CIS RAM:
This Math Will Save You

Presented by: Chris Cronin
HALOCK Security Labs

August 29, 2018

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 Certifications

Purpose of Today's Presentation

- Everyone needs a risk assessment.
- Your risk assessment must be based on your Duty of Care or you are exposed.
- CIS® has published a method based on **Duty of Care Risk Analysis ("DoCRA")** to protect you.

HALOCK®
Purpose Driven Security

ALTERNATIVE TITLE

The Questions a Judge Will Ask You the Day You Are Sued for a Data Breach

Presented by: Chris Cronin
HALOCK Security Labs

August 29, 2018

HALOCK®
Purpose Driven Security

ALTERNATIVE TITLE

Translating Cyber Security For the Board Room

Presented by: Chris Cronin
HALOCK Security Labs

August 29, 2018

HALOCK®
Purpose Driven Security

ALTERNATIVE TITLE

How Your Security Assessments Annoy Your Regulator

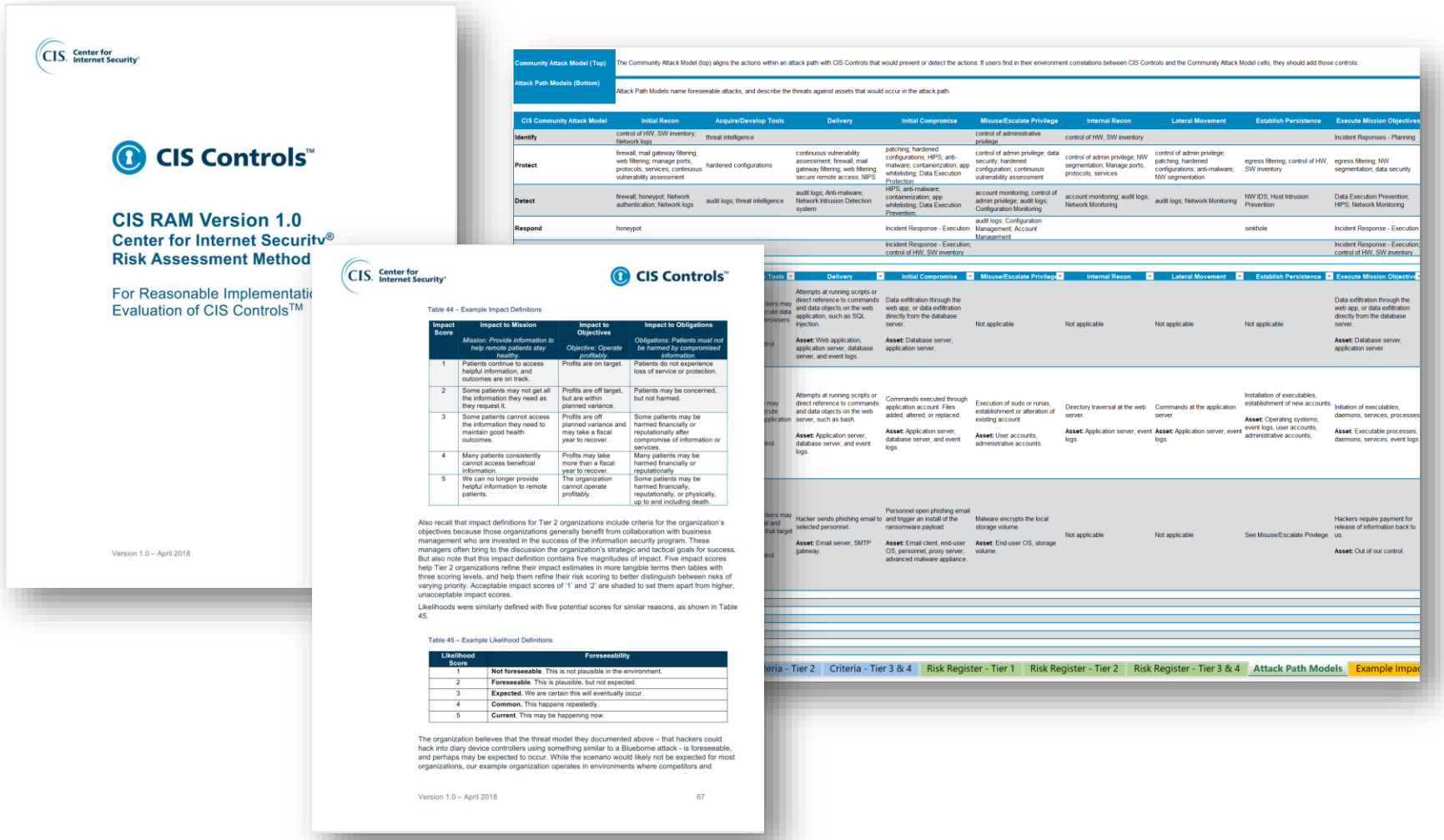
Presented by: Chris Cronin
HALOCK Security Labs

