- That's why security regulations ask for "reasonable controls" and "risk analysis."



FOLEY
FOLEY & LARDNER LLP

53

Courts Look for the "Reasonable Person"

- Someone who thinks through the likelihood and impact of threats that might create harm …
- … designs safeguards that are not more burdensome than those risks

The risk to those who are protected by controls.

The burden to us when we apply the controls.

FOLEY
FOLEY & LARDNER LLP

54

What is the Duty of Care Risk Analysis ("DoCRA") Standard?

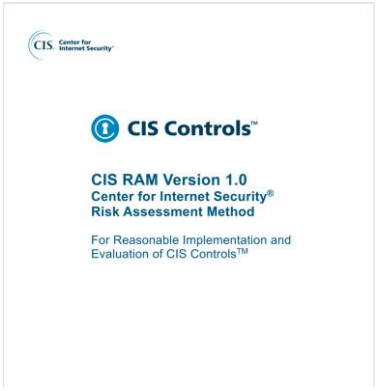
A freely available standard for conducting risk assessments.

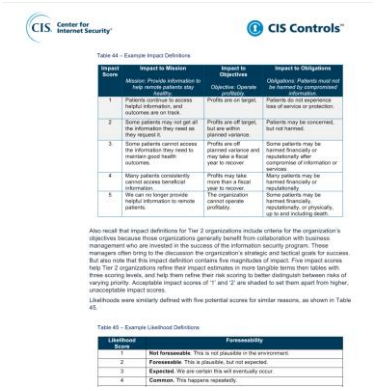
A method for demonstrating reasonableness.

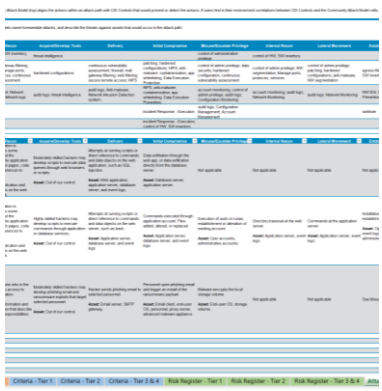
Prevails in litigation and regulation.

Originally developed by HALOCK Security Labs to help clients establish a goal for "enough" security.

FOLEY
FOLEY & LARDNER LLP







DoCRA Practically Applied: CIS RAM

FOLEY
FOLEY & LARDNER LLP

Basic Form

	Our Profit	Consumer Privacy
Acceptable	*Profit plan is on track*	*No harm*
Unacceptable	*Not profitable*	*Observable harm*

Harm to us

Harm to others

FOLEY
FOLEY & LARDNER LLP

More Practical Form

	Our Profit	Consumer Privacy
Negligible	*Profit plan is unaffected.*	*No harm.*
Acceptable	*Profit plan within planned variance.*	*Encrypted or unusable information cannot create harm.*
Unacceptable	*Not profitable. Recoverable within the year.*	*Recoverable harm among few consumers or minor harm among many consumers.*
High	*Not profitable. Recoverable in multiple years.*	*Harm among many consumers.*
Catastrophic	*Cannot operate profitably.*	*Cannot protect consumers from harm.*

Let's Get Real

To evaluate balance well, define **Your**:

Mission:
What makes the risk worth it for others?

Objectives:
What are your indicators of success?

Obligations:
What care do you owe others?

Some Common Impact Criteria

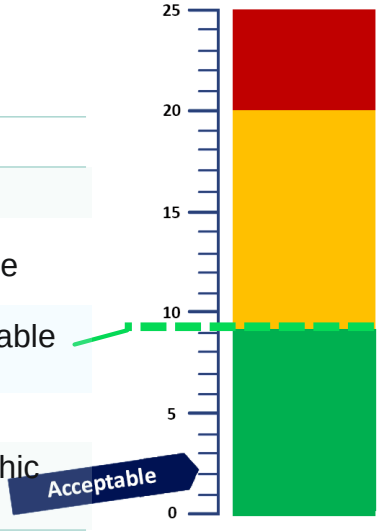
Industry Example	Mission	Objectives	Obligations
Commercial Bank	Customer performance	Return on assets	Customer information
Nonprofit Healthcare	Health outcomes	Balanced budget	Patient privacy
University	Educate students	Five year plan	Student financials
Manufacturer	Custom products	Profitability	Protect customer IP
Electrical generator	Provide power	Profitability	Public safety and privacy

