The Questions A Judge Asks You After A Data Breach

Tod Ferran, CISSP, QSA, ISO 27001 Lead Auditor

Managing Consultant, HALOCK Security Labs

HALOCK Overview

- Founded in 1996
- 100% focus on information security
- Privately owned by seasoned practitioners
- Authors of CIS RAM and the DoCRA Standard
- Founding Members of the DoCRA Council
- 450_+ Active Business Clients in US and Canada

Industry Focus

Healthcare

Cloud Providers

Insurance

Banking

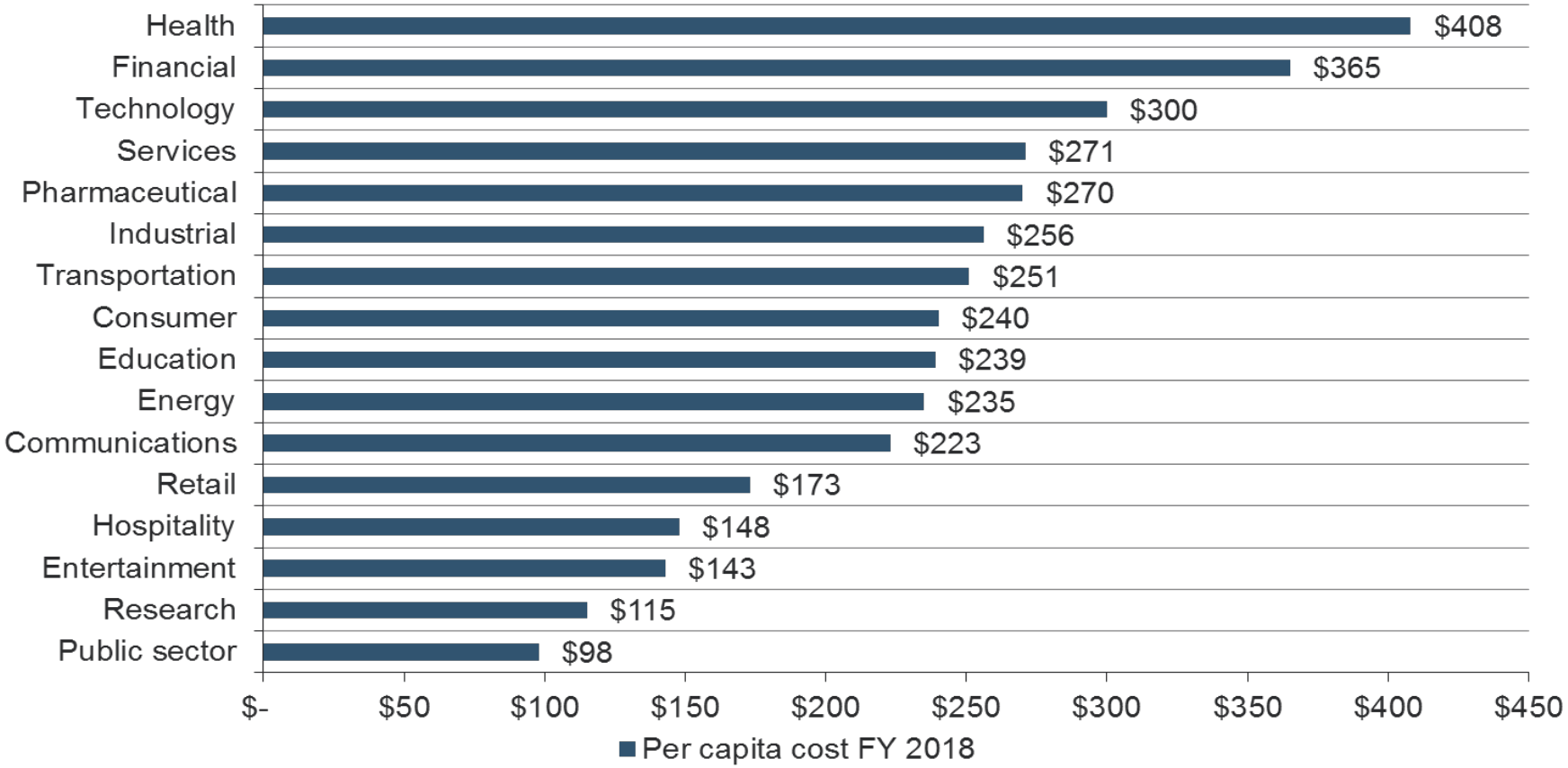
Retail

Energy

Higher Education

HALOCK®

Health Care Industry Has Highest Breach Costs



Source: Ponemon Institute© Research Report (sponsored by IBM Security), *2018 Cost of a Data Breach Study: United States* (July 2018)

Recent OCR Enforcement Action: Medical Records Service

- 3.5M records accessed by hacker
- OCR Director Roger Severino
  - "Entities entrusted with medical records must be on guard against hackers. The *failure to identify potential risks and vulnerabilities to ePHI* opens the door to breaches and violates HIPAA."
- $100,000 penalty to HHS
- Corrective Action Plan
  - (A) Conduct Risk Analysis