August 29, 2018

How Current Security Assessments Are Failing Us

	Evaluates Risk to Information Assets						Evaluates Due 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 ISO 27005, NIST SP 800-30, RISK IT	●	●	●	●	◑	●	○	○	◔
FAIR Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	●	◑	○	○	○	○	○	○	○
Maturity Model Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	○	○	○	○

CIS RAM



What is CIS RAM?

- Detailed instructions for conducting cyber security risk assessments.
- Instructions for defining acceptable risk.
- Aligned with judicial and regulatory understanding of “reasonable” and “appropriate.”
- Workbook with templates and examples.
- Based on new **Duty of Care Risk Analysis (“DoCRA”)** standard.

Where You'll See CIS RAM / DoCRA

- Announced by CIS in April, 2018.
- SANS Institute and CIS Posters.
- Law suits by states' Attorneys General after security breaches.
- Adoption by MS-ISAC member states.
- Other adoption steps in progress …

CIS RAM and DoCRA Principles

1. Risk analysis must consider the interests of all parties that may be harmed by the risk.
2. Risks must be reduced to a level that authorities and potentially affected parties would find appropriate.
3. Safeguards must not be more burdensome than the risks they protect against.

Being Judged

Oops

- How do *you* determine when cyber security risk is acceptable?
- What if that's your judge?
- What if that's your regulator?
- What if that's your CEO or a Board Director?
- Not a comfortable feeling, right?

What is Risk Analysis?

- **Risk Analysis:** What is the likelihood of harm to ourselves and others that is caused by a threat?
- **Acceptable risk:** The likelihood of harm that ourselves and others would accept.

Let's Illustrate … *simple*

	Our Profit	**Customer Financial Privacy**
Acceptable	*Profit plan is on track*	*No financial harm*
Unacceptable	*Not profitable*	*Money lost or credit rating hurt*

Harm to us

Harm to others

Let's Illustrate … *terrible*

	Our Profit	**Customer Financial Privacy**
Acceptable	*Up to $5,000,000*	*Up to $5,000,000*
Unacceptable	*Over $5,000,000*	*Over $5,000,000*

DON'T ASSUME OTHERS' RISK TOLERANCE EQUALS YOURS!

Let's Illustrate … *simple*

	Our Profit	**Customer Financial Privacy**
Acceptable	*Profit plan is on track*	*No financial harm*
Unacceptable	*Not profitable*	*Money lost or credit rating hurt*

Be Prepared to Compare Unlike Things

Let's Illustrate … *practical*

	Our Profit	**Customer Financial Privacy**
Negligible	*Profit plan is unaffected.*	*No financial harm.*
Acceptable	*Profit plan within planned variance.*	*Encrypted or unusable information cannot create harm.*
Unacceptable	*Not profitable. Recoverable within the year.*	*Recoverable money lost or credit rating hurt among few customers.*
High	*Not profitable. Recoverable in multiple years.*	*Financial harm among many customers.*
Catastrophic	*Cannot operate profitably.*	*Cannot protect customers from harm.*

Establishing Impact Definitions

- To evaluate balance well, define these things:
  - Your **Mission**:

    What makes the risk worth it for others?
  - Your **Objectives**:

    What are your indicators of success?
  - Your **Obligations**:

    What care do you owe others?

Some Common Impact Criteria

Industry Example	Mission	Objectives	Obligations
Commercial Bank	Financial performance	Return on assets	Customer financials
Hospital	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

Bank's Full Risk Assessment Criteria

Impact Score	Mission "Financial Performance"	Objectives "Return on Assets"	Obligation "Customer Financials"
1. Negligible	Customer returns at or above market.	Maintain RoA targets.	Customer finances not harmed.
2. Low	Customer returns at market by end of fiscal year.	RoA performance within planned variance.	Customer info released, but cannot cause harm.
3. Medium	One product underperforms against market after a year.	Missed RoA targets up to 1%	Recoverable harm caused to few customers.
4. High	Multiple products under perform for multiple years.	Missed RoA targets up to 5% for multiple years.	Recoverable harm caused to thousands or more customers.
5. Catastrophic	Cannot meet market returns.	Cannot earn sufficient RoA to operate.	We cannot safeguard financial information.

