



The Industry Risk Assessment Disconnect and the Solution

Jim Mirochnik

CAMPIT – October 3rd 2018

Jim Mirochnik, MBA, PCI QSA, PMP, ISO 27001 Auditor



Some of My Passions & Interests



"I've lived through many catastrophes in my life, some of which actually happened."
- Mark Twain



What we're going to cover today



The Industry Disconnect



What Makes This a Problem



Why This is Important



A Better Way



How It Works



What Next?

The Industry Disconnect



We have been **missing the connection** between our:

Risk Assessments and
What is expected of us
from our **legal system**
(*judges, regulators,
etc.*)

The cornerstone of information security management is **Risk Management**

Problem #1:

Some organizations are not performing Risk Assessments regularly.

Problem #2:

Our Risk Assessments are being performed with too narrow of a perspective.





Traditional Risk Assessments

- Utilize a standard definition of Risk:

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$

- Calculate Impacts using the categories of **Confidentiality, Integrity, Availability (CIA)**

- **Traditional Risk Assessments** calculate impacts to
 - (A) your organization and
 - (B) in technical terms (CIA)!

Here is what is wrong with that!

- **Judges and regulators** are concerned with impacts
 - (A) beyond to just **YOU** and
 - (B) impacts in business terms.

There is a bigger problem than this narrow perspective.

We are not making the connection between the language of InfoSec and the language that the legal system utilizes.

Five Important Legal Language Terms

- 1 Reasonable Person refers to a party that exercises care, skill and judgment to protect others from harm during their normal course of business.
- 2 Duty of Care refers to the responsibility that a reasonable person has to avoid harm to another. *Example: shoveling snow from your sidewalk*
- 3 Due Care means that safeguards are used to protect others in a way that is “reasonable” and “appropriate.”
- 4 Reasonable to the organization (the safeguard’s burden is not greater than the risk it protects against)
- 5 Appropriate to all parties (risk that is low enough that all potentially harmed parties would accept it)

Why This is Important

Defining **Duty of Care** in your Risk Assessment is the key!

So what is the downside of not evaluating against **Duty of Care** in our Risk Assessments?

- **Executives** are asking for the balance that Duty of Care demonstrates.
- **Regulators** evaluate compliance using Duty of Care.
- **Judges** evaluate negligence by evaluating Duty of Care and will ask these eight questions.

What Judges Will Ask You After Your Breach

Will you be able to answer them?

1. Was the threat foreseeable?
2. Did you consider the harm it could have caused?
3. Did the breach victims benefit from your use of their data?
4. What benefit did you gain from your use of the data?
5. What alternative safeguards would have mitigated the risk?
6. Would those alternative safeguards have imposed an undue burden on you?
7. How well would these alternative safeguards have reduced the risk of harm?
8. Would the proposed safeguards have created other undesirable risks?

WHAT IS YOUR DEFINITION OF ACCEPTABLE RISK?

Define yours.

Why This is Important



TARGET



UPMC

University of Pittsburgh
Medical Center



Three Case Studies
Involving Duty of Care

Why This is Important



TARGET



- Had a breach
- Did they use Duty of Care?

NO

- The verdict / judgment

\$150M+ in fines and settlements

That doesn't even include brand damage!



Why This is Important



- Real damages to employees
- Did they use Duty of Care?
YES
- The verdict/judgment
No negligence

Why Is This Important?






- No breach or damages
- Did they use Duty of Care?

NO

- The verdict/judgment
\$100M fine

Why Is This Important?

What is the **common theme** through all three examples?

	<u>Duty of Care Observed?</u>	<u>Results</u>
 TARGET	No	Fines and lawsuits
 UPMC University of Pittsburgh Medical Center	Yes	No Fines
 LifeLock®	No	Fines

Duty of Care provides protection with or without a breach!

