CMMC/CCPA

Using Duty of Care Risk Analysis to Comply With New Requirements

HALOCK®

Today’s Objectives

I DISCUSS CMMC REQUIREMENTS

I DISCUSS CCPA REQUIREMENTS

I SYMPATHIZE WITH YOU

THEN I BLOW YOUR MIND

Cybersecurity Maturity Model Certification

(CMMC)

What is CMMC?

A new *security* standard

- Department of Defense’s supply chain security standard
- 350,000 DoD vendors and downstream vendors must certify

Operated by CMMCAB

- CMMC Accreditation Board
- A new, independent nonprofit (think: PCI Security Council)

What Does CMMC Entail?

Protects CUI

- Controlled Unclassified Information

Looks similar to NIST 800-171 and CSF

- Crosswalks to NIST 800-53, CIS Controls
- Compliance requirements are based maturity and risk
- Maturity is risk-based – Levels ‘1’ through ‘5’
- Requires risk assessment

CMMC Timeline

In Development Now

- Assessors and Implementers being accredited/registered now
- Standard is published
- Training and accreditation is being tested and refined

Full Rollout Scheduled

- Spring 2021

CMMC Control Requirements

- Access Control
- Asset Mgmt
- Audit & Accountability
- Awareness & Training
- Config Mgmt
- ID Auth
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Recovery
- Sec. Assess
- Situational Awareness
- System/Comm Protection
- System/Info Integrity
- Risk Mgmt

* HINT *

California Consumer Privacy Act

(CCPA)

What is CCPA?

A new *privacy* regulation

- Required by California to protect personal information (PI)
- Very deep into every business process that uses PI

Who must comply?

- Have a gross annual revenue of over $25 million, or
- Handle information of 50,000 or more California residents, or
- Derive 50% or more of their annual revenue from selling PI.

What Does CCPA Entail?

Addresses Personal Information

- PI about California consumers, households, devices.

How to think of it …

- Personal information is a commodity that consumers own and may share. Organizations must use it according to consumers’ consent.

CCPA Timeline

In full effect July 1, 2020

- Office of Attorney General may pursue
- Class action suits are in play now

Updates may be on their way!

- CPRA is on the agenda for November 2020

CCPA Control Requirements

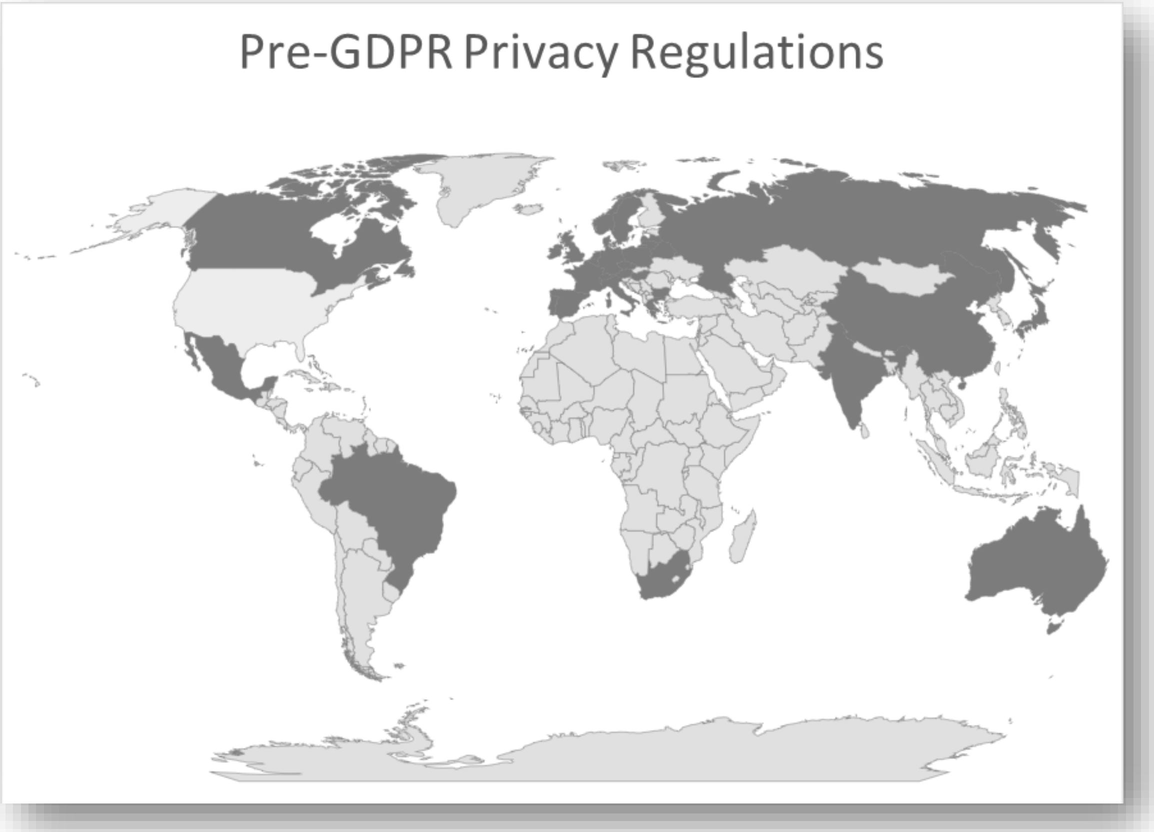
- Notice
- Access Control
- Right to be Forgotten
- Specification / Exception
- PI Transfer
- Consumers' Choice
- Disclosure
- Non-Discrimination
- Third-Party Controls
- Reasonable Security

