Is There Such a Thing as Reasonable Privacy?

Surviving and Thriving in the Age of Privacy Risk

Chris Cronin

- Partner at HALOCK Security Labs
- Chair, the DoCRA Council
- Principal Author of CIS RAM and DoCRA Standard
- Information Security Focus for 15 Years
  - Risk Analysis
  - Risk Management
  - Incident Response
  - Fraud Investigations
  - Governance
  - ISO 27001 Certification

The Importance of CAMP IT Conferences

I’m going to talk to you today about privacy

And specifically about whether privacy can be reasonable

Organizations are concerned about how demanding new privacy regulations may be.

New privacy regulations are asking us to do

new things that may seem hard to do.

We'll talk about what makes them hard …

And how to make them **reasonable**.

Topics

THE AGE OF PRIVACY RISK

BEING REASONABLE

SOLVING PRIVACY PROBLEMS USING DOCRA

The Age of Privacy Risk

Security v Privacy

Security	Privacy
Don’t let ***other people*** abuse information or systems	Don’t ***you*** abuse personal information

Security v Privacy (alt.)

Security	Privacy
1. Protect the confidentiality, integrity, and availability of information … (*authenticity?*)	1. Be accountable and transparent when handling personal information.
2. Protect the assets information is contained in.	2. Only use it for approved purposes.

Your Roles Regarding Security and Privacy

Security	Privacy
Protector and Guardian	Steward

Pre-GDPR U.S. Privacy Laws and Regulations

Federal Regulations for Limiting Access to Personal Information

- Limit what data is gathered, limit access, use reasonable security
  - COPPA/FRPA/FRCA, etc.
  - Gramm Leach Bliley Act
  - HIPAA Privacy Rule

State Statutes and Regulations

- Breach notifications, limiting access, reasonable security, stewardship
  - Each of the 50 states requires a variety of protections

Meanwhile … in the rest of the world …

- ❑ Publicly-stated policy
- ❑ Opt-in / Opt-out
- ❑ Respond to queries
- ❑ … and corrections
- ❑ “Onward transfer”
- ❑ Responsible party
- ❑ Arbitrator
- ❑ Reasonable security

The Age of Privacy Risk – Common Requirements (CCPA / GDPR)

Requirement	CCPA	GDPR
Know where personal information is and where it goes	✓	✓
Publicly post the privacy policy	✓	✓
Individuals may opt-in or opt-out of certain uses	✓	✓
Organizations cannot otherwise discriminate	✓	✓
Right to disclosure, download, or deletion	✓	✓
Reasonable (or) appropriate security controls	✓	✓
Protection of children's information	✓	✓
Penalties	✓	✓

The Age of Privacy Risk – Variations (CCPA / GDPR)

Requirement	CCPA	GDPR
Right to correct	✗	✓
Restrict or deny processing - Marketing, analysis, statistical modeling	✗	✓
Right to restrict automated decision-making - Decision tools, artificial intelligence	✗	✓
Economically quantify the value of personal records (Watch out!)	✓	✗
Opt-out of sale of personal information (TBD!)	✓	✗

Why We Say “Privacy Risk”

GDPR and CCPA will both need risk analysis to determine what reasonable safeguards are in your case.

- **GDPR:** “Guidance on the implementation of **appropriate measures** and on the **demonstration of compliance** by the controller or the processor, especially as regards the **identification of the risk** related to the processing, their assessment in terms of origin, nature, **likelihood and severity**, and the identification of best practices to mitigate the risk … ”

- **CCPA:** Reasonably related · reasonably anticipated · reasonable steps · reasonably accessible · reasonably necessary · reasonably aligned …

This New Era of Privacy Risk

The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights …

This Regulation respects all fundamental rights:

- *the respect for private and family life, home and communications,*
- *the protection of personal data,*
- *freedom of thought, conscience and religion,*
- *freedom of expression and information,*
- *freedom to conduct a business …*

- Recital 4, GDPR

So Reasonable Privacy is About Balancing …

… each person's interests against your own interests.