A Better Way

- It's not enough to just do a risk assessment.
- Your risk assessment must be based on your **Duty of Care** or you are exposed.
- **DoCRA** is a new standard for Duty of Care Risk Analysis (<https://docra.org>)

DoCRA



A Better Way

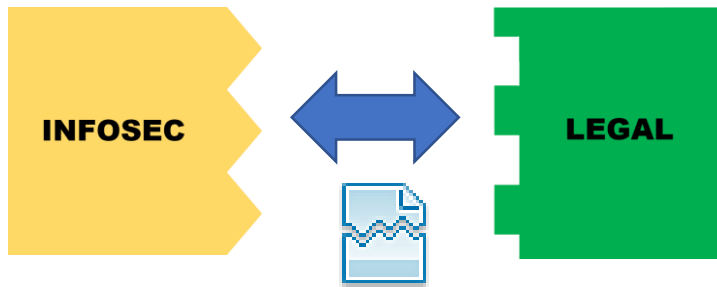
Before



Now

- We had a missing connector
- We had an industry disconnect

- We have that connector
- We have a solution



DoCRA is the connector between InfoSec and what our Legal System is requiring of us

DoCRA +  CIS Controls™ = CIS RAM

- [CIS RAM](#) is the first implementation of **Duty of Care Risk Analysis (DoCRA)** in the information security industry.
- CIS RAM launched by **CIS® (Center for Internet Security)** in April 2018.
- One of four Risk Frameworks on SANS Institute and CIS Posters.
- Becoming the standard by which federal regulators and state Attorneys General evaluate negligence in breach cases.

A Better Way

DoCRA is what makes the **legal connection**



Evaluates Duty of Care



Method	Standard of Care	Identifies Vulnerabilities	Considers Threats	Evaluates Harm to Self	Evaluates Harm to Others	Estimates Likelihood	Defines Acceptable Risk	Defines Reasonableness	Evaluates Safeguard Risk
DoCRA CIS RAM	●	●	●	●	●	●	●	●	●
IT Risk Assessments ISO27005, NIST SP800-30, RISK IT	●	●	●	●	◐	●	○	○	◐
FAIR Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	●	◐	○	○	○	○	○	○	○
Maturity Model Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	○	○	○	○

Why do **Judges** like Duty of Care Risk Analysis?



- Gives judges a **clear-cut definition** if a defendant was negligent.
- Judges by law have to balance the defendant's burden against harm to others.
- This is encoded as the “**Hand Rule**” or “**Calculus of Negligence.**”

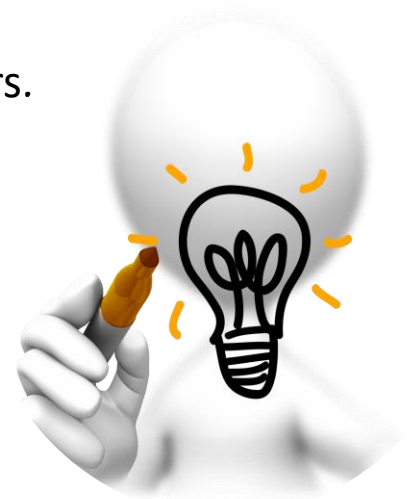
A risk is reasonable if

$$\text{Burden} < \text{Impact} \times \text{Likelihood}$$

- **Multi-factor balancing tests** are how duty of care and due care are determined.

Why do **Regulators** Like Duty of Care Risk Analysis?

- Since **1993** regulations are required to balance **cost and benefit**.
- “**Executive Order 12866**” has been in effect for the past 25 years.
 - HIPAA Security Rule
 - Gramm Leach Bliley Act
 - Federal Trade Act
 - 23 NYCRR Part 500, and most state regulations.
- Regulations have since then included the terms “**risk**,” “**reasonable**,” and “**appropriate**” to indicate the cost-benefit standard for compliance.



We can't explain it
all in an hour,

But here are
the basics ...



