

The Questions a Judge Will Ask You After a Data Breach: and How You Can Prepare for Them

Speaker:

- Chris Cronin, Principal Author - CIS RAM

Moderated by Barbara Boehler – Compliance Week



Agenda for Today's Webcast

This webcast will last for 60 minutes

2:00 p.m.	Introduction Barbara Boehler - Compliance Week
2:05 p.m.	Presentation Chris Cronin - CIS RAM
2:50 p.m.	Q&A
3:00 p.m.	Closing

Introduction

The Series, Schedule and Instructions

Upcoming Webcasts

Visit our website for future webcast dates and topics www.complianceweek.com

Instructions

▼ Ask a Question

Use the “Ask a Question” function (left side of your screen)

All questions will be anonymous

► Event Resources

To download today’s presentation, click on “Event Resources” dropdown menu on the left-hand side of your screen

CPE

Please disable your pop-up blockers to access the automatic CPE exam presented at the webcast conclusion

Sponsored by



Speaker



Chris Cronin

- Partner at HALOCK Security Labs
- Chair, the DoCRA Council
- Principal Author of CIS RAM and DoCRA Standard
- Member of the Sedona Conference - Working Group 11
- Expert witness to State Attorneys General
- Information Security Focus for 15 Years
 - Risk Assessments and Risk Management
 - Incident Response and Fraud Investigations
 - Governance and Internal Audit
 - ISO 27001 Certification

Three Lessons

LESSON 1 The Law and Business Are Not Adversaries.

LESSON 2 “**Reasonable**” Safeguards Are Up to Business to Define and Defend.

LESSON 3 “**Duty of Care Risk Analysis**” Defines Reasonable for Business, Law, and InfoSec.

Today's Message

- Judges (and regulators ... and security frameworks) are asking for “**reasonable**” controls.
- Judges and regulators will ask you questions to determine whether your controls were reasonable.
 - “**Reasonable**” is a **big gift** to business, if you know how to use it.
- It's about **balance** between protecting others and the burden of security controls.

Lesson 1:

The Law and Business are Not Adversaries

- Regulations and torts are often seen as *adversarial to business* ... legal matters that interfere with commerce and enterprise.
- U.S. law was born and shaped in an entrepreneurial culture. Statutes, regulations, and torts are *shaped to work with business*.
- Since 1993 federal regulations *require cost-benefit analysis* to justify their enforcement.
- Judges allow defendants to show if *safeguards balanced the potential of harm* against the burden they posed.

Balance

Potential of harm
to *others*



Potential of harm
from *burdens*

Balance in Regulations



Since 1993, regulations are required to be enforced using cost-benefit analysis. The burden of safeguards must not be greater than the harm to the public. (Executive Order 12866)

Since then, risk assessments have been required in regulations to identify “reasonable” controls.

Regulations That Require Risk Assessments and Reasonable Controls

- HIPAA Security Rule / HITECH
- Gramm Leach Bliley Act (Safeguards Rule)
- Massachusetts 201 CMR 17
- 23 NYCRR Part 500
- California Consumer Privacy Act
- Ohio Data Breach Law of 2018
- EU GDPR

Information Security Frameworks That Require Risk Assessments

- PCI DSS
- ISO 27001
- SOC 2 / SOC for Cybersecurity
- NIST Risk Management Framework (SP 800)
- NIST Cybersecurity Framework
- COSO/CobiT

Balance in Courts



Courts generally find negligence where the likelihood of harm **was greater** than the burden to prevent that harm.

Burden \leq Probability x Liability
("Learned Hand Rule" or "Calculus of Negligence")

Judges Use Balancing Tests in Law Suits to Determine Reasonableness of Safeguards

- “Did the defendant foresee the likelihood and magnitude of threats that harmed the plaintiff?”
- “Did the plaintiff use safeguards to reduce that likelihood and magnitude?”
- “Would the utility (benefit) of the risk have been jeopardized by alternative safeguards?”
- “Would the costs of safeguards have been greater than the risks?”
- “Did the defendant use a standard of care to design their safeguards?”






But Balance is Not Often Used in Security Assessments



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	●	○	○	○	○	○	○	○	○

Our Security Assessments Should Prepare Us For Judges and Regulators



This is what DoCRA Does

Duty of Care Risk Analysis (DoCRA)

- Freely available standard for assessing risk of any kind.
- Prepares subject matter experts to speak the language of laws and regulations.
- Qualitative method that can plug into other quantitative and qualitative risk frameworks.
- Made free to the public by HALOCK Security Labs in 2018.
- www.docra.org

DoCRA Principles (DoCRA Standard)

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.