Being Reasonable

What Do Regulators and Judges Ask When Evaluating Reasonable Controls?*

- Did you think through the likelihood of potential incidents?
- Did you think about the magnitude of harm that would come to others who could foreseeably have been harmed?
- Did you consider the value in engaging in the risk to begin with? Was it worth the risk to you and to others?
- What safeguards did you consider that could have reduced the likelihood and impact?
- Would those safeguards have been more costly than the risk?
- Would the safeguards have created other risks?

* Questions vary by state

Where the Law is Heading

- **7.1 As part of the Information Security Program, Orbitz shall include risk management, which at a minimum includes:**

  a. Documented criteria for reasonable safeguards that appropriately protect Consumers while not being more burdensome to Orbitz than the risks they address. These criteria shall include:

    i. Obligations owed to the Consumers for protecting their Personal Information,

    ii. The social utility of Orbitz's handling of Consumers' Personal Information,

    iii. The foreseeability and magnitude of harm caused by security threats,

    iv. The burden of Orbitz's utility and objectives posed by safeguards,

    v. The overall public interest in the proposed solution.

**Commonwealth of Pennsylvania v Expedia and Orbitz, December, 2019*

Let’s Look at Risk Analysis

Risk = Impact x Likelihood

ISO 27005	FAIR	CIS RAM	Applied Information Economics	NIST 800-30

Let’s Look at Risk Analysis

Risk	=	Impact	x	Likelihood
12	*=*	*4*	*x*	*3*

Let’s Look at Risk Analysis

Risk	=	Impact	x	Likelihood
12	*=*	*4*	*x*	*3*

Impact	Likelihood
1	*1*
2	*2*
3	*3*
4	*4*
5	*5*

Let’s Look at Risk Analysis

Risk	=	Impact	x	Likelihood
15	*=*	*3*	*x*	*5*
		1		*1*
		2		*2*
		3		*3*
		4		*4*
		5		*5*

"I get it, but what do 1, 2, 3, 4, 5 mean?"

Risk	=	Impact	x	Likelihood
15	=	*3*	*x*	*5*

1. Negligible
2. Acceptable
3. Unacceptable
4. High
5. Catastrophic

1. Not possible
2. Rare, if at all
3. Occasional
4. Common
5. Frequent

HALOCK®

"Better. But it's still open to interpretation."

Risk	=	Impact *"Profit"*	x	Likelihood
15	=	*3*	*x*	*5*
		1. On plan		*1. Not possible*
		2. Within variance		*2. Rare, if at all*
		3. Out of variance		*3. Occasional*
		4. Profit in 3 yrs		*4. Common*
		5. Out of business		*5. Frequent*

HALOCK®

"I can probably accept some of these risks"

Risk	=	Impact	x	Likelihood
Accept "< 9"		*"Profit"*		
6	=	*3*	*x*	*2*
		1. On plan *2. Within variance* *3. Out of variance* *4. Profit in 3 yrs* *5. Out of business*		*1. Not possible* *2. Rare, if at all* *3. Occasional* *4. Common* *5. Frequent*

"Risk only to me? What about balance?"

Risk	=	Objectives Impact	Mission Impact	Obligations Impact	x	Likelihood
		"Profit"	*"User health"*	*"Others"*		
12	=	*3*	*2*	***4***	*x*	***3***
		1. On plan	*1. Significant results*	*1. No harm*		*1. Not possible*
		2. Within variance	*2. Few flat results*	*2. Concern*		*2. Rare, if at all*
		3. Out of variance	*3. Significant misses*	*3. Few embarrassed*		*3. Occasional*
		4. < 3 yrs profit loss	*4. Majority misses*	*4. Many exploited*		*4. Common*
		5. Out of business	*5. Cannot help users*	*5. Millions exploited*		*5. Frequent*

* Risk criteria for a Social Health App

Pause … What did you just do there?

- We looked at
  1. The potential to harm profit (Objectives)
  2. The potential to harm our service (Mission)
  3. The potential to harm others (Obligations)
- Why did we do this?
  1. We have a right to meet our business objectives.
  2. We and our customers have a right to benefit from our mission.
  3. The public has a right to privacy and security.
- To balance these three items, we must evaluate them.