- DoCRA broadens that narrow perspective of impact definitions to evaluate your Duty of Care Impacts across three perspectives:
 - Your Mission: What you do for the world.
 - Your Objectives: What you do for yourself.
 - Your Obligations: The care you owe others.
 - A DoCRA based Risk Assessment calculates impacts **(A) across these three perspectives and (B) in business terms.**



ACME Memorial Hospital Calculated Acceptable Risk Definition (CARD)

How it Works: Example

Impact Score	Mission: Patient Care	Objectives: Balanced Budget	Obligation: Patient Data
1. Negligible	No impact to patient care	\$0.00	No impact to patient confidentiality
2. Acceptable	Patient may feel inconvenienced	Up to \$250,000	Creates no harm to patient
3. Unacceptable	Few patient records may be altered	Above \$250,000 Up to \$1,000,000	May create harm to fewer than 100 patients
4. High	“Sentinel event” or need for transfer to hospital	Above \$1,000,000 Up to \$5,000,000	May create harm to more than 100 patients
5. Catastrophic	Death of a patient	Over \$5,000,000	Create harm on a repeated, or continuous basis

Likelihood Score	Likelihood Definition
1	Not foreseeable
2	Foreseeable, but not expected
3	Expected to occur at some time
4	A common occurrence
5	Continuous

Decision Matrix

	Impact				
Likelihood	1	2	3	4	5
1	Green	Green	Green	Green	Green
2	Green	Green	Green	Green	Red
3	Green	Green	Red	Red	Red
4	Green	Green	Red	Red	Red
5	Green	Red	Red	Red	Red



How it Works: Maturity Assessment

Example 1 – Maturity Assessment

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication (MFA)			
Asset	Patient Record Application	Current Control	User name and password required for log-in
Maturity	1 (on a Scale of 1 to 5)		

- **Judge Comments:** *“This looks bad. Is 1 enough? Where should you be? You clearly are not implementing this control.”*
- **Regulator Comments:** *“1 out of 5, you are not following the regulation.”*
- **Management Comments:** *“If the doctors don’t want MFA, can I accept this risk?”*

- **NO** Does this protect you?
- **NO** Does this support decision making?
- **NO** Does this provide consistency?



How it Works: Maturity Assessment

Example 1 – Maturity Assessment

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication		
Asset	Patient Record Application	Current Control Implementation: Password
Maturity	1 (on a Scale of 1 to 5)	

- **Judge Comments:** *"This looks good, but how should you be? You clearly are not implementing this control."*
- **Regulator Comments:** *"You are not following the regulation."*
- **Management Comments:** *"My doctors don't want MFA, can I accept this risk?"*

YES Does this protect you?

YES Does this support decision making?

NO Does this provide consistency?



How it Works: Gap Assessment/Audit

Example 2 – Gap Assessment / Audit

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication (MFA)			
Asset	Patient Record Application	Current Control	User name and password required for log-in
Gap	Management does not require users to log in with MFA	Remediation	Implement MFA on all sensitive applications, such as patient record

- **Judge Comments:** *“You have a gap. You clearly are not implementing this control.”*
- **Regulator Comments:** *“You have a gap, you are not following the regulation.”*
- **Management Comments:** *“This auditor is impossible to please. Our doctors will never go for it, they hate MFA. Can I accept this risk?”*

- **NO** Does this protect you?
- **NO** Does this support decision making?
- **NO** Does this provide consistency?



How it Works: Gap Assessment/Audit

Example 2 – Gap Assessment / Audit

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication			
Asset	Patient Record Application	Current Control	Multi-factor authentication is required
Gap	Management does not require remote users to log in with MFA	Impact	Applications, such as patient record

- **Judge Comments:** *"You have not started implementing this control."*
- **Regulator Comments:** *"You have a gap you are not following the regulation."*
- **Management Comment:** *"The regulator is impossible to please. Our doctors will never go for it, even with MFA. Can I accept this risk?"*

NO Does this protect you?

NO Does this support decision making?

NO Does this provide consistency?