  - (B) Develop and Implement a Risk Management Plan

DoCRA Training for IT and Business Leaders

Foundations

Understand DoCRA

- Its history and authority
- Its current uses
- Its benefits to clients

Workshop

Learn to use DoCRA

- Regulatory compliance
- Post-breach oversight
- Litigation defense

Take Aways

- **Harm to others**
- **Define Acceptable Risk**
- **Evaluate Safeguards**

Foundations Agenda

What – Risk analysis is.

Why – We do it.

What – DoCRA is.

Why – Risk analysis is consistently required.

How – DoCRA works.

How – You can use DoCRA.

HALOCK®

* Three Key Messages

Message 1:

Infosec and business are not necessarily adversaries.

Message 2:

"**Reasonable**" safeguards should be defined by business.

Message 3:

DoCRA speaks "**reasonable**" for business, infosec, attorneys, regulators."

What is Risk Analysis

A way of expressing the likelihood of harm

Risk = Impact x Likelihood

Can be qualitative or quantitative

What is Risk Analysis

Qualitative Risk Analysis Example

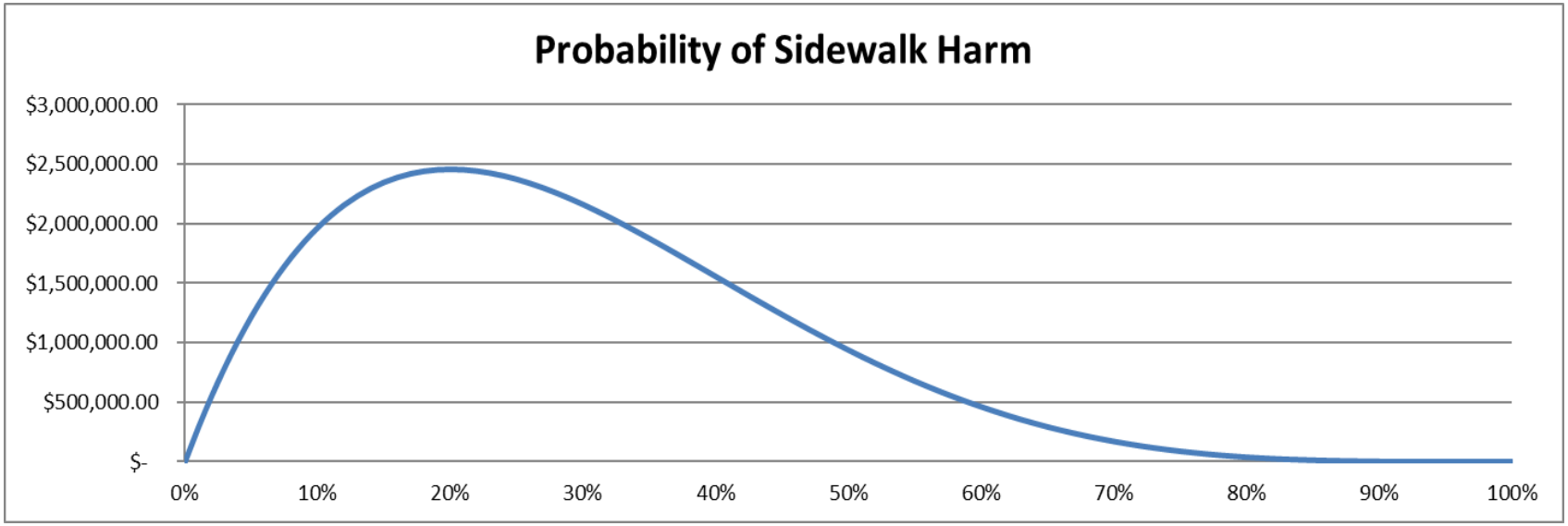
"This sidewalk could foreseeably get icy, causing a customer to slip, fall, and be hurt."