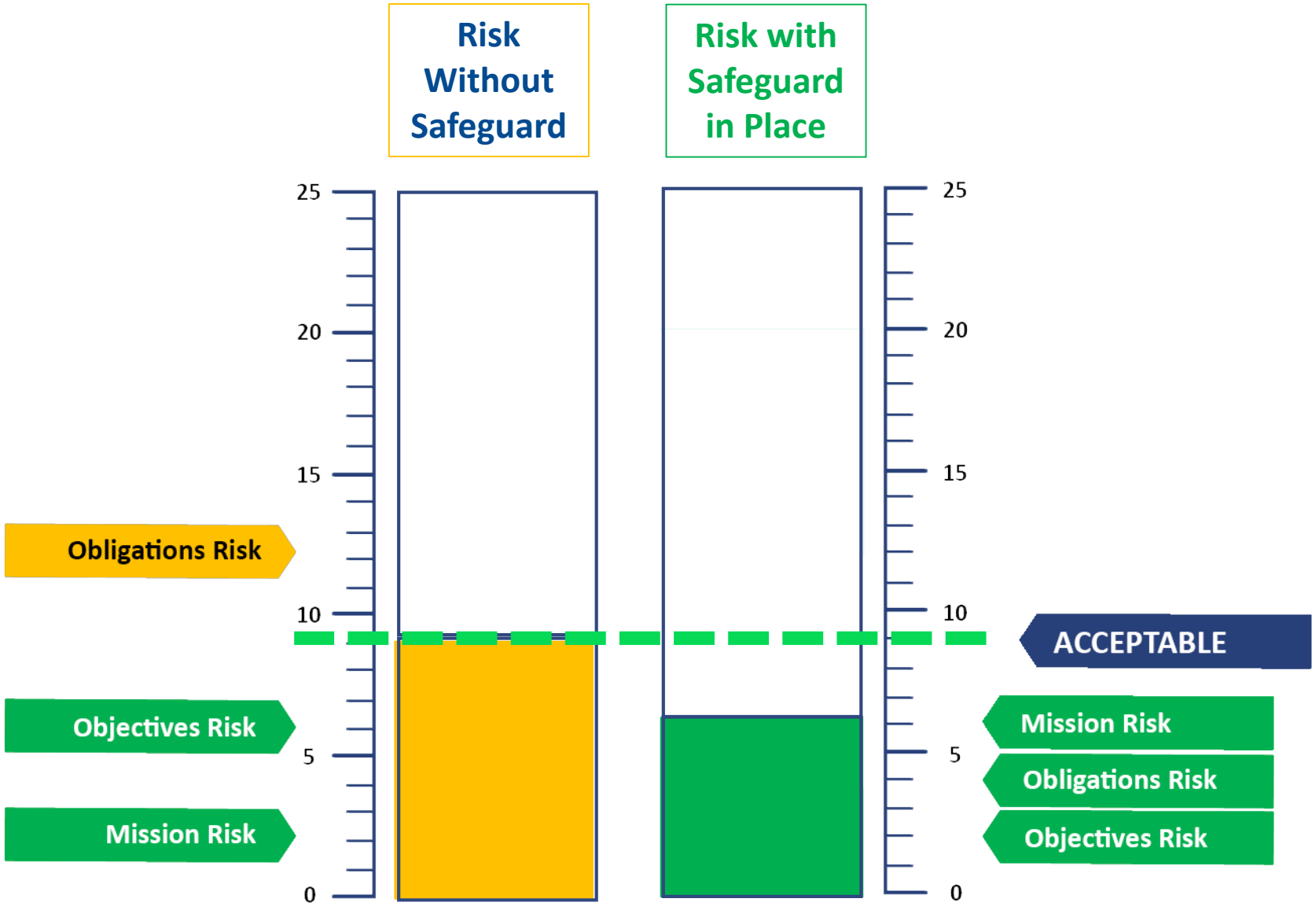
Impact definitions are unique to each of us

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

Duty of Care Risk Analysis as its Simplest

Neither your conduct nor your controls may create the likelihood of harm – to others, yourself, or your purpose – that is severe enough to require reparation.

How do I know if a Control is Reasonable?



