RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

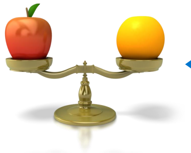
SESSION ID: **RMG-F01**

# Securing the Budget You Need! Translating Security Risks to Business Impacts

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

CEO, Senior Partner
HALOCK Security Labs
@halock

# What we are going to cover today



1. The Problem – Securing Budget

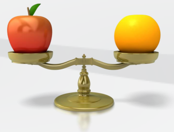
2. The Solution – A Common Language

3. Implementing – A Common Language

4. Real Life Examples – How it Works

5. Applying It – Now, 3 months, 6 months

- **Raise your hand if you have 100% of the budget you truly need to get your job done right?**
- **Raise your hand if you have 100% of the staff you truly need to get your job done right?**
- Today we will talk about:
  - Why does this problem occur?
  - How does this problem manifest itself?
  - How you can all raise your hand the next time you are asked if you have 100% of the budget or staff you need.



# Why does this problem occur?

- Laws, Regulations and Standards all ask that we design our controls **based on Risk**
  - HIPPA, GDPR, CCPA, 23 NYCRR 500, GLBA
  - PCI, ISO 27001, NIST SP 800-53, CIS Controls

- **Traditional Risk Assessments** prioritize Risk based on Impact on Assets:
  - **Risk = Likelihood x Impact**

- **Traditional Risk Assessments** calculate **Impacts** using the categories of:
  - **Confidentiality, Integrity, Availability (CIA)**

## Why does this problem occur? (Continued)

- Traditional Risk Assessments focus on:

**(A) Your Organization** → **Narrow Scope**

**(B) Technical Impacts** (CIA) → **Technical Focus**

## Why is this an Issue?

- Those who control the budget focus on:

**(A) Beyond Your Organization** → **Broad Scope**

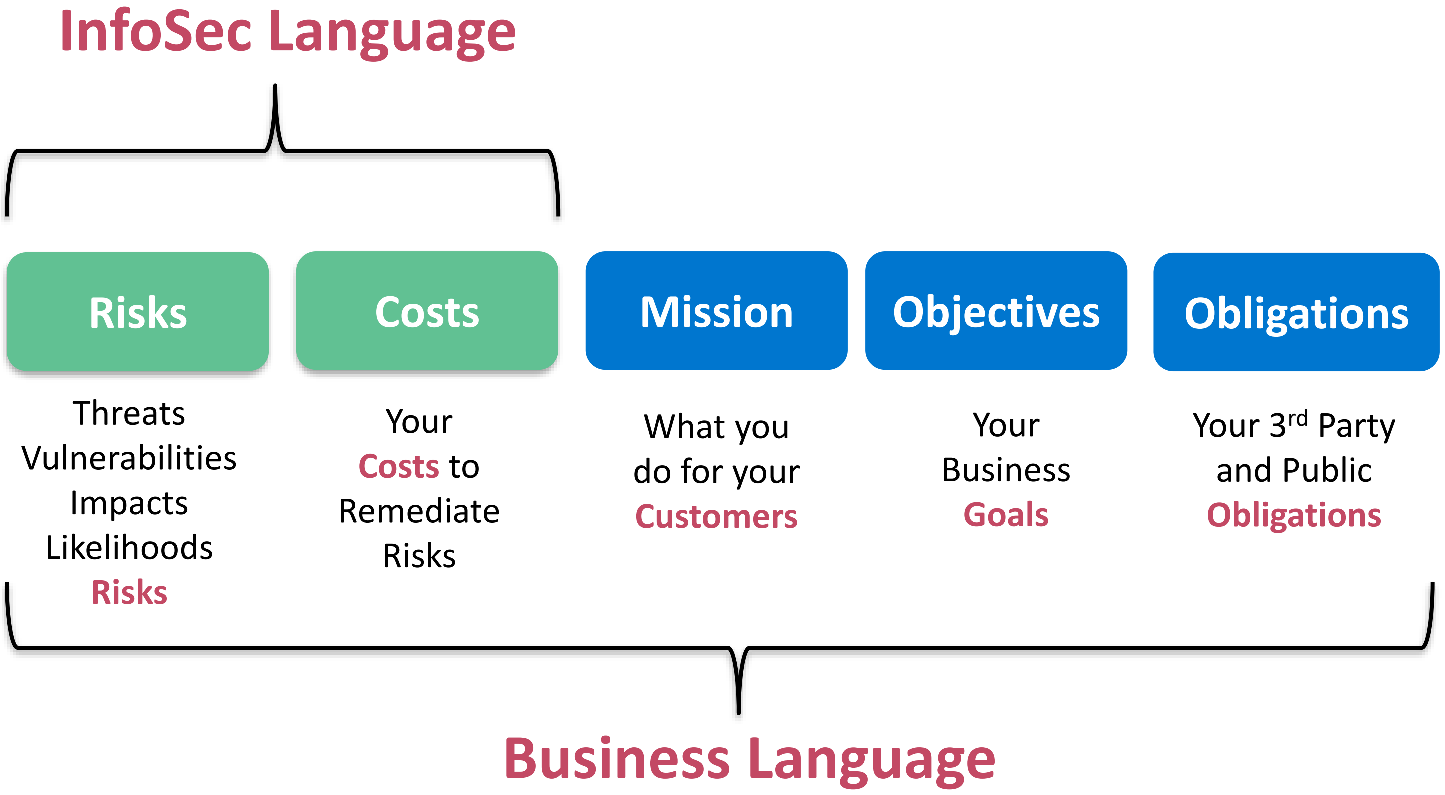
**(B) Business Impacts** → **Business Focus**

# How does this problem manifest itself?

**We have been speaking different languages.**

**Information Security** speaks in *risks and costs*.

**Business** speaks in terms beyond *risks and costs*.



InfoSec Language

**Risks**

Threats
Vulnerabilities
Impacts
Likelihoods
**Risks**

**Costs**

Your
**Costs** to
Remediate
Risks

**Mission**

What you
do for your
**Customers**

**Objectives**

Your
Business
**Goals**

**Obligations**

Your 3rd Party
and Public
**Obligations**

Business Language

# Who wins the budget debate most of the time?

Risks & Costs
Risks, Costs, Customers, Business Goals, Obligations
InfoSec
Business

Unless you recently experienced a breach or the project has political clout, the **Business / Revenue Generators win that debate most of the time!**

**Duty of Care Risk Analysis (DoCRA)** is the prescription for creating a common language between InfoSec and Business!

**DoCRA** is based on the legal concept of "**Due Care**." This means, we must protect others from the harm we may cause them, by implementing controls that are not more burdensome to us than the risk of the harm to others.