* HINT *

Security v Privacy

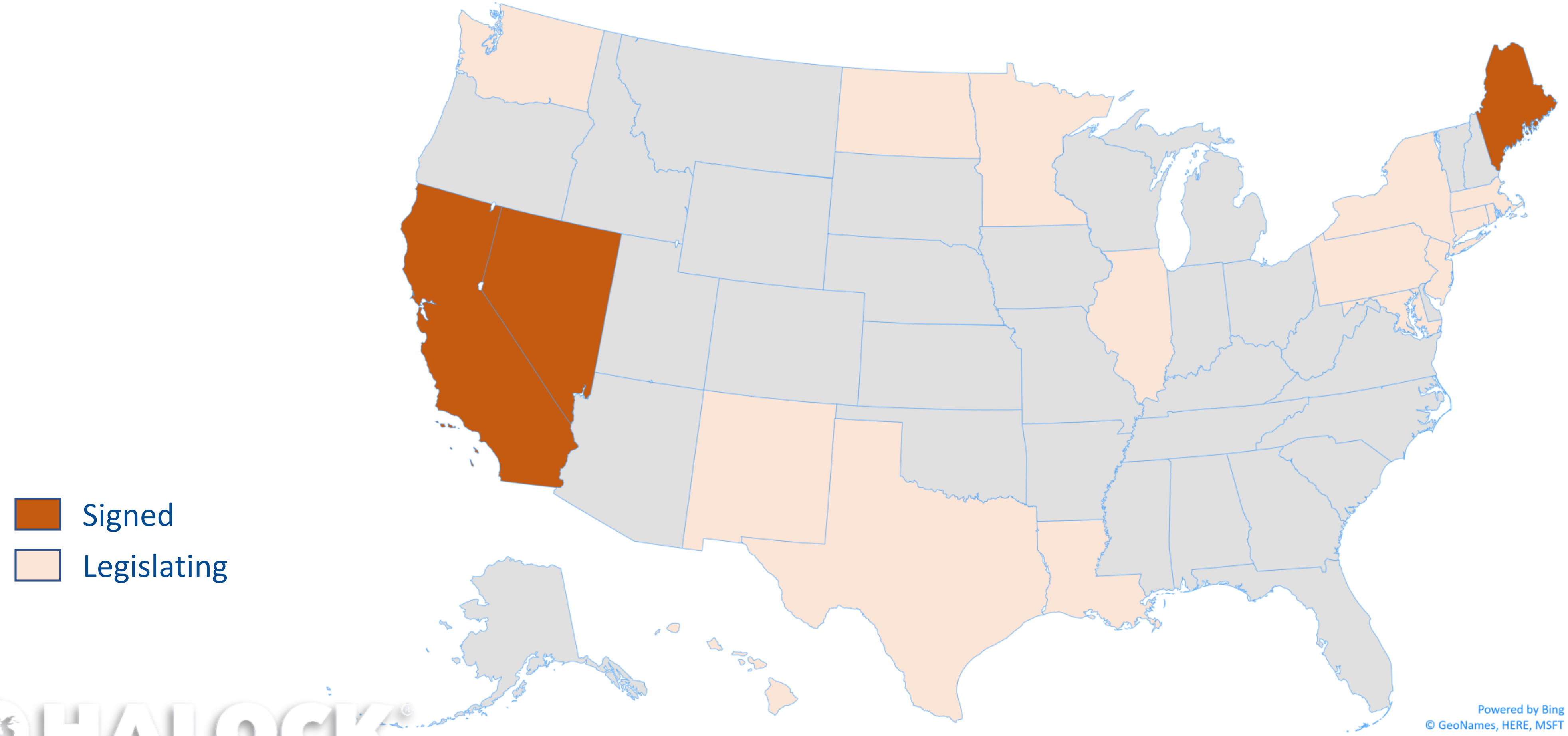
Security	Privacy
Don't let ***other people*** abuse information or systems	Don't ***you*** abuse personal information

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

State Privacy Law Activity – 2020
Stewardship of Others' Personal Information



Powered by Bing
© GeoNames, HERE, MSFT

… oh … and …

- HIPAA Security Rule
- Gramm Leach Bliley Act
- 23 NYCRR Part 500
- GDPR
- FISMA
- FERPA
- State Security Laws

- NIST 800-53
- PCI DSS
- NIST Cybersecurity Framework
- ISO 27001/27001
- NIST 800-171
- CIS Controls
- Sarbanes Oxley

“The Fog of More” – Tony Sager, CIS

- Applied antivirus
- Policies
- Firewalls
- Training
- Segmentation
- Access controls
- Encryption
- Right to be forgotten

Pen Testing!

Hardening

Opt-in

MFA!

Vulnerability scans

BYOD

VPN!

Whitelisting

Secure development

IoT!