CIS RAM



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

For Reasonable Implementation and
Evaluation of CIS Controls™

Version 1.0 – April 2018



Table 44 – Example Impact Definitions

Impact Score	Impact to Mission	Impact to Objectives	Impact to Obligations
	<i>Mission: Provide information to help remote patients stay healthy.</i>	<i>Objective: Operate profitably.</i>	<i>Obligations: Patients must not be harmed; computerized information.</i>
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 than 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.
5	Current. This may be happening now.

The organization believes that the threat model they documented above – that hackers could hack into diary device controllers using something similar to a Blueborne attack – is foreseeable, and perhaps may be expected to occur. While the scenario would likely not be expected for most organizations, our example organization operates in environments where competitors and

Version 1.0 – April 2018

67

Community Attack Model (Top)									
The Community 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, they should add those controls.									
Attack Path Models (Bottom)									
Attack Path Models name foreseeable attacks, and describe the threats against assets that would occur in the attack path.									
CIS Community Attack Model	Initial Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
Identify	control of HW, SW inventory, network logs	threat intelligence		control of admin privilege; patching, hardened configurations, HPS, anti-malware, containerization, app whitelisting, Data Execution Prevention	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 filtering, control of HW, SW inventory	Incident Response - Planning
Protect	firewall, mail gateway filtering, web filtering, manage ports, protocols, services, continuous vulnerability assessment	hardened configurations	continuous vulnerability assessment; firewall, mail gateway filtering, web filtering, secure remote access, NPS	HPS, 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, Host Intrusion Prevention	egress filtering, NW segmentation, data security
Detect	firewall, honeypot, Network authentication, Network logs	audit logs, threat intelligence	audit logs, Anti-malware; Network Intrusion Detection system	Incident Response - Execution, control of HW, SW inventory	Incident Response - Execution, control of HW, SW inventory			Incident Response - Execution, control of HW, SW inventory	Data Execution Prevention, HPS, Network Monitoring
Initial Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives	
Initial Recon is as is some about the e of the application (web pages, code d references to ems.	Moderately skilled hackers may develop scripts to execute data queries through web browsers or scripts.	Attempts at running scripts or direct reference to commands and data objects on the web application, such as SQL injection.	Data exfiltration through the web app, or data exfiltration directly from the database server.	Not applicable	Not applicable	Not applicable	Not applicable	Data exfiltration through the web app, or data exfiltration directly from the database server.	Asset: Database server, application server.
b application and notices on the web stack.	Asset: Out of our control.	Asset: Web application, application server, database server, and event logs.	Asset: Database server, application server.						
pplication is as is some about the e of the application (web pages, code d references to ems.	Highly skilled hackers may develop scripts to execute commands through application or database services.	Attempts at running scripts or direct reference to commands and data objects on the web server, such as bash.	Commands executed through application account. Files added, altered, or replaced.	Execution of sudo or runas, establishment or alteration of existing account.	Directory traversal at the web server.	Commands at the application server.	Installation of executables, establishment of new accounts.	Initiation of executables, daemons, services, processes.	Asset: Operating systems, event logs, user accounts, administrative accounts.
b application and notices on the web stack.	Asset: Out of our control.	Asset: Application server, database server, and event logs.	Asset: Application server, database server, and event logs.	Asset: User accounts, administrative accounts.	Asset: Application server, event logs.	Asset: Application server, event logs.	Asset: Executable processes, daemons, services, event logs.		
etermine who in the n has access to formation.	Moderately skilled hackers may develop phishing email and ransomware exploits that target selected personnel.	Hacker sends phishing email to selected personnel.	Personnel open phishing email and trigger an install of the ransomware payload.	Malware encrypts the local storage volume.	Not applicable	Not applicable	See Misuse/Escalate Privilege.	Hackers require payment for release of information back to us.	Asset: Out of our control.
ic information and asides that describe responsibilities.	Asset: Out of our control.	Asset: Email server, SMTP gateway.	Asset: Email client, end-user CIS, personnel, proxy server, advanced malware appliance.	Asset: End-user OS, storage volume.					

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 Center for Internet Security (CIS) in April, 2018.
- SANS Institute and CIS Posters.
- Law suits by state Attorneys General after security breaches.
- Adoption by MS-ISAC member states.
- New “DoCRA for ...” standards in development.

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?