**Due Care** is level of care that the <u>legal system expects an organization to perform</u>.

# DoCRA: Invented for the courtroom - Effective in the boardroom

- The two places where things definitively get resolved are the **courtroom and the boardroom.**
- DoCRA was **invented to communicate in business terms** to Judges in the courtroom.
- DoCRA is equally effective in the boardroom.

The **DoCRA** Risk Assessment method delivers three powerful capabilities:

1. **Legally defensible** position by defining what is **legally “reasonable”**
2. **Process to evaluate whether to “invest” or “accept” the risk** for risk mitigation
3. ***Common language*** between InfoSec and business / regulators / legal system

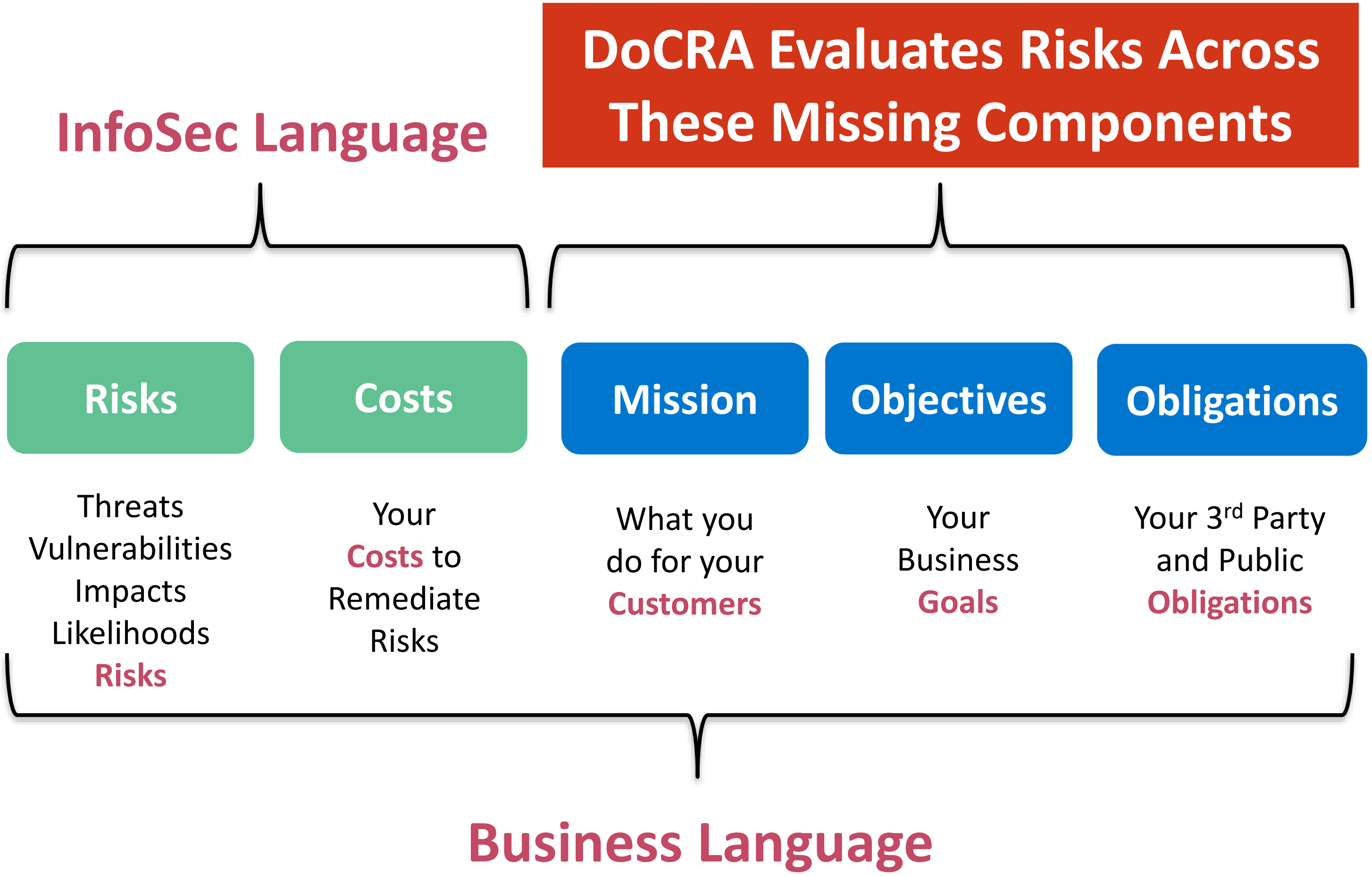
Each of these three capabilities are extremely powerful and useful. The focus of this presentation is on building a **Common Language** to secure Budget.