Audit!

IDS / IPS

Secure DNS

I Sympathize With You

I Blow Your Mind

THEY ALL KNOW YOU CAN'T GET TO 100%

- CMMC
- CCPA
- HIPAA Security Rule
- Gramm Leach Bliley Act
- 23 NYCRR Part 500
- GDPR
- FISMA
- FERPA
- State Security Laws

- NIST 800-53
- PCI DSS
- NIST Cybersecurity Framework
- ISO 27001/27001
- NIST 800-171
- CIS Controls
- Sarbanes Oxley

THEY ALL KNOW YOU CAN’T GET TO 100%

You’re Not Even Supposed To!

THEY ALL KNOW YOU CAN’T GET TO 100%

And They’re OK With That!

THEY ALL KNOW YOU CAN'T GET TO 100%

… this is why they say
*"**reasonable**" and "**risk-based** …"*

What Do Regulators and Judges Ask After Your Breach?*

- 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

That’s Duty of Care Risk Analysis

Impact $_{(\textit{Others})}$ **x Likelihood**

Impact $_{(\textit{You})}$ **x Likelihood**

Where the Law is Heading

- **7.1 As part of the Information Security Program, Orbitz, Expedia 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 (example)

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

Let’s Look at Risk Analysis (Qualitative)

Risk	=	Impact	x	Likelihood
12	*=*	*4*	*x*	*3*
		1		*1*
		2		*2*
		3		[✓ *3*]
		[✓ *4*]		*4*
		5		*5*

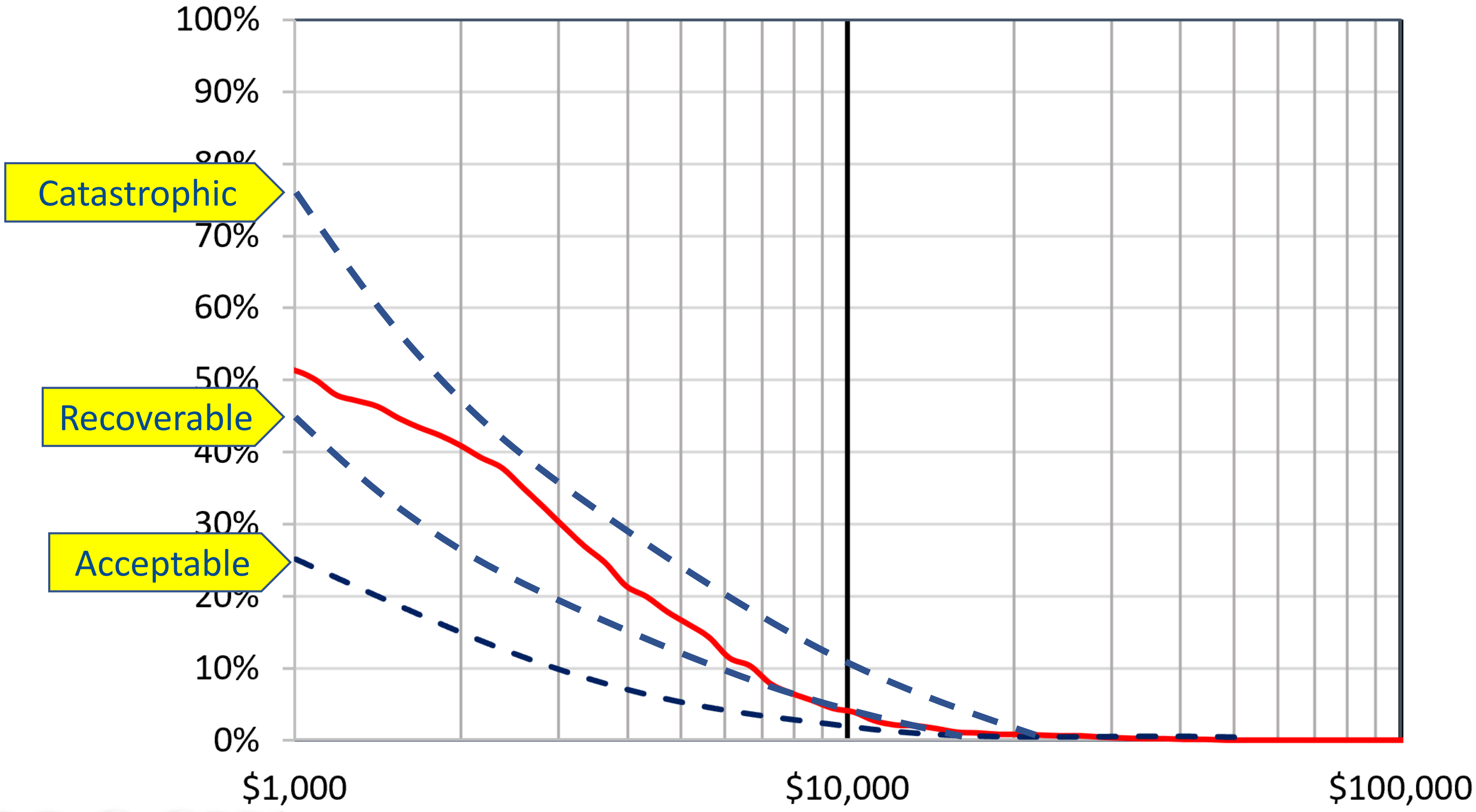
Let’s Look at Risk Analysis (Quantitative)