Lesson 2:



Business Defines “Reasonable”

Because laws and regulations recognize that all organizations are different, then each organization must **define “reasonable” for themselves.**

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*

	<u>Our Profit</u>	<u>Customer Financial Privacy</u>
<u>Acceptable</u>	<i>Profit plan is on track</i>	<i>No financial harm</i>
<u>Unacceptable</u>	<i>Not profitable</i> 	<i>Money lost or credit rating hurt</i> 

Let's Illustrate ... *terrible*

	<u>Our Profit</u>	<u>Customer Financial Privacy</u>
<u>Acceptable</u>	<i>Up to \$5,000,000</i>	<i>Up to \$5,000,000</i>
<u>Unacceptable</u>	<i>Over \$5,000,000</i>	<i>Over \$5,000,000</i>

**DON'T ASSUME OTHERS' RISK
TOLERANCE EQUALS YOURS!**

Let's Illustrate ... *simple*

	<u>Our Profit</u>	<u>Customer Financial Privacy</u>
<u>Acceptable</u>	<i>Profit plan is on track</i>	<i>No financial harm</i>
<u>Unacceptable</u>	<i>Not profitable</i>	<i>Money lost or credit rating hurt</i>

Be Prepared to
Compare Unlike Things

Let's Illustrate ... *practical*

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

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 = <u>9</u>
Accept Risk	< <u>9</u>

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	$3 \times 2 = \underline{6}$
Accept Risk	$< \underline{6}$

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) Customer returns at-market		(3) Missed RoA targets up to 1%	(3) Recoverable harm to few customers.
Likelihood		Risk Score: Max(Impact) x Likelihood	
(3) Expected, but rare		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) Customer returns above market		(2) RoA within planned variance	(1) Customer finances not harmed
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
(4) Expected occasionally		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) One product underperforms YoY		(3) Missed RoA targets up to 1%	(4) Recoverable harm to thousands of customers
Likelihood		Risk Score: Max(Impact) x Likelihood	
(3) Expected, but rare		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) One product underperforms YoY		(3) Missed RoA targets up to 1%	(4) Recoverable harm to thousands of customers
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
(4) Expected occasionally		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) One product underperforms YoY		(3) Missed RoA targets up to 1%	(4) Recoverable harm to thousands of customers
Likelihood		Risk Score: Max(Impact) x Likelihood	
(3) Expected, but rare		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) Customer returns above market		(2) RoA within planned variance	(1) Customer finances not harmed
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
(4) Expected occasionally		8	

Lesson 3:

DoCRA Defines Reasonable for Business, Law, and InfoSec.

Because DoCRA

- Follows the rules of these three disciplines.
- Addresses what matters to each discipline.

Why do Judges Like Duty of Care Risk Analysis?