# How does DoCRA create a Common Language?

**Information Security** speaks in *risks and costs*.

**Business** speaks in terms beyond *risks and costs*.

**DoCRA fills in the missing components** to create a common language as a universal translator.



InfoSec Language

DoCRA Evaluates Risks Across These Missing Components

**Risks**

Threats
Vulnerabilities
Impacts
Likelihoods
**Risks**

**Costs**

Your
**Costs** to
Remediate
Risks

**Mission**

What you
do for your
**Customers**

**Objectives**

Your
Business
**Goals**

**Obligations**

Your 3rd Party
and Public
**Obligations**

Business Language

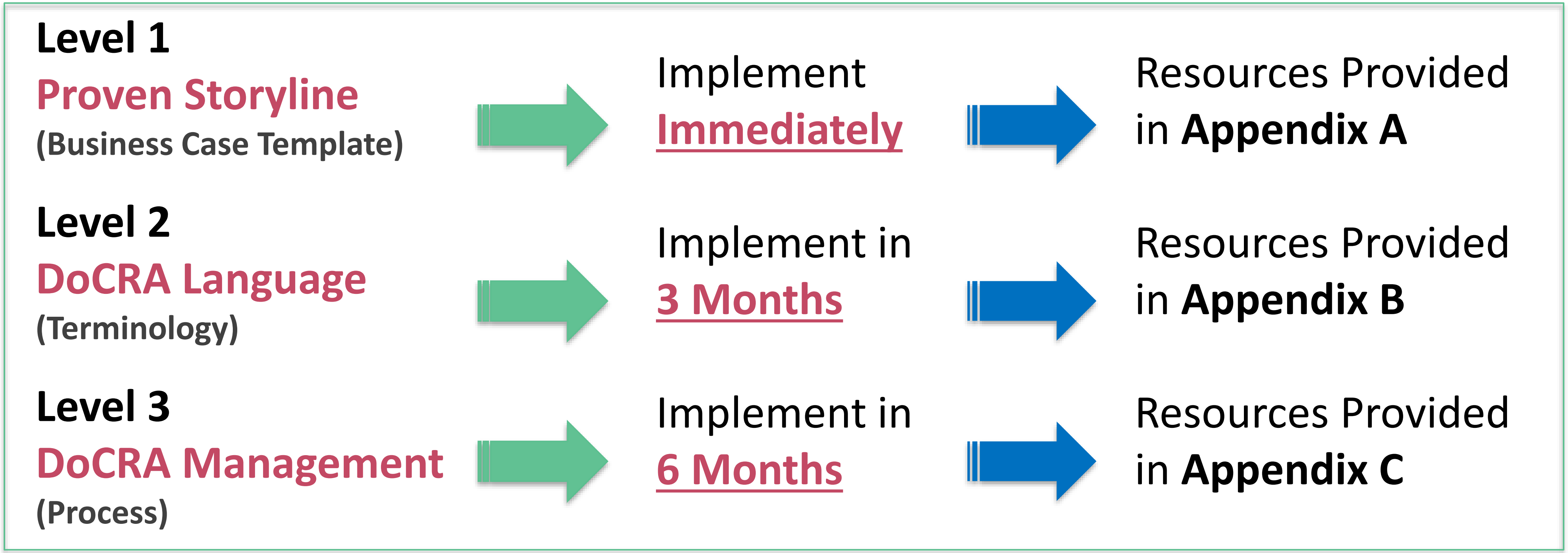
# About DoCRA…

- The **Duty of Care Risk Analysis** (DoCRA) methodology was launched as a standard in early 2018
- DoCRA is a non-profit organization
- DoCRA donated a version of its Risk Assessment Methodology to CIS® (Center for Internet Security)
- CIS published this Risk Assessment Method (CIS RAM), containing DoCRA, with the CIS Controls Version 7 in April, 2018
- DoCRA can be utilized with CIS, NIST, ISO or any control set

# About DoCRA… (Continued)

- DoCRA has experienced **significant adoption**
- Over 26,000 downloads of the CIS RAM Methodology
- Used by state Attorneys General to determine whether controls were legally "reasonable" during a breach
- Utilized by federal regulators to develop post-breach corrective action plans (injunctive relief)

# Here is what you will receive today:



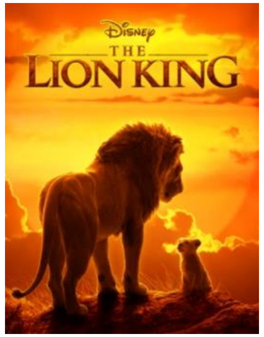
**Level 1**
**Proven Storyline**
**(Business Case Template)**
→ Implement **Immediately** → Resources Provided in **Appendix A**

**Level 2**
**DoCRA Language**
**(Terminology)**
→ Implement in **3 Months** → Resources Provided in **Appendix B**

**Level 3**
**DoCRA Management**
**(Process)**
→ Implement in **6 Months** → Resources Provided in **Appendix C**

# Level 1 – Proven Storyline

- Do you know what the movies Rocky, Star Wars, The Matrix, Spider Man, The Lion King, Lord of the Rings, Harry Potter, and countless other hits have in common?



- **These Blockbuster Movies** follow a **proven storyline** called “**The Hero’s Journey**”
- **Your Budget Requests** should also follow a **proven storyline…** **“The Budget Journey”**

# Level 1 – Proven Storyline

- A financial template is rarely sufficient!
- Utilize a **Proven Financial** Template with a **Proven Storyline** for requesting budget
- **“The Budget Journey”**

**Step 1: Establish where you are** – The current state

**Step 2: Highlight the discontinuity** – How the current state does not meet the needs of the business

**Step 3: Quantify the discontinuity** – The size of the gap between current state and what is needed

**Step 4: Identify the solution** – The solution and how it solves the problem

**Step 5: Evaluate not having the solution** – The potential impacts of not having the solution

**Step 6: Describe implementing the solution** – The cost and approach for implementing the solution

**Step 7: Executive Summary** – One page to summarize the Budget Request

# Level 2 – Implementing DoCRA Language Involves:

- Defining a line in the sand – below which you accept the risk and above which you need to do something to mitigate the risk

# Level 2 – Implementing DoCRA Language

## Define a clear line at which you will start to mitigate risk

- If we have an "*unacceptable*" impact that is "*expected to occur within 3 years*" to our Mission, Objectives or Obligations then we agree we must take action to reduce risk.
- Based on the below Acceptable Risk Definition we will do the following:
  - Risks scoring less than "9" are acceptable to the business and we are not required to invest further
  - Risks scoring "9" or greater require us to do something and invest further to mitigate

| Likelihood Score | Likelihood Definition |
|---|---|
| 1 | Not foreseeable - Within 3 Years |
| 2 | Foreseeable, not expected – Within 3 Years |
| 3 | Expected to occur- Within 3 Years |
| 4 | Common – Within 1 Year |
| 5 | Continuous – Multiple Times a Year |

| Risk Acceptance | Score |
|---|---|
| Invest against risk | 3 x 3 = > 9 |
| Accept Risk | < 9 |