Risk	=	Impact	x	Likelihood
$1.05MM	*=*	*2.5MM*	*x*	*42.2%*
		$0		*0%*
		< $100k		*< 2.1%*
		[✓ *< $2.5MM*]		*< 5.7%*
		< $25MM		[✓ *< 42.2%*]
		> 25MM		*> 42.2%*

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

Risk	=	Impact	x	Likelihood
15	*=*	*3*	*x*	*5*
		1. Negligible		*1. Not possible*
		2. Acceptable		*2. Rare, if at all*
		[✓ 3.] Unacceptable		*3. Occasional*
		4. High		*4. Common*
		5. Catastrophic		*[✓ 5.] Frequent*

(for quants, indicate limits along your curve)



* Courtesy Hubbard Decision Research

“Better. But it’s still open to interpretation.”

Risk	=	Impact	x	Likelihood
		“Profit”		
15	*=*	*3*	*x*	*5*

1. On plan

2. Within variance

[✓ *3. Out of variance*]

4. Profitable in 3 yrs

5. Out of business

1. Not possible

2. Rare, if at all

3. Occasional

4. Common

[✓ *5. Frequent*]

"I can probably accept some of these risks"

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

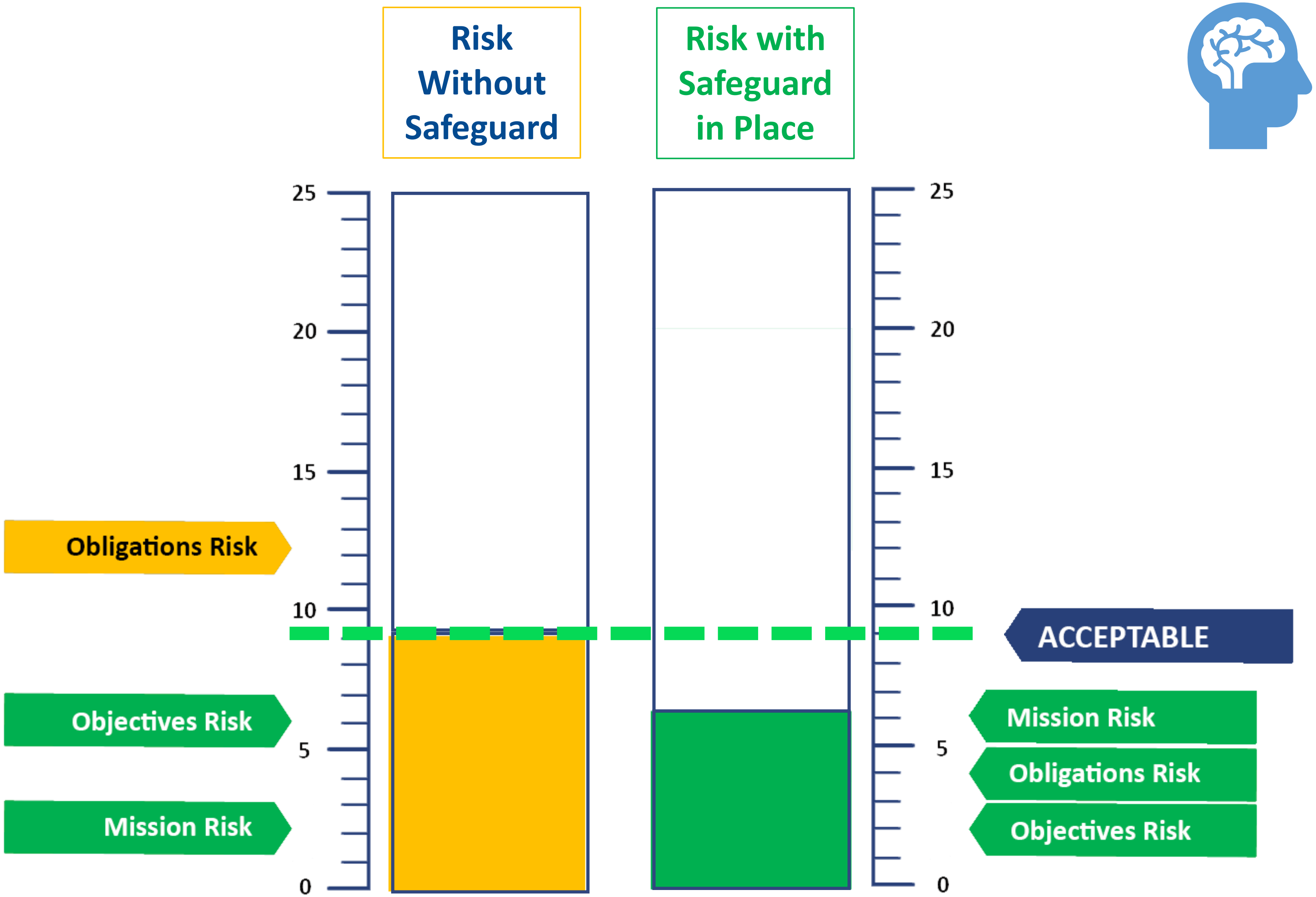
Neither your conduct, nor your controls, may create a likelihood of harm (to yourself or others) large enough to require correction.