A Better Way: Traditional Risk Assessment

Example 3 – Traditional Risk Assessment

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication on Sensitive Applications			
Asset	Patient Record Application	Current Control	User name and password required for log-in
Vulnerability	User name and password is the only requirement to log in	Threat	Hackers may guess or acquire user credentials, log-in and steal patient data
Likelihood	Medium	Impact	High
Remediation	Implement MFA on all sensitive applications, such as the patient record		

- **Judge Comments:** *“You have high risk, yet you are not implementing this control.”*
- **Regulator Comments:** *“You have high risk, yet are not following the regulation.”*
- **Management Comments:** *“This risk assessment tells us we have to use MFA. Our doctors will never go for it, they hate MFA. Can I accept this risk?”*

- **NO** Does this protect you?
- **NO** Does this support decision making?
- **NO** Does this provide consistency?



A Better Way: Traditional Risk Assessment

Example 3 – Traditional Risk Assessment

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication on Servers and Applications			
Asset	Patient Record Application	Current Control	User name and password required to log-in
Vulnerability	User name and password is the only requirement to log in	Threat	Malicious users can impersonate user and steal patient data
Likelihood	Medium	Impact	High
Remediation	Implement MFA on all servers, applications, and patient record		

- **Judge Comments:** "You have high risk, so you have to be implementing this control."
- **Regulator Comments:** "You have high risk, but you are not following the regulation."
- **Management Comments:** "This risk assessment tells us we have to use MFA. Our doctors will never go for it. They have to say 'Can I accept this risk?'"

NO Does this protect you?

NO Does this support decision making?

NO Does this provide consistency?



A Better Way: DoCRA Risk Assessment #1

Example 4 – DoCRA-based Risk Assessment with Safeguard #1

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication on Sensitive Applications			
Asset	Patient Record Application	Current Control	User name and password required for log-in
Vulnerability	User name and password is the only requirement to log in	Threat	Hackers may guess or acquire user credentials, log-in and steal patient data
Mission Impact		Objectives Impact	
(3) - Unacceptable. Few patient records may be altered		(2) - Acceptable. Our ability to achieve 10-year plan is marginally interrupted	
		Obligations Impact	
		(4) - High. May create harm to more than 100 patients	
Likelihood		Risk Score: Max(Impact) x Likelihood	
(3) Foreseeable and Expected		$3 \times 4 = 12$	
		12	

Safeguard #1	Implement MFA on all sensitive applications, such as the patient record		
Safeguard #1 Risk	Physicians will have a difficult time accessing patient records while at off-site clinics using mobile app version of the patient record. If doctors do not have second factor tokens with them when patients are acutely ill, doctors would not be able to access patient records, thus compromising patient health.		
Mission Impact		Objectives Impact	
(4) – High. “Sentinel event” or need for transfer to hospital		(2) - Acceptable. Our ability to achieve 10-year strategic plan is marginally interrupted	
		Obligations Impact	
		(4) - High. May create harm to more than 100 patients	
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
(4) A common occurrence		$4 \times 4 = 16$	
		16	



How it Works: DoCRA Risk Assessment #2

Example 4 – DoCRA-based Risk Assessment with Safeguard #2

CIS Control 12.1 Require All Remote Login to Use Multi-factor Authentication on Sensitive Applications			
Asset	Patient Record Application	Current Control	User name and password required for log-in
Vulnerability	User name and password is the only requirement to log in	Threat	Hackers may guess or acquire user credentials, log-in and steal patient data
Mission Impact		Objectives Impact	
(3) - Unacceptable. Few patient records may be altered		(2) - Acceptable. Our ability to achieve 10-year plan is marginally interrupted	
		Obligations Impact	
		(4) - High. May create harm to more than 100 patients	
Likelihood		3 x 4 = 12	Risk Score: Max(Impact) x Likelihood
(3) Foreseeable and Expected		12	

Safeguard #2	Configure the application to present and remotely store only the records that are needed for patient visit.		
Safeguard #2 Risk	If mobile device is lost or stolen, few than 100 records could be exposed if passwords are guessed, and lost-device-data-wipe process fails.		
Mission Impact		Objectives Impact	
(1) - Negligible. Patient health outcomes would not be effected		(2) - Acceptable. Our ability to achieve 10-year strategic plan is marginally interrupted	
		Obligations Impact	
		(2) - Acceptable. Up to 100 patients may have their records exposed	
Likelihood		3 x 2 = 6	Safeguard Risk Score: Max(Impact) x Likelihood
(3) Foreseeable and Expected		6	