Likelihood Score	Likelihood Definition
1	Not foreseeable
2	Foreseeable but unexpected
3	Expected, but rare
4	Expected occasionally
5	Common

Plain Language	Score
Invest against risk	3 x 3 = **9**
Accept Risk	**< 9**

Hospital's Full Risk Assessment Criteria

Impact Score	Mission "Health Outcomes"	Objectives "Balanced Budget"	Obligation "Patient Privacy"
1. Negligible	Health outcomes would not be effected.	Budget would not be effected.	Patients' privacy would not be harmed.
2. Low	Patients would feel inconvenienced.	Budget performance within planned variance.	Patients would be concerned, but no harm would result.
3. Medium	Some patient's health outcomes would suffer.	Budget variance would be recoverable within a year.	Few patients would suffer reputational or financial harm
4. High	Many patient health outcomes would suffer.	Budget would be recoverable after multiple years.	Many patients would suffer reputational or financial harm.
5. Catastrophic	Patients could not rely on positive health outcomes.	We would not be able to financially operate.	We would not be able to safeguard patient information.

Likelihood Score	Likelihood Definition
1	Not foreseeable
2	Foreseeable but unexpected
3	Expected, but rare
4	Expected occasionally
5	Common

Plain Language	Score
Invest against risk	3 x 2 = **6**
Accept Risk	**< 6**

Hey! You're Using Ordinals!

- "Selecting values '1' through '5' may be simple, but they do not indicate probability."

- CIS RAM and DoCRA can be conducted using probability analysis too.
  - Just stick with the principles and practices listed in CIS RAM and the DoCRA Standard.

Example 1 – Inappropriate Risk

CIS Control 1.1 - Utilize an Active Discovery Tool			
Asset	All routable devices	Owner	IT
Vulnerability	Sporadic asset scans	Threat	Undetected compromised systems
Risk Scenario	Irregular asset scans may not identify compromised systems that join the network and attack routable systems.		

Mission Impact	Objectives Impact	Obligations Impact
2	3	3

Likelihood	Risk Score: Max(Impact) x Likelihood
3	9

Safeguard	Implement NAC, and a system assessment process for alerted devices.
Safeguard Risk	A moderate cost would have minimal impact on the budget. Installation of the tool is likely not disruptive.

Mission Impact	Objectives Impact	Obligations Impact
1	2	1

Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
4	8

Example 2 – Unreasonable Safeguard

Control 14.4 - Encrypt All Sensitive Information in Transit			
Asset	Web applications	Owner	Product Management
Vulnerability	Inter-server PII in plain text	Threat	Sniffers can capture PII
Risk Scenario	Hackers place packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		

Mission Impact	Objectives Impact	Obligations Impact
3	3	4

Likelihood	Risk Score: Max(Impact) x Likelihood
3	12

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.

Mission Impact	Objectives Impact	Obligations Impact
3	3	4

Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
4	16

Example 3 – Reasonable Safeguard

Control 14.4 - Encrypt All Sensitive Information in Transit			
Asset	Web applications	Owner	Product Management
Vulnerability	Inter-server PII in plain text	Threat	Sniffers can capture PII
Risk Scenario	Hackers place packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		

Mission Impact	Objectives Impact	Obligations Impact
3	3	4

Likelihood	Risk Score: Max(Impact) x Likelihood
3	12

Safeguard	Create a VLAN limited to the application server, database server, IPS sensor.
Safeguard Risk	Promiscuous sniffer would be detected by IPS if on those servers.

Mission Impact	Objectives Impact	Obligations Impact
1	2	1

Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
4	8

Why do Judges Like Duty of Care Risk Analysis?

- Gives judges a clear-cut definition of whether a defendant was negligent.
- Judges by law have to balance the defendant's burden against harm to others.
- Encoded as the "Hand Rule" or "Calculus of Negligence."
  - A risk is reasonable if "Burden < Probability x Likelihood"
- Multi-factor balancing tests are how **duty of care** and **due care** are determined.