Risk = Foreseeable x Hurt Customer

What is Risk Analysis

Quantitative Risk Analysis Example

"The probability of reduction in our profits from harmed customers is expressed as …"



Why We Analyze Risk

We want to prevent or minimize harm.

That's lofty …

Harm can come from anywhere

At any time.

HALOCK®

Why We Analyze Risk

We want to prevent or minimize foreseeable harm.

That's important,

but you have many important

things to do.

Why We Analyze Risk

We want to evaluate and prioritize reduction of foreseeable harm.

That's better.

But who's harm?

Why We Analyze Risk

- We want to evaluate and prioritize reduction of foreseeable harm to ourselves and to **ANYONE** ...

Very good.

But at what cost?

HALOCK®

Why We Analyze Risk

- We want to evaluate and prioritize reduction of foreseeable harm to ourselves and others, but not with a burden that's greater than the risk.

Ahh.

That makes sense.

Another Reason Why We Analyze Risk

Security standards are nearly ***impossible*** to perfectly achieve and maintain. So they ***require risk analysis***.

- NIST 800-53
- CIS Controls
- NIST Cybersecurity Framework
- PCI DSS (one of the prescriptive controls)

Compliance != Duty of Care

Yet **Another Reason** We Analyze Risk

Regulators *will not and should not* specify the controls we use in our organizations. So they *require risk analysis*.

- HIPAA Security Rule
- 201 CMR 17.00
- 23 NYCRR Part 500
- GLBA Safeguards Rule
- FISMA
- CCPA
- Federal Trade Act

Risk Management is Universally Required

We cannot demand one, a universal cybersecurity framework.

So we demand risk management to reduce risk to others and ourselves.

If you could design the universal rules for managing cybersecurity risk … ***What would balance look like?***

DoCRA Principles
(Duty of Risk Analysis)

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.

HALOCK®

What **DoCRA** Is …

- Duty of Care Risk Analysis (DoCRA) Standard.
  - Harm to others,
  - Define Acceptable Risk,
  - Evaluate Safeguards
- CIS RAM - Method for analyzing risks.
- Defines “**reasonable**” and “**appropriate**” using plain language.
- Brings together the interests of business, technologists, regulators, and litigators.

What **DoCRA** Is …

- Freely available to the public.
  - (Creative Commons license)
- Three principles and ten practices for assessing risk to demonstrate **due care**.
- Currently used by CIS® (Center for Internet Security) as the basis for CIS RAM.
- Can use any standard of care (not just CIS Controls) to evaluate cybersecurity or information risk.