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*

How do I know if a Control is Reasonable?



Evaluating Difficult Control Challenges

Risk assess requirements from CCPA and CMMC to find reasonable controls.

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

CMMC Case: When CUI should be unencrypted!

“Reasonable Right to be Forgotten”

<table>
<tr><th colspan="12">Right to be forgotten</th></tr>
<tr><td colspan="2">Risk Scenario</td><td colspan="10">Unsubscribed users may request deletion from our analytics, reducing health benefits of the app.</td></tr>
<tr><td colspan="2">Threat</td><td colspan="4">Delete requests</td><td colspan="2">Vulnerability</td><td colspan="4">Smaller datasets are less insightful</td></tr>
<tr><td colspan="4">Objectives Impact</td><td colspan="4">Mission Impact</td><td colspan="4">Obligations Impact</td></tr>
<tr><td colspan="4">(3) Out of variance</td><td colspan="4">(3) Significant misses</td><td colspan="4">(1) No harm</td></tr>
<tr><td colspan="6">Likelihood</td><td colspan="6">Risk Score: Max(Impact) x Likelihood</td></tr>
<tr><td colspan="6">(4) Common</td><td colspan="6">12</td></tr>
</table>

<table>
<tr><td colspan="2">Safeguard</td><td colspan="10">Leave all personal data in the analytics data set.</td></tr>
<tr><td colspan="2">Safeguard Risk</td><td colspan="10">Third party researchers may use or breach un-subscribers’ personal information.</td></tr>
<tr><td colspan="4">Objectives Impact</td><td colspan="4">Mission Impact</td><td colspan="4">Obligations Impact</td></tr>
<tr><td colspan="4">(4) Up to 3 years profit loss</td><td colspan="4">(3) Significant misses</td><td colspan="4">(4) Many exploited</td></tr>
<tr><td colspan="6">Likelihood</td><td colspan="6">Safeguard Risk Score: Max(Impact) x Likelihood</td></tr>
<tr><td colspan="6">(3) Occasional</td><td colspan="6">12</td></tr>
</table>

“Reasonable Right to be Forgotten”

<table>
<tr><th colspan="6">Right to be forgotten</th></tr>
<tr><td>Risk Scenario</td><td colspan="5">Unsubscribed users may request deletion from our analytics, reducing health benefits of the app.</td></tr>
<tr><td>Threat</td><td colspan="2">Delete requests</td><td>Vulnerability</td><td colspan="2">Smaller datasets are less insightful</td></tr>
<tr><td colspan="2">Objectives Impact</td><td colspan="2">Mission Impact</td><td colspan="2">Obligations Impact</td></tr>
<tr><td colspan="2">(3) Out of variance</td><td colspan="2">(3) Significant misses</td><td colspan="2">(1) No harm</td></tr>
<tr><td colspan="3">Likelihood</td><td colspan="3">Risk Score: Max(Impact) x Likelihood</td></tr>
<tr><td colspan="3">(4) Common</td><td colspan="3">12</td></tr>
</table>

<table>
<tr><td>Safeguard</td><td colspan="5">Remove identifiable information from each requested record. Provide aggregations to researchers.</td></tr>
<tr><td>Safeguard Risk</td><td colspan="5">New analytics may be hampered by missing data points in un-subscribers’ data</td></tr>
<tr><td colspan="2">Objectives Impact</td><td colspan="2">Mission Impact</td><td colspan="2">Obligations Impact</td></tr>
<tr><td colspan="2">(1) On plan</td><td colspan="2">(2) Few flat results</td><td colspan="2">(2) Concern</td></tr>
<tr><td colspan="3">Likelihood</td><td colspan="3">Safeguard Risk Score: Max(Impact) x Likelihood</td></tr>
<tr><td colspan="3">(2) Rare, if at all</td><td colspan="3">4</td></tr>
</table>

HALOCK

“Reasonably Unencrypted CUI”

Encrypting PII between API 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 API 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