FOLEY
FOLEY & LARDNER LLP

Defining Acceptable Risk

LIKELIHOOD	
1	Not possible
2	Not foreseeable
3	Foreseeable
4	Expected
5	Common

IMPACT	
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic

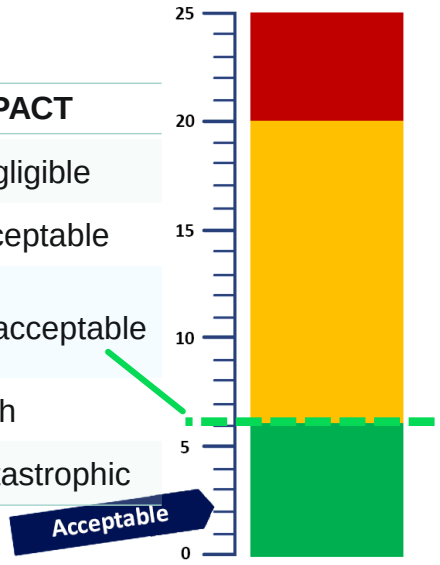


FOLEY
FOLEY & LARDNER LLP

Defining Acceptable Risk

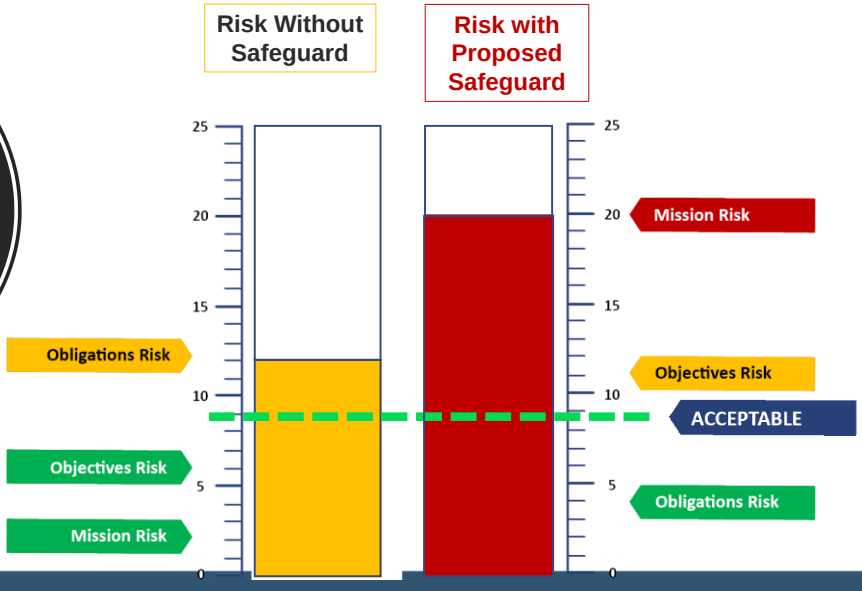
LIKELIHOOD	
1	Not possible
2	Not foreseeable
3	Foreseeable
4	Expected
5	Common