Solving Privacy Problems Using DoCRA

Evaluating Three Difficult Privacy Challenges

Risk assess requirements from CCPA to find a reasonable control.

Case 1: The right to be forgotten when we need the data!

Case 2: Verifying consumers are who they say they are!

Case 3: Reasonable security practices … ?

Case 1: The Right to be Forgotten

Problem: A health app analyzes user data to provide insightful advice to their subscribers. They also sell the data to health researchers. So how do they respond to requests to be forgotten?

CCPA – *1798.105(d)(7) A business or a service provider* ***shall not be required*** *to comply with a consumer's request* ***to delete the consumer's personal information if*** *it is necessary for the business or service provider to maintain the consumer's personal information in order to … use the consumer's personal information, internally, in a lawful manner that* ***is compatible with the context in which the consumer provided the information****.*

CCPA – “Business Purpose”

*“**Business purpose**” means the use of personal information for the business’ or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information **shall be reasonably necessary** and proportionate to achieve the operational purpose for which the personal information was collected or process.*

“Reasonable Right to be Forgotten”

Right to be forgotten			
Risk Scenario	Unsubscribed users may request deletion from our analytics, reducing health benefits of the app.		
Threat	Delete requests	Vulnerability	Smaller datasets are less insightful
Objectives Impact	Mission Impact	Obligations Impact	
(3) Out of variance	(3) Significant misses	(1) No harm	
Likelihood	Risk Score: Max(Impact) x Likelihood		
(4) Common	12		

Safeguard	Leave all personal data in the analytics data set.
Safeguard Risk	Third party researchers may use or breach un-subscribers’ personal information.

Objectives Impact	Mission Impact	Obligations Impact
(4) Up to 3 years profit loss	(3) Significant misses	(4) Many exploited
Likelihood	**Safeguard Risk Score: Max(Impact) x Likelihood**	
(3) Occasional	12	

“Reasonable Right to be Forgotten”

Right to be forgotten			
Risk Scenario	Unsubscribed users may request deletion from our analytics, reducing health benefits of the app.		
Threat	Delete requests	Vulnerability	Smaller datasets are less insightful
Objectives Impact	Mission Impact	Obligations Impact	
(3) Out of variance	(3) Significant misses	(1) No harm	
Likelihood	Risk Score: Max(Impact) x Likelihood		
(4) Common	12		

Safeguard	Remove identifiable information from each requested record. Provide aggregations to researchers.
Safeguard Risk	New analytics may be hampered by missing data points in un-subscribers’ data

Objectives Impact	Mission Impact	Obligations Impact
(1) On plan	(2) Few flat results	(2) Concern
Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood	
(2) Rare, if at all	4	

Case 2: Verifying consumers' identities

Problem: When consumers contact the company to request personal information what reasonable controls would be sufficient?

CCPA – *1798.100(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.*

1798.140(y) "Verifiable consumer request" means a request that is made by a consumer … that the business can reasonably verify…

“Reasonable Verification of Users”

Un-subscriber’s registered email used to verify identity during privacy requests			
Risk Scenario	Hackers access an un-subscriber’s email account and access their health data from us.		
Threat	Unauthorized access to health data	Vulnerability	Remote users are difficult to identify
Objectives Impact	Mission Impact	Obligations Impact	
(1) On plan	(1) Significant results	(3) Few embarrassed	
Likelihood	Risk Score: Max(Impact) x Likelihood		
(3) Occasional	9		

Safeguard	Privacy requests go a support specialist who fields fraud detection “red flags” questions.
Safeguard Risk	Partial salary for specialist may be up to $30,000

Objectives Impact	Mission Impact	Obligations Impact
(1) On plan	(1) Significant results	(1) No harm
Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood	
(5) Frequent	5	

Case 3: Reasonable Security Practices

Problem: Should inter-server PII be encrypted if encrypted communications block the IPS from seeing inter-server attacks?