Where **DoCRA** is Used

- Regulatory compliance.
- Post-breach regulatory oversight.
  - Designing corrective action plans for “reasonable” security.
  - Offering terms for injunctive relief.
- Litigation.
  - State Attorneys General
  - Complex breach cases
- Vendor and BAA risk assessments
  - Apply our criteria when assessing and treating risk to the data/systems shared

HALOCK®

Message 1:
InfoSec and Business are Not Adversaries

- Regulations and controls are often seen as adversarial to business … legal or workflow matters that interfere with commerce and enterprise.
- We don’t live in a ‘zero’ risk world
  - Not expected
  - Not reasonable
- Since 1993 federal regulations require cost-benefit analysis to justify their enforcement.
- Judges and regulators allow businesses to show whether safeguards balanced the potential of harm against the burden they posed.

HALOCK®

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.

Balance in Courts

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

Burden <= Probability x Liability

But Balance is Not Often Used in Security Assessments

How Current Security Assessments Are Failing Us

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	●	○	○	○	○	○	○	○	○

HALOCK®

Being Judged

How Judges 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 Regulators are Interpreting 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 customers/patients agree with this acceptance criteria?

You: … No.

How Regulators Interpret FAIR and Quantitative 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 curve over here, our probable loss is low.

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

You: …

Strategically Helping Our Business

- Upper management need to know how these tough conversations will go without the right preparation.
- Show management that due care works in their favor.
  - Sets limits on cybersecurity investments.
  - Integrates business purpose in security decisions.
  - Communicates a consistent message of mutual respect for self and others.

Message 2:
Business Defines "Reasonable"

Because laws and regulations recognize that all organizations are different,

then each organization must define "**reasonable**" for themselves.

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

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 3 = 9
Accept Risk	< 9

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) Patients feel inconvenienced	(3) Budget variance would be recoverable within a year.	(3) Few patients would suffer reputational or financial harm

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) Health outcomes would not be effected.	(2) Budget performance within planned variance.	(1) Patients' privacy would not be 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 PHI in plain text	Threat	Sniffers can capture PHI
Risk Scenario	Hackers place packet sniffers within DMZ, capture plain-text PHI, and exfiltrate data.		

Mission Impact	Objectives Impact	Obligations Impact
(3) Some patient's health outcomes would suffer.	(3) Budget variance would be recoverable within a year	(4) Many patients would suffer reputational or financial harm.

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) Some patient's health outcomes would suffer.	(3) Budget variance would be recoverable within a year	(4) Many patients would suffer reputational or financial harm.

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) Some patient's health outcomes would suffer.	(3) Budget variance would be recoverable within a year	(4) Many patients would suffer reputational or financial harm.

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

Message 3:
DoCRA Speaks "Reasonable" to Business, InfoSec, Attorneys, Regulators

DoCRA makes sense to law, business, and InfoSec because:

- It follows the rules of these three disciplines, and
- It addresses what matters to each discipline.

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.
- This is encoded as the "Hand Rule" or "Calculus of Negligence."
  - "**Burden < Probability x Likelihood**"
- Multi-factor balancing tests are how duty of care and due care are determined.