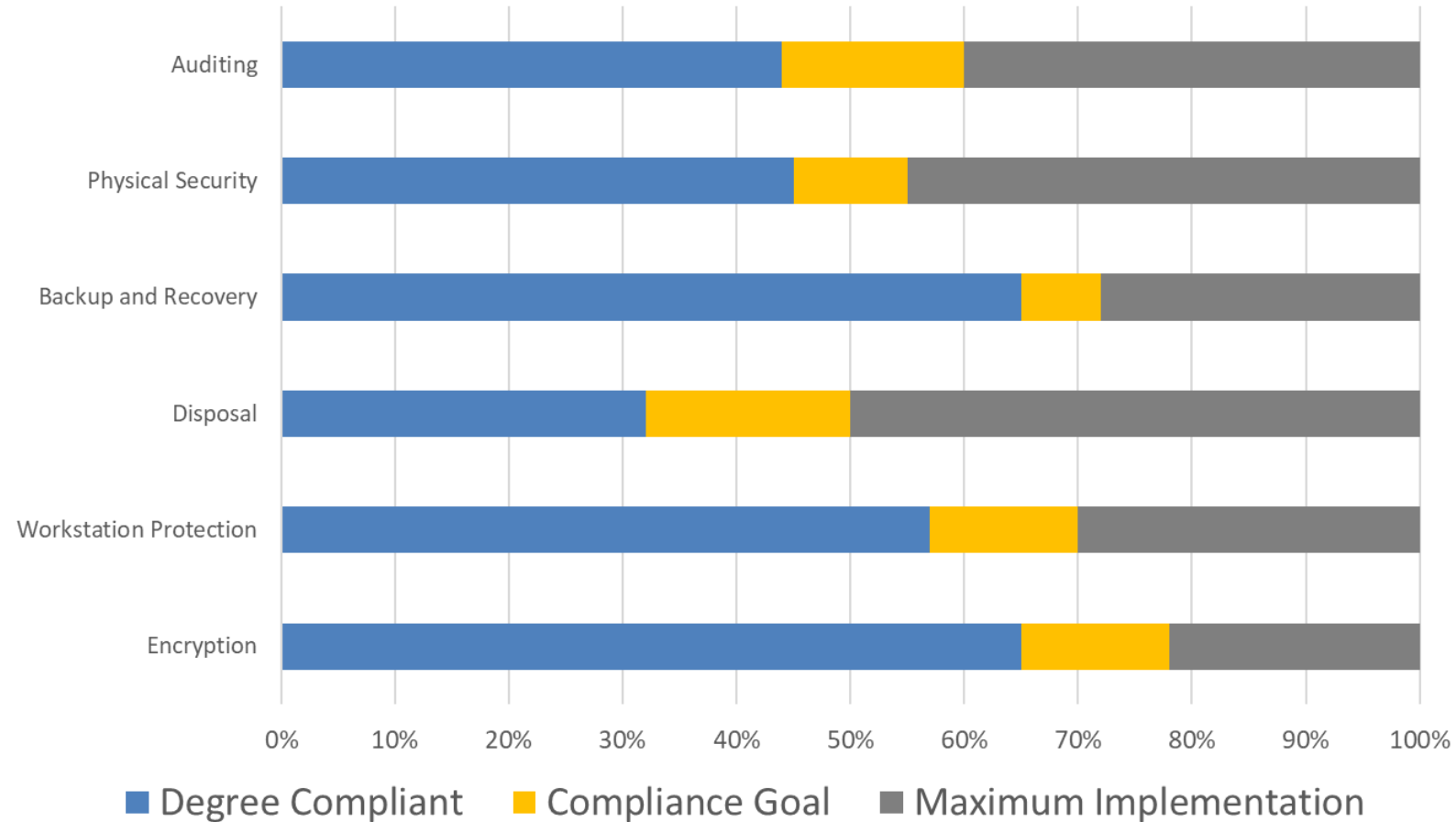
- Gives judges a clear-cut test for whether a defendant was negligent.
- Judges by law have to balance the defendant's burden against harm to others.
- Encoded as the “Hand Rule” or “Calculus of Negligence.”
 - A risk is reasonable if “Burden < Probability x Likelihood”
- Multi-factor balancing tests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

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?

Security Compliance Based on *Risk Assessment*



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?

Method	Evaluates Risk to Information Assets						Evaluates Due Care		
	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.

Regulator: 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?