**Risk = Likelihood x Impact**

| Impact Score | MISSION (For Our Customers) | OBJECTIVES (Business Goals) | OBLIGATIONS ($3^{RD}$ Party & Public) |
|---|---|---|---|
| 1. Negligible | | | |
| 2. Acceptable | | | |
| 3. Unacceptable | | | |
| 4. High | | | |
| 5. Catastrophic | | | |

# Level 2 – Implementing DoCRA Language

- Populate Impact Definitions for to Mission, Objectives and Obligations with business impacts that relate to your business

| Likelihood Score | Likelihood Definition |
|---|---|
| 1 | Not foreseeable - Within 3 Years |
| 2 | Foreseeable, not expected – Within 3 Years |
| 3 | Expected to occur- Within 3 Years |
| 4 | Common – Within 1 Year |
| 5 | Continuous – Multiple Times a Year |

| Risk Acceptance | Score |
|---|---|
| Invest against risk | 3 x 3 = > 9 |
| Accept Risk | < 9 |

Risk =
Likelihood x Impact

| Impact Score | MISSION (For Our Customers)<br>• Customer Financial Performance | OBJECTIVES (Business Goals)<br>• Profitability | OBLIGATIONS ($3^{RD}$ Party & Public)<br>• Customer Privacy |
|---|---|---|---|
| 1. Negligible | Customer returns at or above market. | Achieve Profitability Goals | 0 to 49 records exposed |
| 2. Acceptable | Customer returns at market by end of fiscal year. | Profitability shortfall but within planned variance | 50 to 99 records exposed |
| 3. Unacceptable | One product underperforms against market for a year. | Missed Profitability Goal by up to 2% for any year | 100 to 999 records exposed |
| 4. High | Multiple products under perform for multiple years. | Missed Profitability Goals by 2-5% for any year. | 1,000 to 9,999 records exposed |
| 5. Catastrophic | Cannot meet market returns. | Missed Profitability Goals by over 5% for any year. | 10,000+ records exposed |

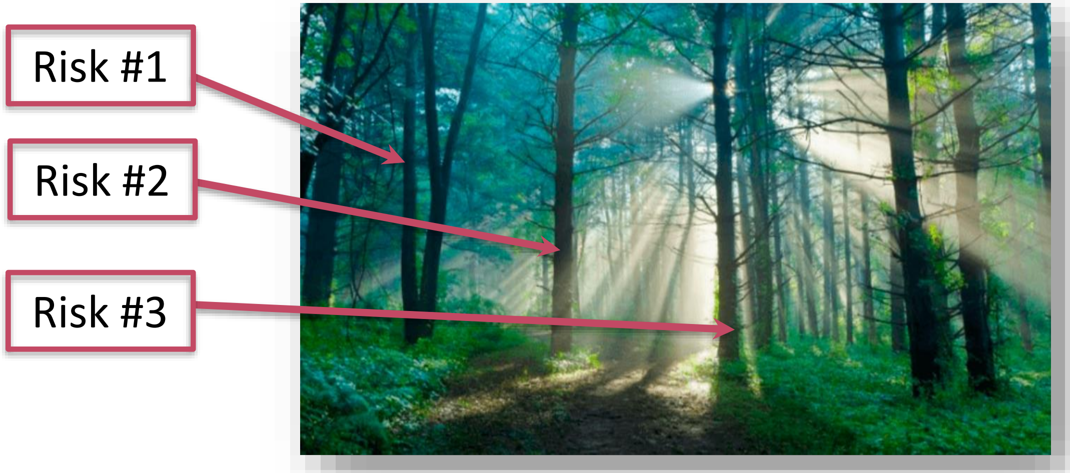
# Level 2 – Implementing DoCRA Language

- Some common concerns at this point…..
  - How do we fill out the business impact scores?
  - Are there templates we can use?
  - How do we get the business to buy-in?
  - It seems daunting and difficult.
- We will discuss how to approach this and there are available downloads / resources in **Section 5: Applying It**

# Level 3 – Management: Implementing DoCRA Process / Analytics

- We often address each risk independently. We have a tendency to talk about one tree, and then another tree and then another tree…

- Executives want to see the forest as well as the trees and DoCRA Analytics allow us to holistically view the forest as well as the trees.