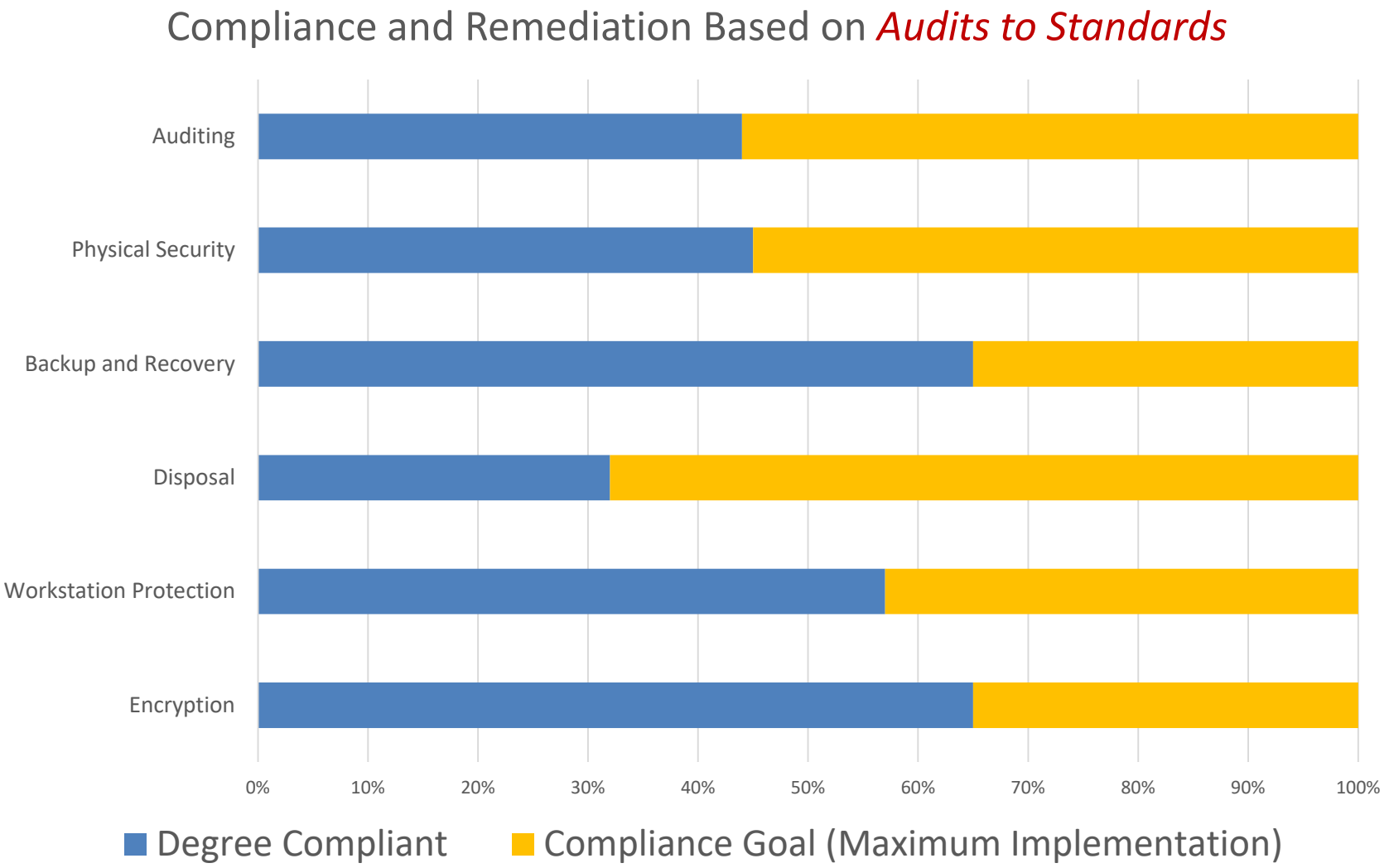
The Questions A Judge Asks You After A Data Breach

- 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?