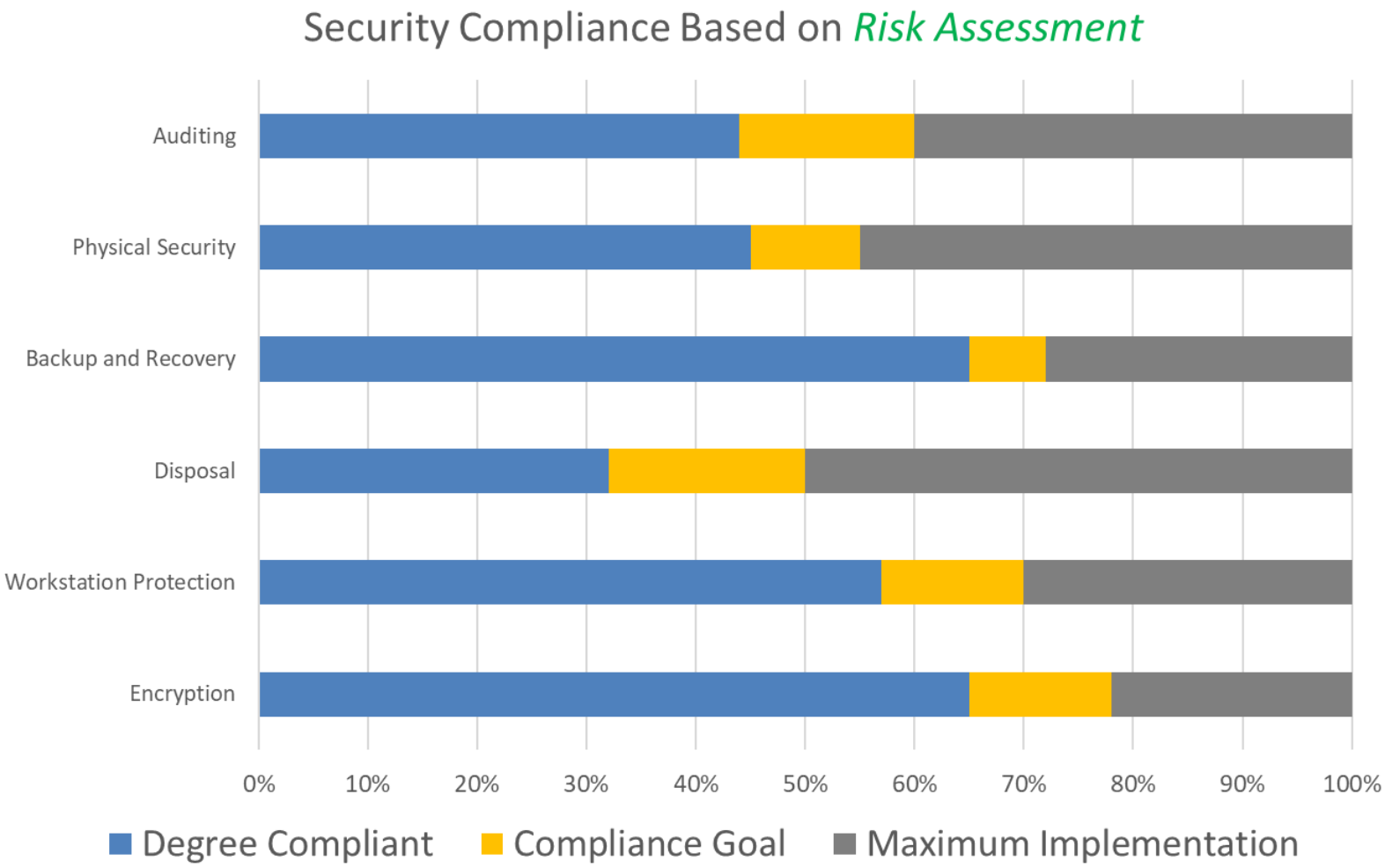
Multi-Factor Balancing Tests Used in Courts

- What controls and vulnerabilities were in place?
- What was the impact and likelihood of the defendant'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?

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.

Why do Executive Like Duty of Care Risk Analysis?



Are You Sure?
My Regulators Tell Me What To Do.

- Have you demonstrated due care yet?
- If you don't analyze risk to find reasonable controls … then they don't have much choice but to tell you what to do.

How Are Other Security Assessments Failing Us?

	Evaluates Risk to Information Assets						Evaluates Due 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 ISO 27005, NIST SP 800-30, RISK IT	●	●	●	●	◑	●	○	○	◔
FAIR Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	●	◑	○	○	○	○	○	○	○
Maturity Model Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	○	○	○	○

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'.

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.

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: …

How Do Organizations Adopt CIS RAM/DoCRA?

- Download CIS RAM from cisecurity.org
- Upgrade your current security assessments with duty-of-care components.
  - Develop risk assessment and acceptance criteria
  - Adding threat models to analysis
  - Evaluate harm to others
  - Evaluating safeguards to determine reasonableness
- Starting fresh with a new DoCRA-based risk assessment.

HALOCK®
Purpose Driven Security

Questions

Chris Cronin
ccronin@halock.com

https://learn.cisecurity.org/cis-ram

Resources

CIS RAM Download

CIS RAM Executive Prospectus

CIS RAM FAQ

Duty of Care Risk Analysis Standard (DoCRA)