How it Works: DoCRA Risk Assessment #2

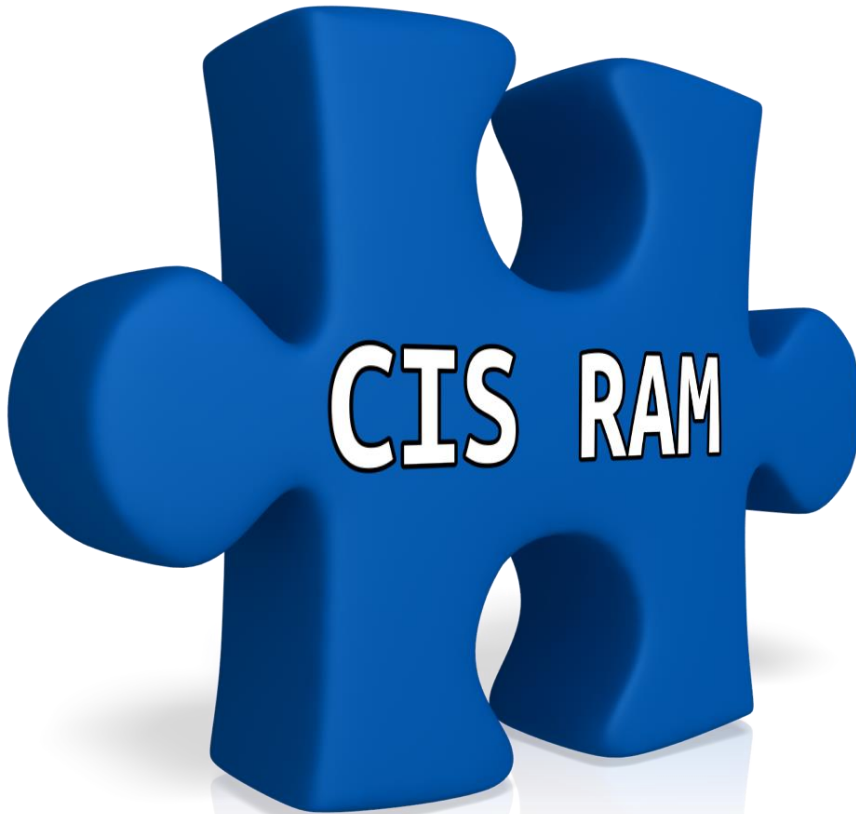
Example 4 – DoCRA-based Risk Assessment with Safeguard #2

Safeguard #2	Configure the application to present and remotely store only the records that are needed for patient visit.		
Safeguard #2 Risk	If mobile device is lost or stolen, few than 100 records could be exposed if passwords are guessed, and lost-device-data-wipe process fails.		
Mission Impact	Objectives Impact	Obligations Impact	
(1) - Negligible. Patient health outcomes would not be effected	(2) - Acceptable. Our ability to achieve 10-year strategic plan is marginally interrupted	(2) - Acceptable. Up to 100 patients may have their records exposed	
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
(3) Foreseeable and Expected		3 x 2 = 6	6

- **Judge Comments:** “MFA would have been too burdensome. The safeguard you used is Reasonable.”
- **Regulator Comments:** “This safeguard addresses the Risk in a Reasonable way.”
- **Management Comments:** “Of course I can accept this risk, it protects everyone.”

- **YES** Does this protect you?
- **YES** Does this support decision making?
- **YES** Does this provide consistency?

What Next?



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

For Reasonable Implementation and
Evaluation of CIS Controls™

Good News
You can
download
CIS RAM for FREE!

What Next?


- ❑ **Step 1:** Download CIS RAM from [cissecurity.org](https://learn.cisecurity.org/cis-ram)
(<https://learn.cisecurity.org/cis-ram>)

- ❑ **Step 2:** Determine if you should
 - (a) *Upgrade* your current security assessments to DoCRA
 - or
 - (b) *Perform a new* DoCRA-based Risk Assessment



What Next?