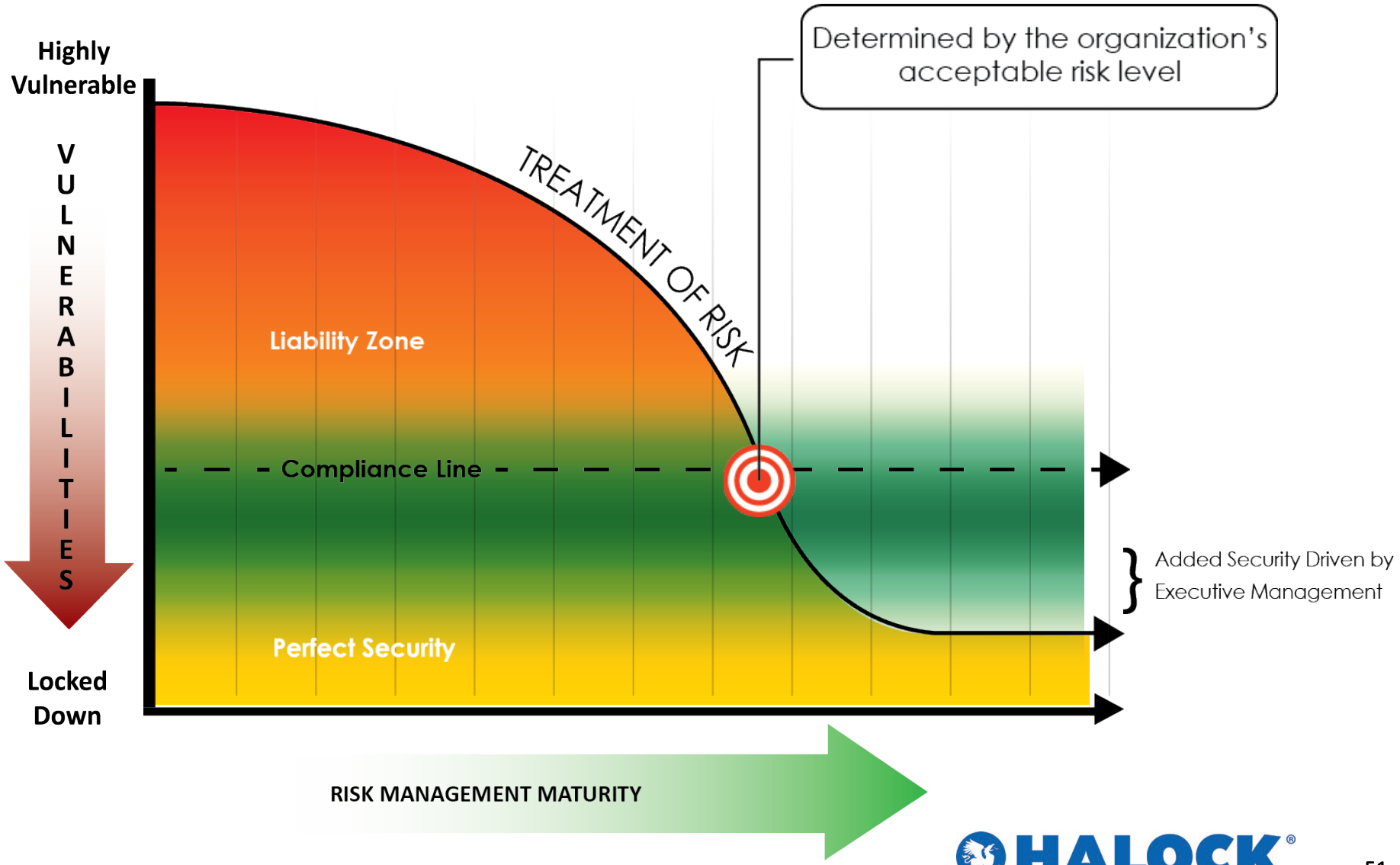
Why do **Regulators** Like Duty of Care Risk Analysis?

- 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.