CCPA – **1798.150**(a)(1) … implement and maintain reasonable security procedures and practices …

“Reasonable Security Practices”

Encrypting PII between web apps and database			
Threat	Sniffers can capture PII	Vulnerability	Inter-server PII in plain text
Risk Scenario	Hackers implement packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		

Objectives Impact	Mission Impact	Obligations Impact
(4) < 3 yrs profit loss	(3) Significant misses	(5) Millions exploited

Likelihood	Risk Score: Max(Impact) x Likelihood
(2) Rare, it at all	10

Safeguard	Encrypt all data between application servers and database servers.
Safeguard Risk	IPS would not be able to inspect inter-server data to detect attacks or exfiltration.

Objectives Impact	Mission Impact	Obligations Impact
(4) < 3 yrs profit loss	(3) Significant misses	(5) Millions exploited

Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
(3) Occasional	15

“Reasonable Security Practices”

Encrypting PII between web apps and database			
Threat	Sniffers can capture PII	Vulnerability	Inter-server PII in plain text
Risk Scenario	Hackers implement packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		

Objectives Impact	Mission Impact	Obligations Impact
(4) < 3 yrs profit loss	(3) Significant misses	(5) Millions exploited

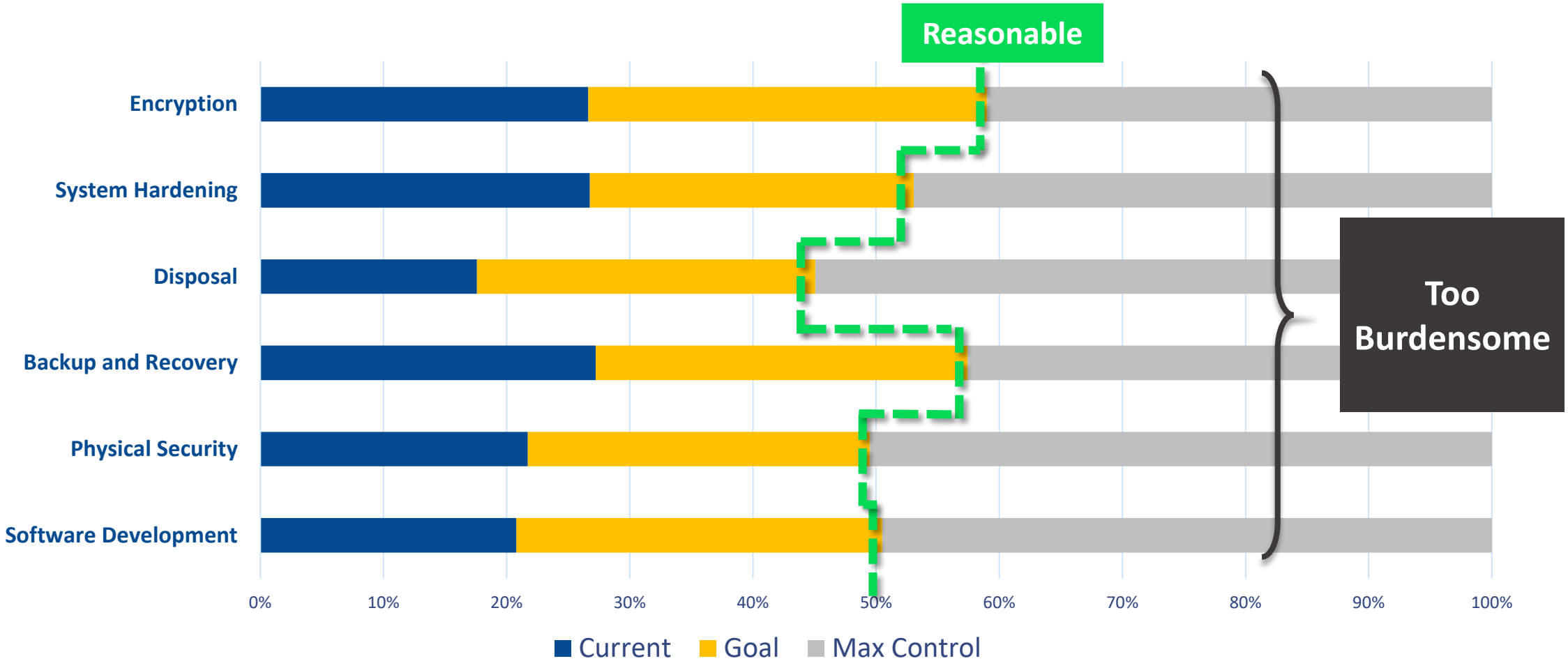
Likelihood	Risk Score: Max(Impact) x Likelihood
(2) Rare, if at all	10

Safeguard	Isolate app server interface, database interface, and IPS sensor in segregated network.
Safeguard Risk	Sniffing hosts would be quickly detected by IPS.