You do not need to start from scratch. Upgrade your existing Risk Assessment to DoCRA, utilizing your existing threats, vulnerabilities, etc.

Method	Standard of Care	Identifies Vulnerabilities	Considers Threats	Evaluates Harm to Self	Evaluates Harm to Others	Estimates Likelihood	Defines Acceptable Risk	Defines Reasonableness	Evaluates Safeguard Risk
 DoCRA CIS RAM	●	●	●	●	●	●	●	●	●
IT Risk Assessments ISO27005, NIST SP800-30, RISK IT	●	●	●	●	◐	●	○	○	◐
FAIR Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	●	◐	○	○	○	○	○	○	○
Maturity Model Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	○	○	○	○

Upgrade Your Risk Assessment to DoCRA (Green bracket)

New DoCRA Risk Assessment (Purple bracket)

What Next?

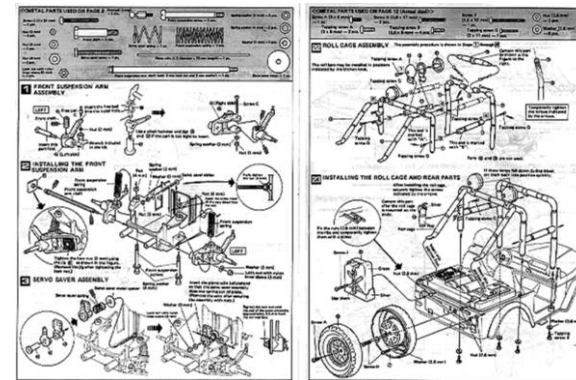
- ❑ **Step 1:** Download CIS RAM from [cissecurity.org](https://learn.cisecurity.org/cis-ram) (<https://learn.cisecurity.org/cis-ram>)
- ❑ **Step 2:** Determine if you should
 - (a) *Upgrade* your current security assessments to DoCRA
 - or
 - (b) *Perform a new* DoCRA based Risk Assessment
- ❑ **Step 3:** Define your implementation team (internal team members and/or hire a professional to help)



- What are three of the scariest words for most adults?

“Some Assembly Required”

- Don't get frustrated. This can be complicated, especially the first time.
- Our recommendation - The stakes are high. **Get a professional to help you!**





Questions

Jim Mirochnik *Senior Partner*

Todd Becker *Principal Consultant*



Appendix

Why is Duty of Care Important to Judges?

To satisfy the Multi-Factor Balancing Tests Used in Courts.

- What controls and vulnerabilities **were in place**?
- What was the impact and likelihood of the **plaintiff's harm**?
- What was the **plaintiff's relationship** to the defendant?
- What **benefit** came with the risk?
- Were **alternative safeguards** evaluated?
- Would the alternatives have created a **burden that was greater than the risk**?





A Better Way

How Will a Judge Interpret **Maturity Model** Assessments?

Judge: Plaintiff claims that your data breach could have been stopped if you had used a DLP system. You were not using one. Can you explain why?

You: When we evaluated our data leakage controls, we were at a '3' and we decided that we didn't need to go to '4'.

Judge: Why? Was the burden of the control greater than the risk to the plaintiff?

You: Ummm. We agreed not to go to '4'.



A Better Way

How Will a Regulator Interpret **Gap** Assessments?

Regulator: Why are you not segmenting your PII network from your corporate network?

You: When we identified that gap our CISO accepted the risk.

Judge: What standard did you use to accept risk? Did your clients agree with this acceptance criteria?

You: ... No.



A Better Way

How Will a Regulator Interpret **FAIR** Assessments?

Regulator: Nice job evaluating the threat. I see the dollar value of your potential losses. But I don't think this control is appropriate for the risk.

You: Well, you can see by this heat map over here, our probable loss is low.

Regulator: Your probable loss? I'm here to protect the public, not your profits.

You: ...