# Level 3 – Management: Implementing DoCRA Process / Analytics

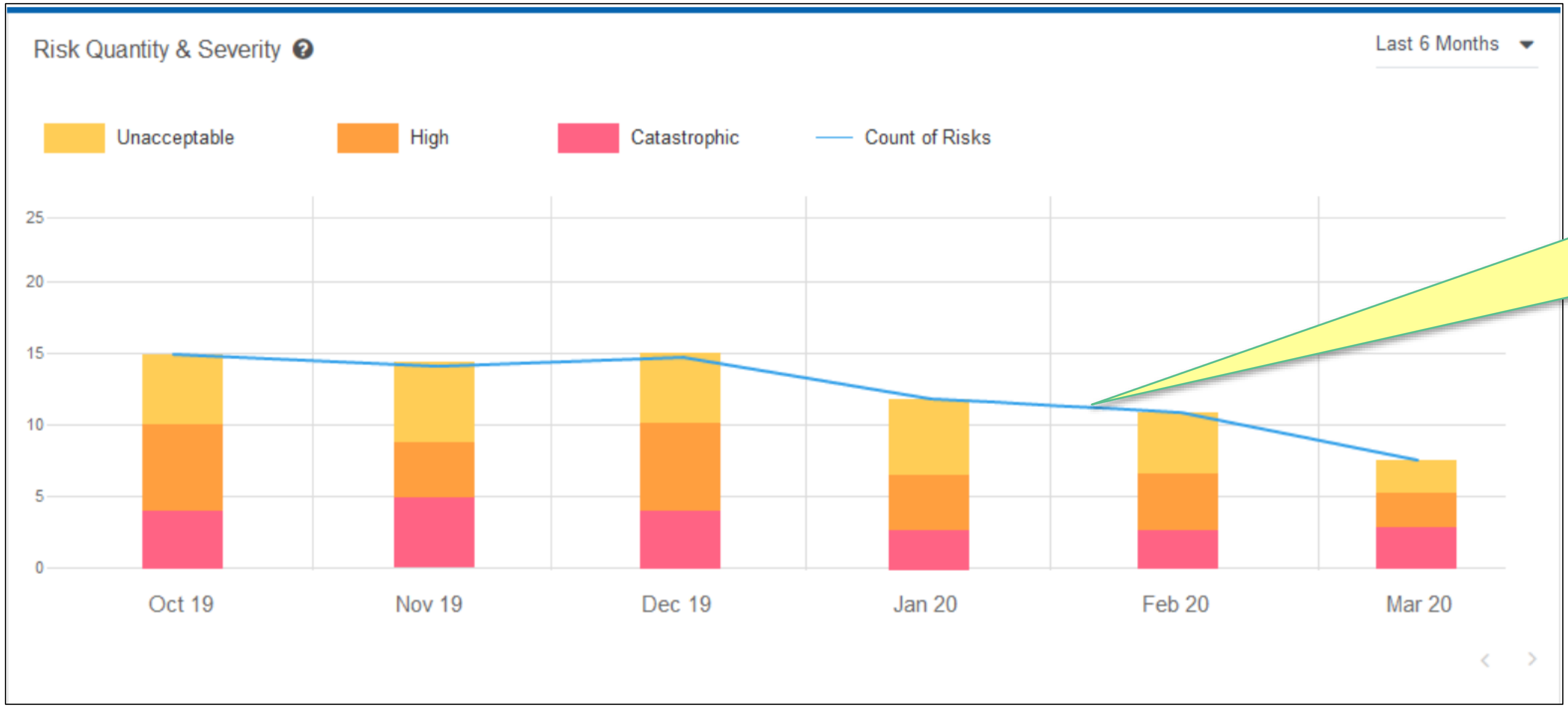
- Perform a Comprehensive DoCRA Risk Assessment (see Appendix D)
- Score all the risks and sort by Highest to Lowest Risk Score
  - This provides insight into risks relative to one another and a view of your highest risks

| ID | Score | Description | Likelihood | MISSION<br>(For Our Customers) | OBJECTIVES<br>(Business Goals) | OBLIGATIONS<br>(3$^{RD}$ Party & Public) |
|---|---|---|---|---|---|---|
| 12 | 20 | PII leaving the perimeter unintentionally | 5 | 3 | 1 | 4 |
| 2 | 15 | Network architecture does not support business continuity requirements | 3 | 3 | 1 | 5 |
| 24 | 8 | Lack of MFA on Web application | 2 | 3 | 4 | 3 |
| 5 | 6 | Passwords for privileged accounts not adequately managed | 2 | 2 | 3 | 2 |
| 9 | 6 | Employee onboarding lacks access roles | 3 | 2 | 1 | 2 |