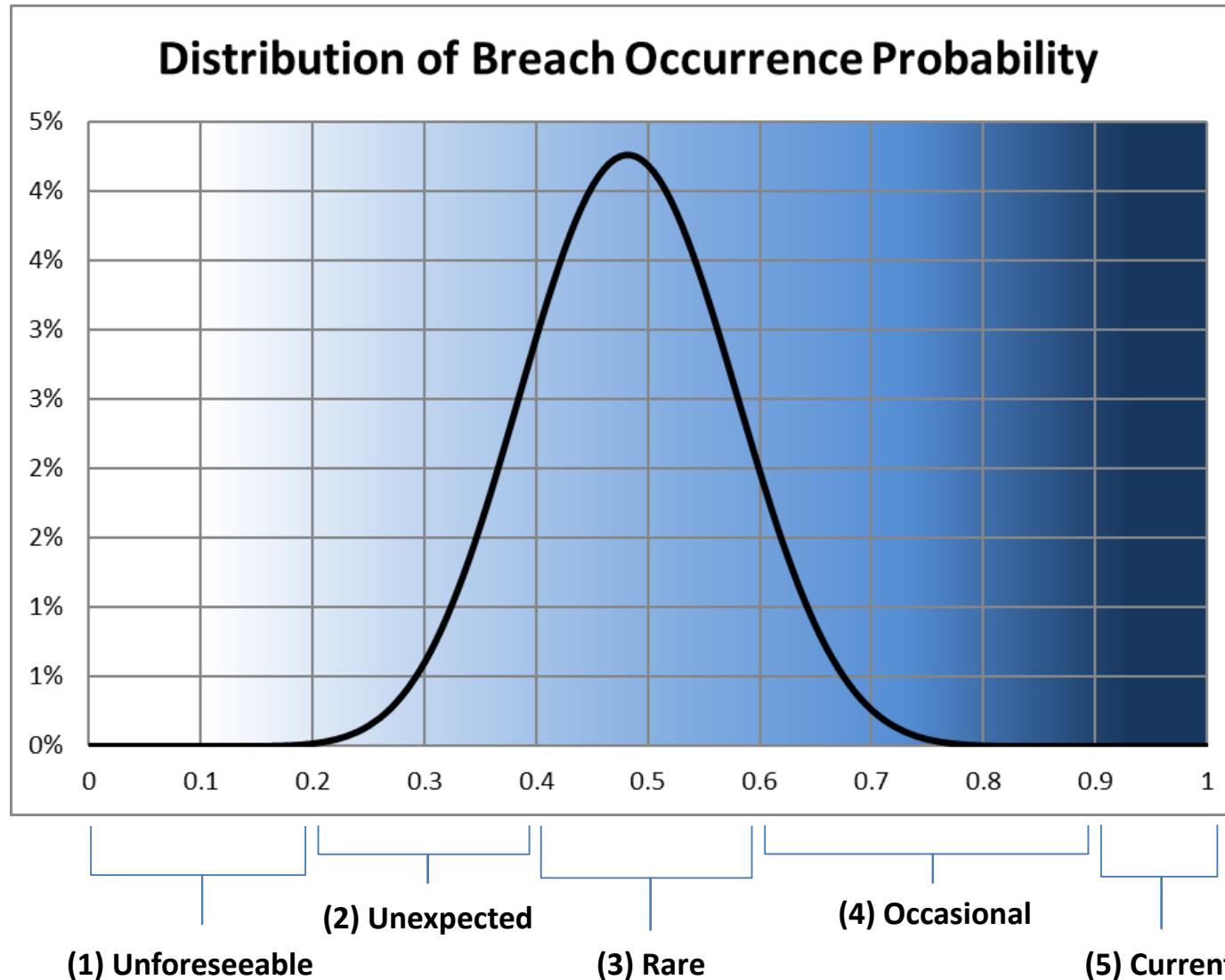
Regulator: Nice job evaluating the threat. I see the dollar value of your potential losses. But I don't think this control is appropriate for the risk.

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: ...

Quick Note: Using Quantitative Analysis with DoCRA



Download:

The Questions a Judge Will Ask You After a Data Breach

- There are fundamental questions that you will be asked after a data breach
- Be prepared to answer them using DoCRA

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?

Implementing DoCRA for Organizations

If you are an Organization looking to implement DoCRA:

- As reference, download CIS RAM from [cisecurity.org](https://www.cisecurity.org)
- Use any security controls framework that applies to you.
- Option 1: 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
- Option 2: Starting fresh with a new DoCRA-based risk assessment.

Implementing DoCRA for Law Firms

If you are a Law Firm looking to help your clients implement DoCRA:

- **Step 1:** HALOCK can conduct a complementary 1 hour introduction course with CLE credits.
- **Step 2:** HALOCK can conduct a complementary ½ day DoCRA Training for your legal team.
- **Step 3:** Law firm can conduct DoCRA Gap Assessment with your clients.

This is Not Simple The First Time – Partner with Qualified Advisors

- Work with security consultants who are experienced with DoCRA-based risk assessments.
- HALOCK provides DoCRA-based risk assessments that include real-world data about threat likelihood (no estimating needed!).
- Regulatory, best-practice, post-breach.

Resources

[CIS RAM Download](#)

[CIS RAM Executive Prospectus](#)

[CIS RAM FAQ](#)

[Duty of Care Risk Analysis Standard \(DoCRA\)](#)

[HALOCK Security Labs](#) (www.halock.com)

Feel free to reach me

Chris Cronin: ccronin@halock.com



Question & Answer Session

Speakers

- Chris Cronin - CIS RAM

Moderator

- Barbara Boehler – Compliance Week

► [Ask a Question](#)

You can submit questions using the “**Ask a Question**” button on the left side of your screen.

COMPLIANCE WEEK



Thank you for joining us

CPE Credit Information

The CPE test will appear in a separate window at the conclusion of the webcast. If you have trouble accessing the test, please email us at info@complianceweek.com. CPE certificates will be emailed to you separately following completion of the exam.

Be sure to disable your pop-up blockers to access the automatic CPE exam presented at the conclusion of the webcast. Please note that a passing score of 80% or higher is needed to receive CPE credit.

View Upcoming Compliance Week Webcasts: www.complianceweek.com/webcasts

Please send feedback to: info@complianceweek.com

Sponsored by