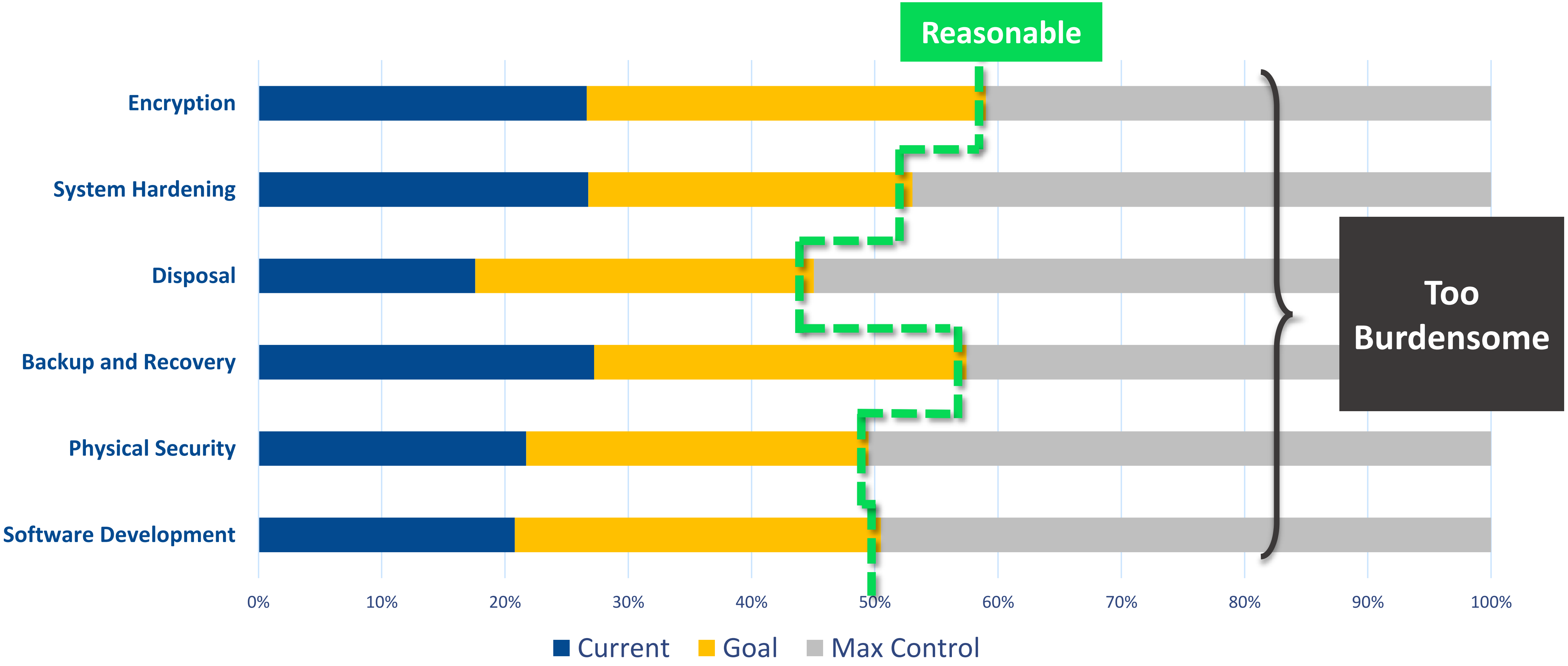
“Reasonably Unencrypted CUI”

<table>
<tr><th colspan="6">Encrypting PII between API and database</th></tr>
<tr><td>Threat</td><td colspan="2">Sniffers can capture PII</td><td>Vulnerability</td><td colspan="2">Inter-server PII in plain text</td></tr>
<tr><td>Risk Scenario</td><td colspan="5">Hackers implement packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.</td></tr>
<tr><td colspan="2">Objectives Impact</td><td colspan="2">Mission Impact</td><td colspan="2">Obligations Impact</td></tr>
<tr><td colspan="2"><i>(4) &lt; 3 yrs profit loss</i></td><td colspan="2">(3) Significant misses</td><td colspan="2">(5) Millions exploited</td></tr>
<tr><td colspan="3">Likelihood</td><td colspan="3">Risk Score: Max(Impact) x Likelihood</td></tr>
<tr><td colspan="3">(2) Rare, if at all</td><td colspan="3">10</td></tr>
</table>

<table>
<tr><td>Safeguard</td><td colspan="5">Isolate API server interface, database interface, and IPS sensor in segregated network.</td></tr>
<tr><td>Safeguard Risk</td><td colspan="5">Sniffing hosts would be quickly detected by IPS.</td></tr>
<tr><td colspan="2">Objectives Impact</td><td colspan="2">Mission Impact</td><td colspan="2">Obligations Impact</td></tr>
<tr><td colspan="2"><i>(4) &lt; 3 yrs profit loss</i></td><td colspan="2">(3) Significant misses</td><td colspan="2">(4) Many exploited</td></tr>
<tr><td colspan="3">Likelihood</td><td colspan="3">Safeguard Risk Score: Max(Impact) x Likelihood</td></tr>
<tr><td colspan="3">(2) Rare, if at all</td><td colspan="3">8</td></tr>
</table>

HALOCK

Risk Management Means We Do Enough to Protect Others, But Not So Much That We Hurt Ourselves