Objectives Impact	Mission Impact	Obligations Impact
(4) < 3 yrs profit loss	(3) Significant misses	(4) Many exploited

Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
(2) Rare, if at all	5

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



Why Other Assessments Come Up Short

	Evaluates Risk to Information Assets					Evaluates Due Care				
Method	**Assets**	**Identifies Vulnerabilities**	**Considers Threats**	**Evaluates Harm to Self**	**Estimates Likelihood**	**Standard of Care**	**Evaluates Harm to Others**	**Defines Acceptable Risk**	**Defines Reasonability**	**Evaluates Safeguard Risk**
CIS RAM DoCRA	●	●	●	●	●	●	●	●	●	●
IT Risk Assessments ISO 27005, NIST SP 800-30, RISK IT	●	●	●	●	●	●	◑	○	○	◔
Probability Applied Information Economics	●	◑	●	●	●	○	○	●	○	◔
FAIR Factor Analysis for Information Risk	●	●	●	●	●	○	◑	○	○	◔
Gap Assessments Audits, "Yes/No/Partial"	◑	◑	○	○	○	●	○	○	○	○
Maturity Model Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	●	○	○	○	○

** Provided by the DoCRA Council - www.docra.org. July 2018*

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

A freely available standard for conducting risk assessments.

A method for demonstrating reasonableness.

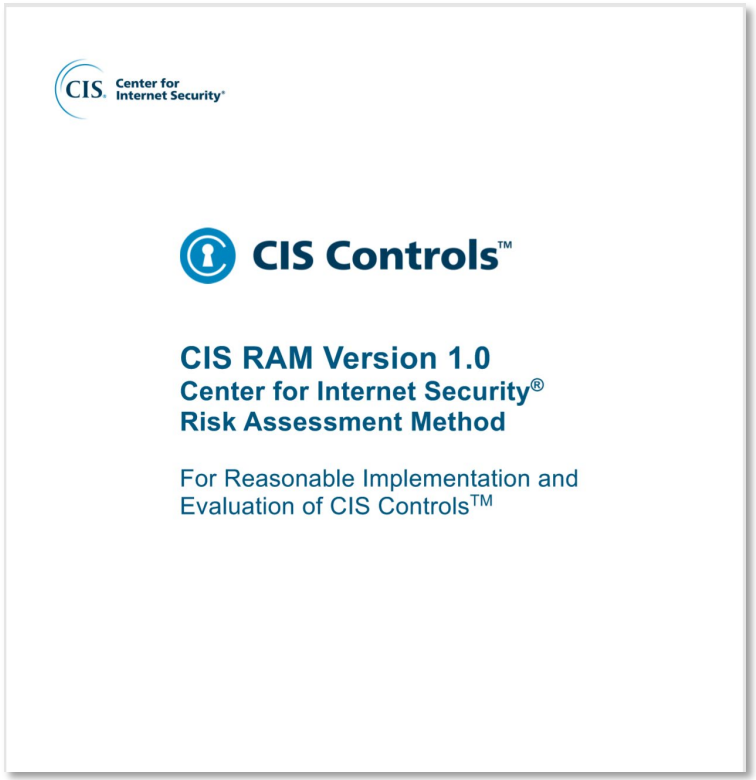
Prevails in litigation and regulation.