3 Implementing

# Level 3 – Management: Implementing DoCRA Process / Analytics

- Provide Decision Makers Meaningful **Risk Quantity Trending**



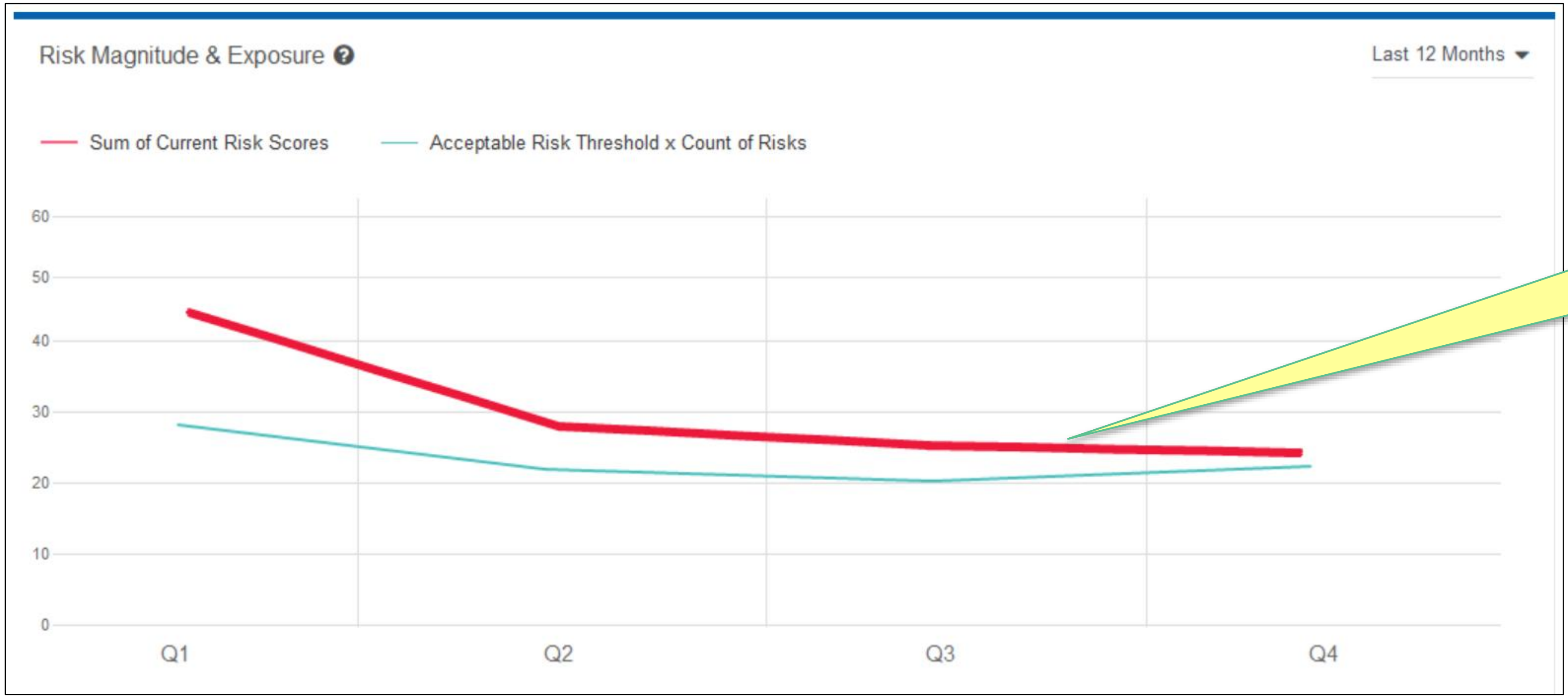
Risk Quantity & Severity

Last 6 Months

This is your
**“Risk Quantity”** and
represents the Total
Number of Risks
above the Acceptable
Risk Level

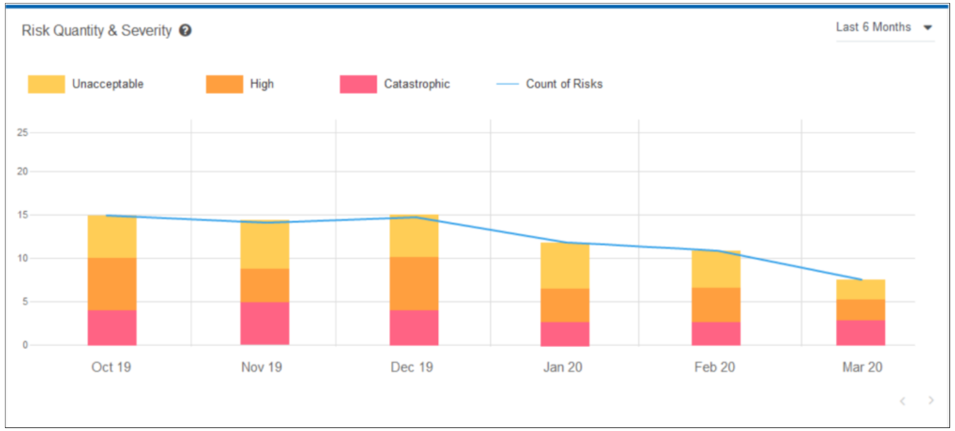
# Level 3 – Management: Implementing DoCRA Process / Analytics

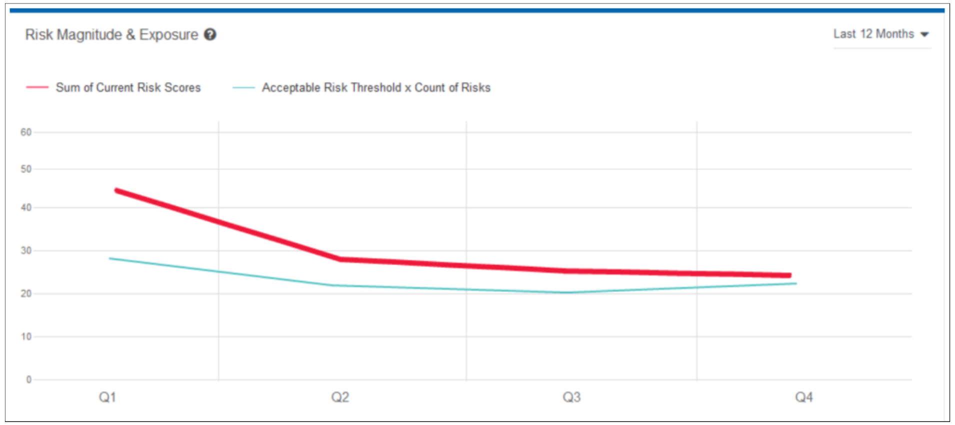
- Provide Decision Makers Meaningful **Risk Severity Trending**



This is your "**Risk Magnitude**" and represents the Sum of all Risk Scores

# Level 3 – Management: Implementing DoCRA Process / Analytics





Combine the two views together (Risk Quantity & Risk Magnitude) to provide decision makers insights about the security program

## Program Health – Trending Translator

| | | | |
|---|---|---|---|
| Quantity ↓<br>Magnitude ↓ | On Target Effective Program | Quantity ↑<br>Magnitude ↑ | More Resources are Needed |
| Quantity ↑<br>Magnitude ↓ | Effective Program More Resources are Needed | Quantity ↓<br>Magnitude ↑ | A Different Focus Is Needed |

# Real-Life Budget Requests with Different Outcomes

- **Example: Data Loss Prevention (DLP) Budget Approval Request**
  - Traditional Approach →

  - DoCRA Approach →

Budget
Approved

# Traditional Approach – DLP Budget Request

**CISO:** “We need a DLP product to catch personal information for claims data that might be leaving the company through email, FTP, web app file shares, or other means.”

**CISO:** “I recommend this $225,000 solution that solves this burning issue and gets us everything we need.”

CFO: “That’s a quarter of your budget.  Is there a more affordable option or could we implement just a portion of it?”

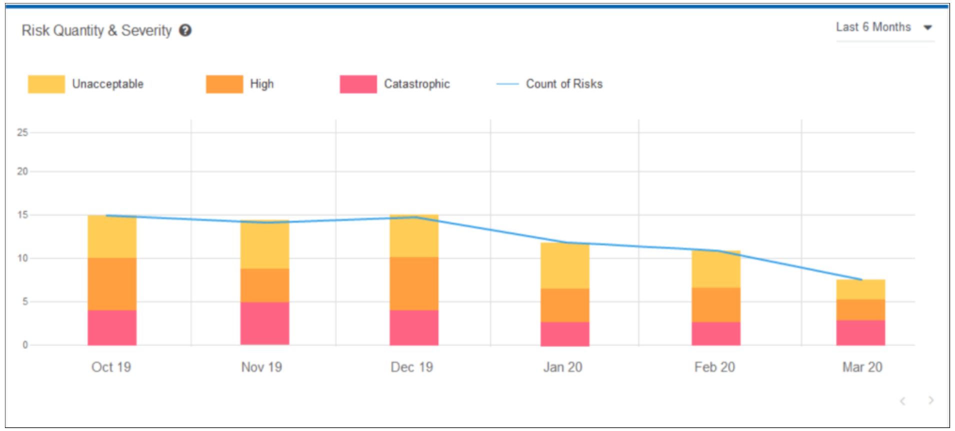
**CISO:** “The entry level, bare-bones solution from this vendor is $50,000, but it will not eliminate all of our risk.”