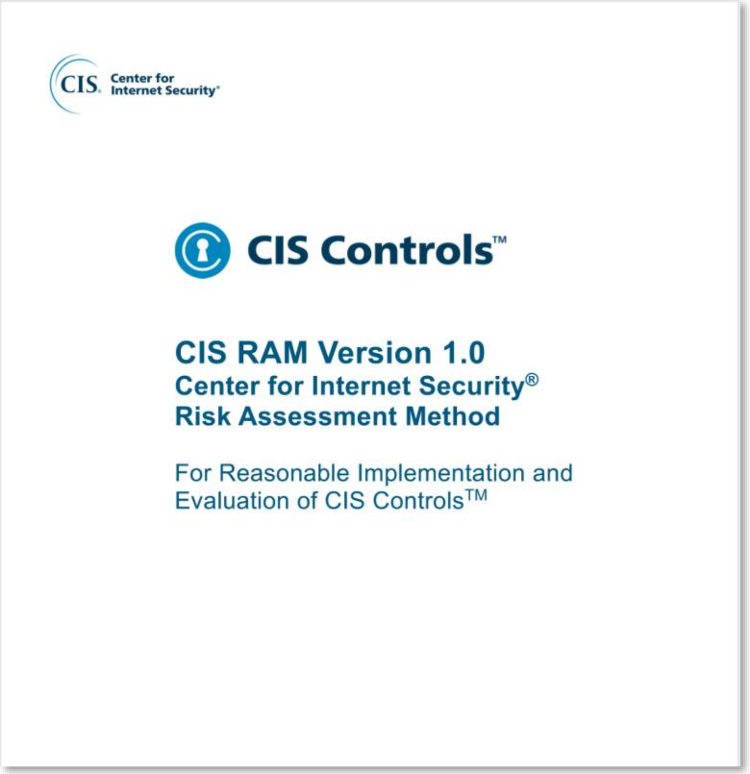
What is the Duty of Care Risk Analysis (“DoCRA”) Standard?

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.

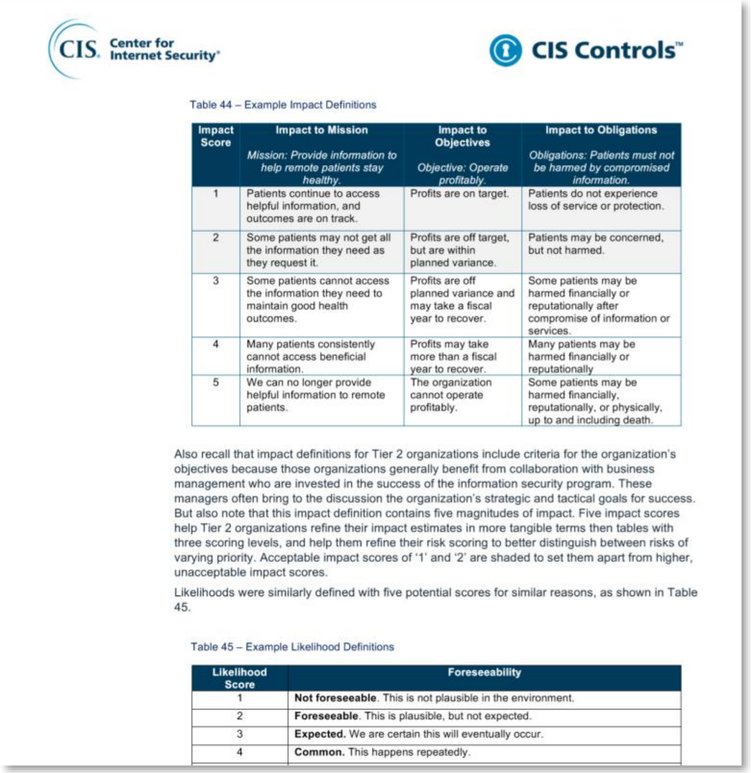


CIS Center for Internet Security®

CIS Controls™

CIS RAM Version 1.0
Center for Internet Security®
Risk Assessment Method

For Reasonable Implementation and Evaluation of CIS Controls^{TM}



CIS Center for Internet Security®

CIS Controls™

Table 44 – Example Impact Definitions

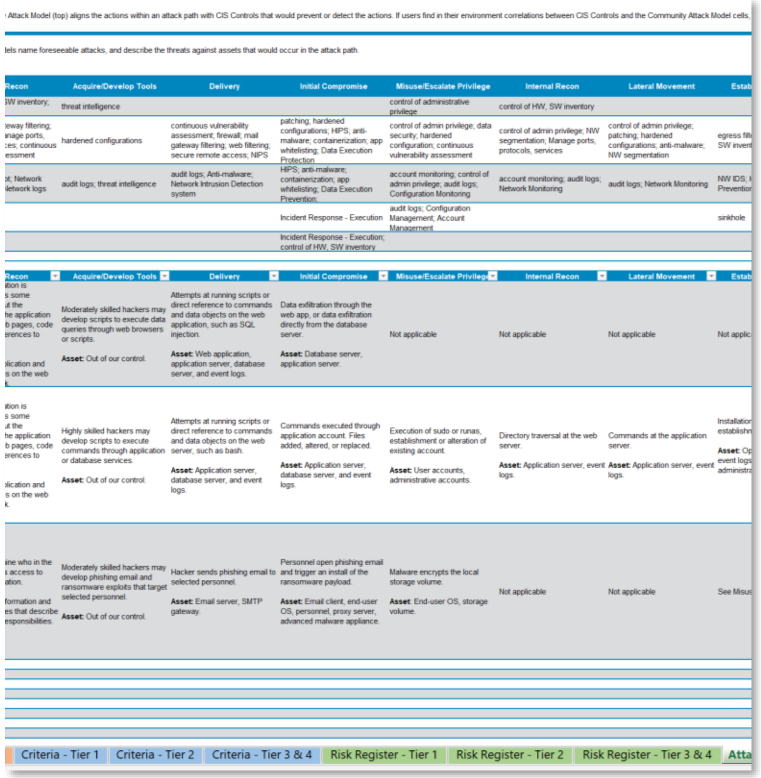
Impact Score	Impact to Mission *Mission: Provide information to help remote patients stay healthy.*	Impact to Objectives *Objective: Operate profitably.*	Impact to Obligations *Obligations: Patients must not be harmed by compromised information.*
1	Patients continue to access helpful information, and outcomes are on track.	Profits are on target.	Patients do not experience loss of service or protection.
2	Some patients may not get all the information they need as they request it.	Profits are off target, but are within planned variance.	Patients may be concerned, but not harmed.
3	Some patients cannot access the information they need to maintain good health outcomes.	Profits are off planned variance and may take a fiscal year to recover.	Some patients may be harmed financially or reputationally after compromise of information or services.
4	Many patients consistently cannot access beneficial information.	Profits may take more than a fiscal year to recover.	Many patients may be harmed financially or reputationally
5	We can no longer provide helpful information to remote patients.	The organization cannot operate profitably.	Some patients may be harmed financially, reputationally, or physically, up to and including death.