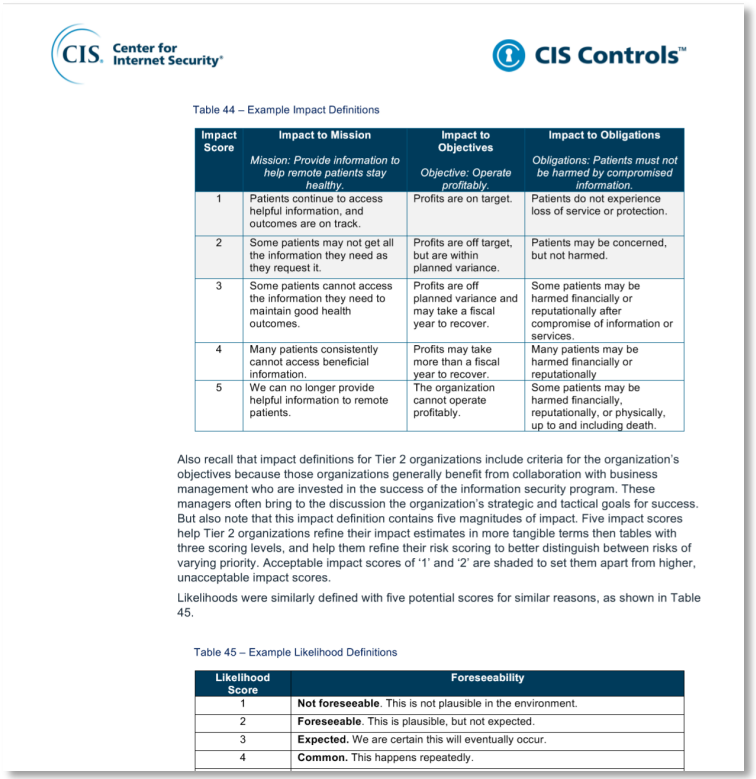
Originally developed by HALOCK Security Labs to help clients establish a goal for “enough” security.

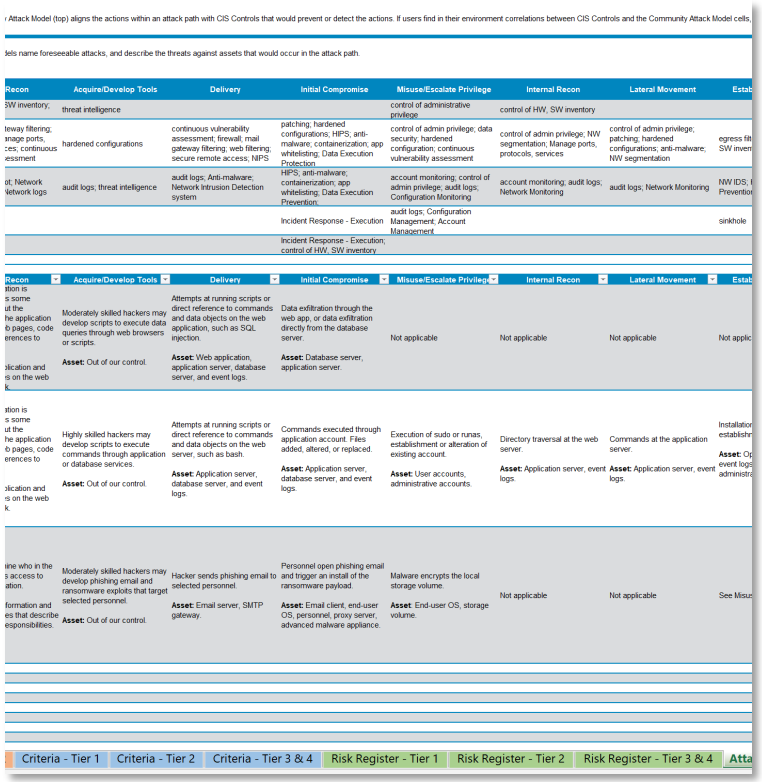
HALOCK®

DoCRA Standard

Use your current risk assessment method	NIST SP 800-30 ISO 27005 CIS RAM RISK IT FAIR Applied Information Economics (Hubbard)
Just follow these three principles	- Risk analysis must consider the interests of all parties that may be harmed by the risk. - Risks must be reduced to a level that authorities and potentially affected parties would find appropriate. - Safeguards must not be more burdensome than the risks they protect against.







DoCRA Practically Applied: CIS RAM

HALOCK®

Thank You

Chris Cronin

HALOCK Security Labs

ccronin@halock.com

ccronin@docra.org