IMPACT	
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic



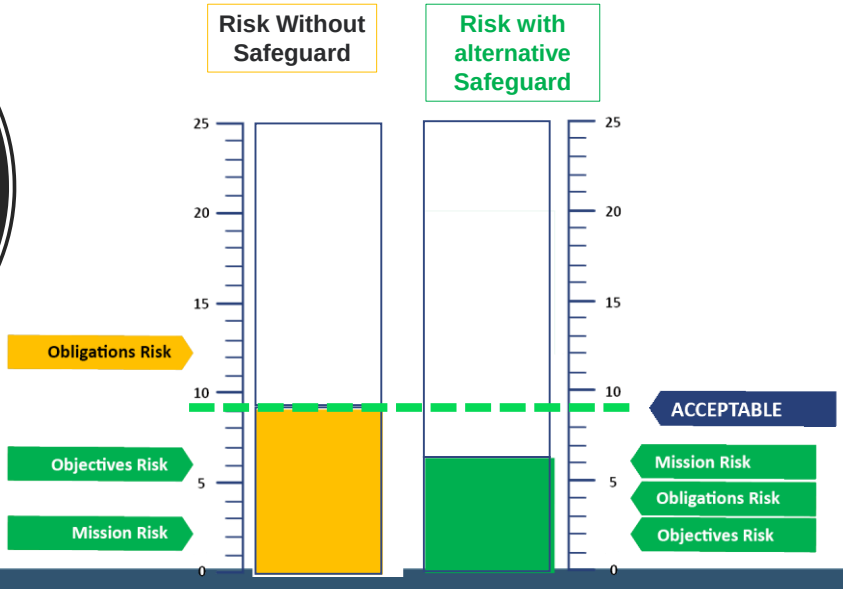
FOLEY
FOLEY & LARDNER LLP

Some Safeguards are NOT Reasonable



FOLEY
FOLEY & LARDNER LLP

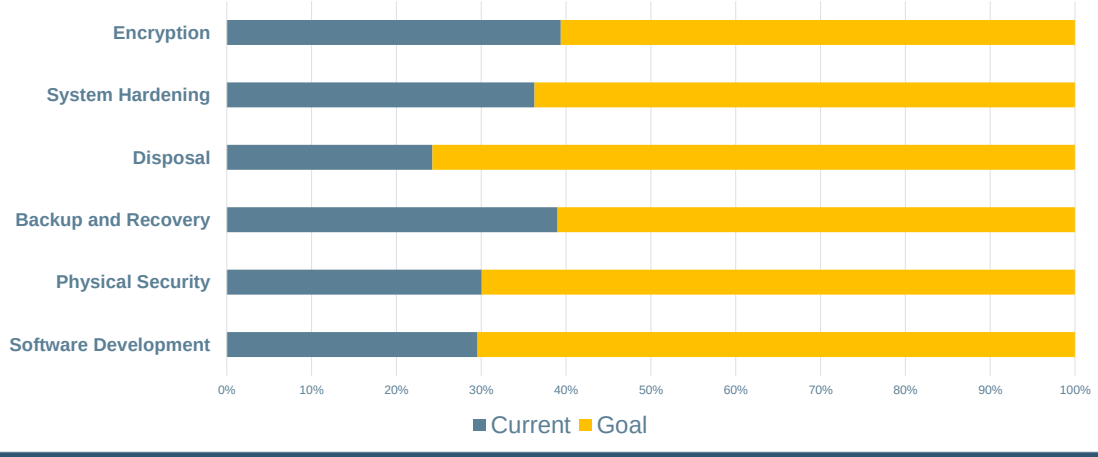
Demonstrating Reasonable Safeguards



FOLEY
FOLEY & LARDNER LLP

64

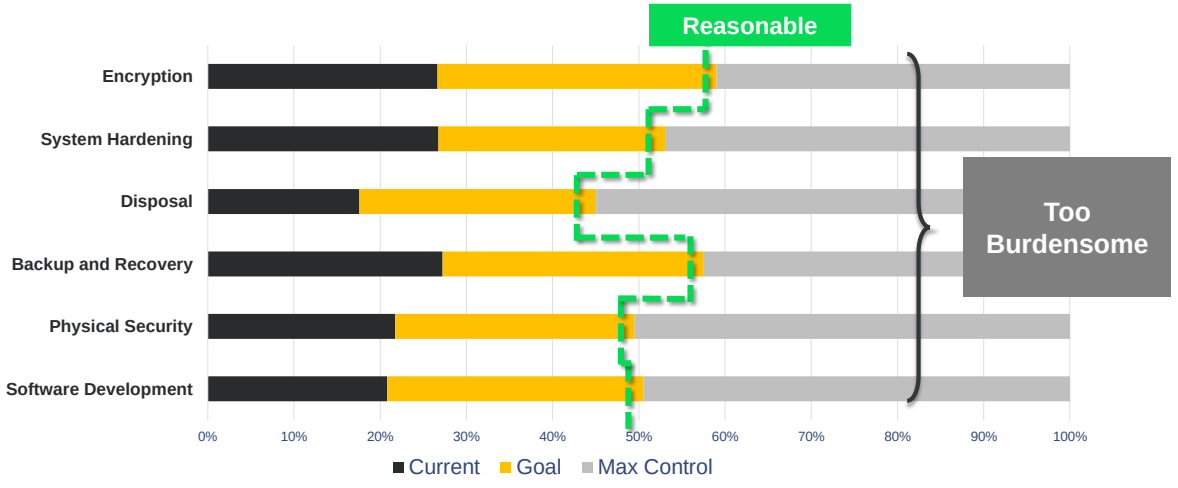
Our Roadmaps from the Compliance Age



FOLEY
FOLEY & LARDNER LLP

65

In the Risk Age We Do Enough to Protect Others, But Not So Much That We Hurt Ourselves



FOLEY
FOLEY & LARDNER LLP

66

Duty of Care Risk Analysis used to balance on obligation vs the organization's mission/objectives

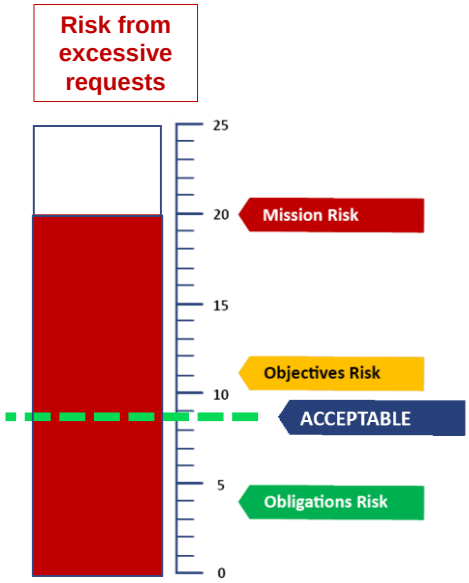
1798.145. (a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

- (3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. **The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.**

FOLEY
FOLEY & LARDNER LLP

67

Requests not Reasonable



FOLEY
FOLEY & LARDNER LLP

68

Thank You

FOLEY
FOLEY & LARDNER LLP