Also recall that impact definitions for Tier 2 organizations include criteria for the organization's objectives because those organizations generally benefit from collaboration with business management who are invested in the success of the information security program. These managers often bring to the discussion the organization's strategic and tactical goals for success. But also note that this impact definition contains five magnitudes of impact. Five impact scores help Tier 2 organizations refine their impact estimates in more tangible terms then tables with three scoring levels, and help them refine their risk scoring to better distinguish between risks of varying priority. Acceptable impact scores of '1' and '2' are shaded to set them apart from higher, unacceptable impact scores.

Likelihoods were similarly defined with five potential scores for similar reasons, as shown in Table 45.

Table 45 – Example Likelihood Definitions

Likelihood Score	Foreseeability
1	**Not foreseeable**. This is not plausible in the environment.
2	**Foreseeable**. This is plausible, but not expected.
3	**Expected.** We are certain this will eventually occur.
4	**Common.** This happens repeatedly.



Attack Model (top) aligns the actions within an attack path with CIS Controls that would prevent or detect the actions. If users find in their environment correlations between CIS Controls and the Community Attack Model cells,

dels name foreseeable attacks, and describe the threats against assets that would occur in the attack path.

Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Estab
SW inventory;	threat intelligence			control of administrative privilege	control of HW, SW inventory		
teway filtering; anage ports, ces; continuous essment	hardened configurations	continuous vulnerability assessment; firewall; mail gateway filtering; web filtering; secure remote access; NIPS	patching; hardened configurations; HIPS; anti-malware; containerization; app whitelisting; Data Execution Protection	control of admin privilege; data security; hardened configuration; continuous vulnerability assessment	control of admin privilege; NW segmentation; Manage ports, protocols, services	control of admin privilege; patching; hardened configurations; anti-malware; NW segmentation	egress filt SW invent
ot; Network letwork logs	audit logs; threat intelligence	audit logs; Anti-malware; Network Intrusion Detection system	HIPS; anti-malware; containerization; app whitelisting; Data Execution Prevention;	account monitoring; control of admin privilege; audit logs; Configuration Monitoring	account monitoring; audit logs; Network Monitoring	audit logs; Network Monitoring	NW IDS; H Preventior
			Incident Response - Execution	audit logs; Configuration Management; Account Management			sinkhole
			Incident Response - Execution; control of HW, SW inventory				

Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Estab
ation is s some ut the he application b pages, code erences to plication and s on the web k.	Moderately skilled hackers may develop scripts to execute data queries through web browsers or scripts. **Asset:** Out of our control.	Attempts at running scripts or direct reference to commands and data objects on the web application, such as SQL injection. **Asset:** Web application, application server, database server, and event logs.	Data exfiltration through the web app, or data exfiltration directly from the database server. **Asset:** Database server, application server.	Not applicable	Not applicable	Not applicable	Not applic
ation is s some ut the he application b pages, code erences to plication and s on the web k.	Highly skilled hackers may develop scripts to execute commands through application or database services. **Asset:** Out of our control.	Attempts at running scripts or direct reference to commands and data objects on the web server, such as bash. **Asset:** Application server, database server, and event logs.	Commands executed through application account. Files added, altered, or replaced. **Asset:** Application server, database server, and event logs.	Execution of sudo or runas, establishment or alteration of existing account. **Asset:** User accounts, administrative accounts.	Directory traversal at the web server. **Asset:** Application server, event logs.	Commands at the application server. **Asset:** Application server, event logs.	Installation establishm **Asset:** Op event logs administra
ine who in the s access to ation. formation and es that describe esponsibilities.	Moderately skilled hackers may develop phishing email and ransomware exploits that target selected personnel. **Asset:** Out of our control.	Hacker sends phishing email to selected personnel. **Asset:** Email server, SMTP gateway.	Personnel open phishing email and trigger an install of the ransomware payload. **Asset:** Email client, end-user OS, personnel, proxy server, advanced malware appliance.	Malware encrypts the local storage volume. **Asset:** End-user OS, storage volume.	Not applicable	Not applicable	See Misus

DoCRA Practically Applied: CIS RAM

Thank You

Chris Cronin

HALOCK Security Labs

ccronin@halock.com