Efficiency of Risk-Based Compliance: The **Expected** Response to Audit Findings

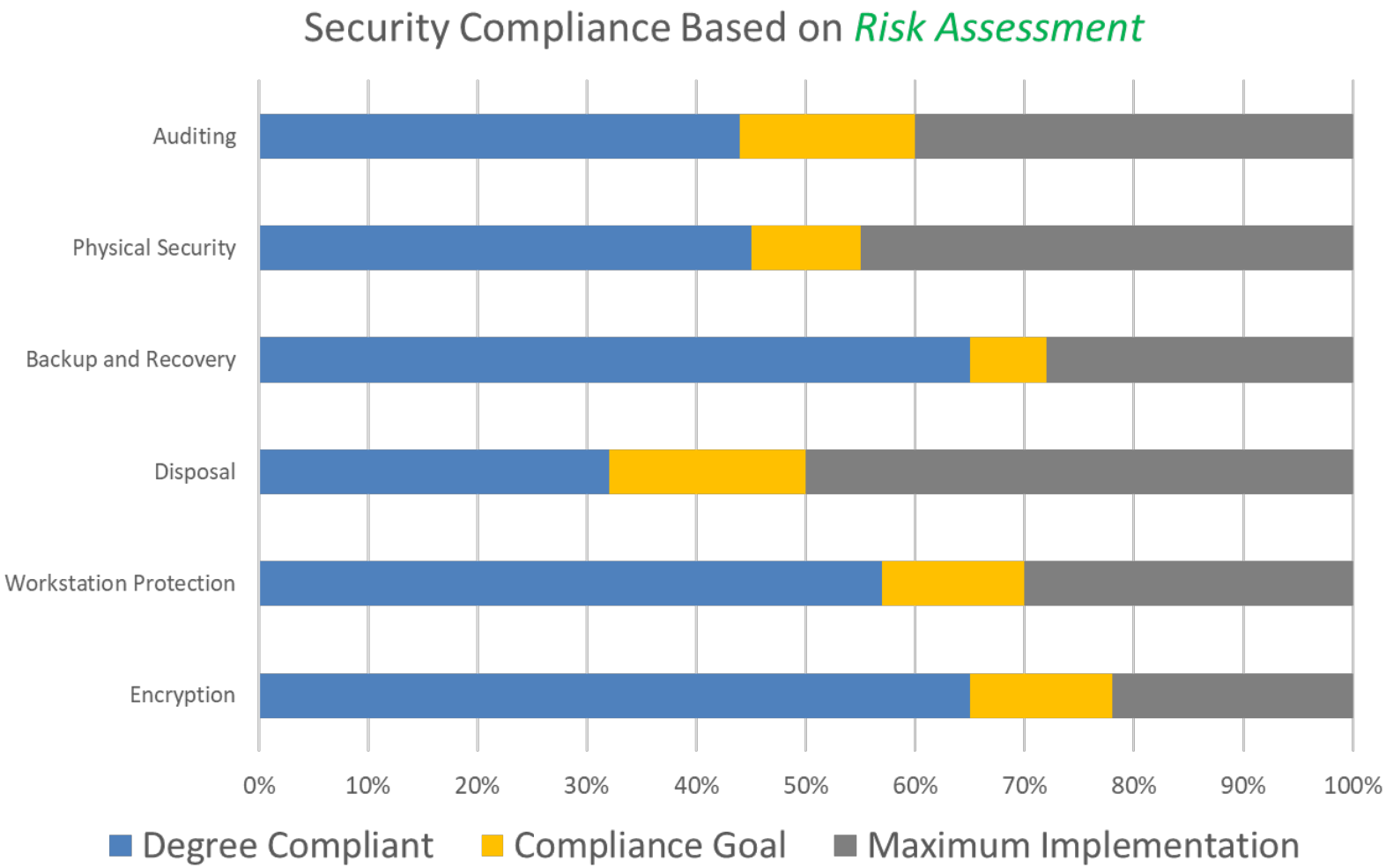


Reducing Liability Over Time



HALOCK®

Efficiency of Risk-Based Compliance: The **Reasonable** Response to Risk Findings



Are You Sure? Regulators Tell Me What To Do.

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

Take Aways

- **Harm to others**
- **Define Acceptable Risk**
- **Evaluate Safeguards**

Questions

Tod Ferran, CISSP, QSA, ISO 27001 Lead Auditor

Managing Consultant, HALOCK Security Labs

tferran@halock.com

HALOCK®

Resources

CIS RAM Download

CIS RAM Executive Prospectus

CIS RAM FAQ

Duty of Care Risk Analysis Standard (DoCRA)