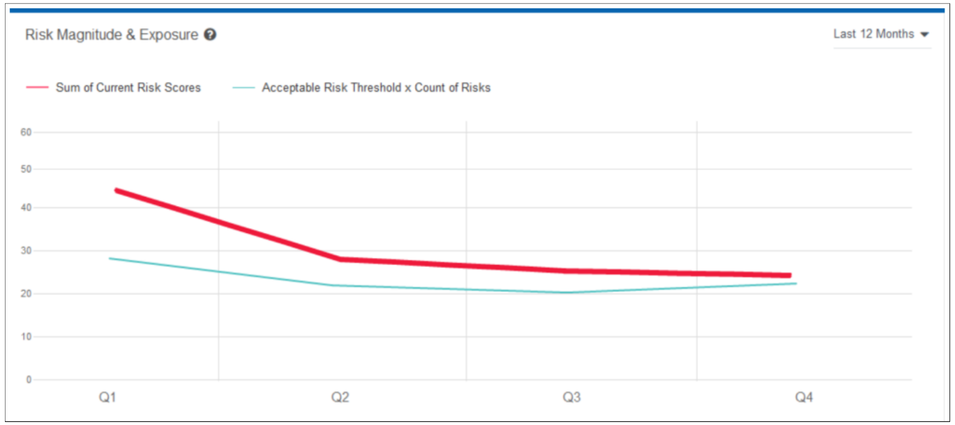
CFO:  **“**Let’s start with approving $50,000 this year, and re-evaluate next year.”

- **What happened?**
  - The CISO expressed what “bad thing” the investment would address.
  - The CFO had no way to know the potential business impact of NOT making the DLP investment.
  - The CFO decided to provide a “fraction” of the budget requested and re-evaluate later.
  - **The CISO received less than 25% of the budget they requested.**
  - **The company is exposed and the CISO is exposed.**

FAIL

# DoCRA Approach – Step 1: Current State





## First, as an Overall Program Update

- The Number of Unacceptable Risks is <u>trending down</u> (Risk Quantity)
- The Sum Current Risk Scores is <u>trending down</u> (Risk Magnitude)
- We are On Track with an <u>Effective Security Program</u>

## Program Health – Trending Translator

| | |
|---|---|
| Quantity ↓<br>Magnitude ↓ | On Target Effective Program |
| Quantity ↑<br>Magnitude ↑ | More Resources are Needed |
| Quantity ↑<br>Magnitude ↓ | Effective Program More Resources are Needed |
| Quantity ↓<br>Magnitude ↑ | A Different Focus Is Needed |

# DoCRA Approach – Step 2 and 3: Level of Discontinuity

## Second, a list of our Highest Risks is provided below:

- The red line represents our Acceptable Risk Level (a “9”), below which we “accept” the risk and at or above which we must do something to “mitigate” the risk.
- Personally Identifiable Information (PII) leaving the perimeter is the Highest Risk in our Risk Register

| ID | Score | Description | Likelihood | MISSION (For Our Customers) | OBJECTIVES (Business Goals) | OBLIGATIONS ($3^{RD}$ Party & Public) |
|---|---|---|---|---|---|---|
| 12 | 20 | PII leaving the perimeter unintentionally | 5 | 3 | 1 | 4 |
| 2 | 15 | Network architecture does not support business continuity requirements | 3 | 3 | 1 | 5 |
| 24 | 8 | Lack of MFA on Web application | 2 | 3 | 4 | 3 |
| 5 | 6 | Passwords for privileged accounts not adequately managed | 2 | 2 | 3 | 2 |
| 9 | 6 | Employee onboarding lacks access roles | 3 | 2 | 1 | 2 |

# DoCRA Approach – Step 4: Implementing the Solution

## The Risk of implementing the Proposed Safeguard (DLP)

– Including the Financial Burden of the Proposed Safeguard results in a Risk of **“6”**

| Likelihood Score | Likelihood Definition |
|---|---|
| 1 | Not foreseeable - Within 3 Years |
| 2 | Foreseeable, not expected – Within 3 Years |
| 3 | Expected to occur- Within 3 Years |
| 4 | Common – Within 1 Year |
| 5 | Continuous – Multiple Times a Year |

| Risk Acceptance | Score |
|---|---|
| Invest against risk | 3 x 3 = > 9 |
| Accept Risk | < 9 |

| Risk Score | 6 |
|---|---|

| Impact Score | MISSION (For Our Customers)<br>• Customer Financial Performance | OBJECTIVES (Business Goals)<br>• Profitability | OBLIGATIONS (3$^{RD}$ Party & Public)<br>• Customer Privacy |
|---|---|---|---|
| 1. Negligible | Customer returns at or above market. | Achieve Profitability Goals | 0 to 49 records exposed |
| 2. Acceptable | Customer returns at market by end of fiscal year. | Profitability shortfall but within planned variance | 50 to 99 records exposed |
| 3. Unacceptable | One product underperforms against market for a year. | Missed Profitability Goal by up to 2% for any year | 100 to 999 records exposed |
| 4. High | Multiple products under perform for multiple years. | Missed Profitability Goals by 2-5% for any year. | 1,000 to 9,999 records exposed |
| 5. Catastrophic | Cannot meet market returns. | Missed Profitability Goals by over 5% for any year. | 10,000+ records exposed |

# DoCRA Approach – Step 5: Not Implementing the Solution

## The Risk of NOT Remediating, "PII leaving the Perimeter"

- A business impact of 1,000 to 9,999 PII records being exposed multiple times a year and a Risk of **"20"**
- Utilizing a $150 cost per lost record (2019 Ponemon Report), we calculate a breach cost of $1,500,000 ($150 x 10,000 records), resulting a missed profitability goal by 2% (which we identified as Unacceptable)

| Likelihood Score | Likelihood Definition |
|---|---|
| 1 | Not foreseeable - Within 3 Years |
| 2 | Foreseeable, not expected – Within 3 Years |
| 3 | Expected to occur- Within 3 Years |
| 4 | Common – Within 1 Year |
| 5 | Continuous – Multiple Times a Year |

| Risk Acceptance | Score |
|---|---|
| Invest against risk | 3 x 3 = > 9 |
| Accept Risk | < 9 |

| Risk Score | 20 |
|---|---|

| Impact Score | MISSION (For Our Customers)<br>• Customer Financial Performance | OBJECTIVES (Business Goals)<br>• Profitability | OBLIGATIONS ($3^{RD}$ Party & Public)<br>• Customer Privacy |
|---|---|---|---|
| 1. Negligible | Customer returns at or above market. | Achieve Profitability Goals | 0 to 49 records exposed |
| 2. Acceptable | Customer returns at market by end of fiscal year. | Profitability shortfall but within planned variance | 50 to 99 records exposed |
| 3. Unacceptable | One product underperforms against market for a year. | Missed Profitability Goal by up to 2% for any year | 100 to 999 records exposed |
| 4. High | Multiple products under perform for multiple years. | Missed Profitability Goals by 2-5% for any year. | 1,000 to 9,999 records exposed |
| 5. Catastrophic | Cannot meet market returns. | Missed Profitability Goals by over 5% for any year. | 10,000+ records exposed |

# DoCRA Approach – Step 6: Implementing The Solution

Providing a clear understanding of:

- One-Time Implementation Costs
- Ongoing Yearly Maintenance Costs
- Internal Labor Requirements and Costs

| Costs | Hardware | Software | Licensing | Consulting Services | (a)<br>Internal Labor Hours | (b)<br>Internal Labor Rate | (d) = (a) x (b)<br>Internal Labor Dollars |
|---|---|---|---|---|---|---|---|
| **One-Time Implementation Costs** | $ 15,000 | $ - | $ 150,000 | $ 30,000 | 300 | $ 100 | $ 30,000 |
| **Yearly Recurring Costs** | $ 5,000 | $ - | $ 5,000 | $ 20,000 | 120 | $ 100 | $ 12,000 |
| | | | | | | | |
| **One-Time Implementation Cost Total** | $ 225,000 | | | | | | |
| **Yearly Recurring Cost Total** | $ 42,000 | | | | | | |

# DoCRA Approach - Step 7: Executive Summary – Budget Request

| | |
|---|---|
| Risk Description | We have Personally Identifiable Information (PII) that, due to lack of controls, could be exfiltrated and could cause: breach response costs, regulatory actions, fines, and a distraction from performing our Mission. |
| Scope | Claim Department located in Chicago, IL |

## Do Nothing - Current State

| Business Impact | State | Description |
|---|---|---|
| MISSION (For Our Customers) | Acceptable | **Business Impact** of "Customer ROI to be 'at market' by end of year" |
| OBJECTIVES (Business Goals) | Unacceptable | **Business Impact** of "Missed Profitability Goal by up to 2%" due to Breach Financial Cost of $1,500,000 with a likelihood of "Multiple Times a Year" |
| OBLIGATIONS (3rd Party & Public) | Unacceptable | **Business Impact** of “Up to 9,999 PII records exposed” (100 times our acceptable level) |

### Risk & Financials

| | | Notes |
|---|---|---|
| Risk Rating | 20 | |
| Estimated Impact Cost | $ 1,500,000 | **Breach cost with likelihood of "Multiple times each year"** |
| One-Time Implementation Cost | NA | |
| Yearly Maintenance Cost | NA | |

## Do Something - Implement DLP Solution

| Business Impact | State | Description |
|---|---|---|
| MISSION (For Our Customers) | Acceptable | **Business Impact** of "Customer returns at or above market" |
| OBJECTIVES (Business Goals) | Acceptable | **Business Impact** of "Profitability shortfall but within planned variance" |
| OBLIGATIONS (3rd Party & Public) | Acceptable | **Business Impact** of “0 to 49 records exposed" |

### Risk & Financials

| | | Notes |
|---|---|---|
| Risk Rating | 6 | |
| Estimated Impact Cost | $ 7,500 | **Breach cost with likelihood of "Expected to occur within 3 years"** |
| One-Time Implementation Cost | $ 225,000 | **within planned variance** |
| Yearly Maintenance Cost | $ 42,000 | |

Budget Approved

# DoCRA Approach – 7 Steps of the Budget Journey

Step 1: Establish where you are

Step 2: Highlight the discontinuity

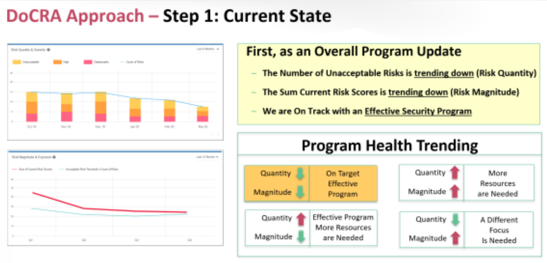
Step 3: Quantify the discontinuity

Step 4: Identify the solution

Step 5: Evaluate not having the solution

Step 6: Define implementing the solution

Step 7: Executive Summary



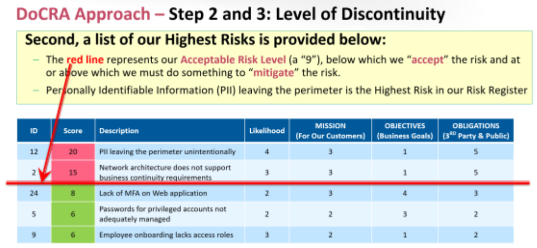
## DoCRA Approach – Step 1: Current State

First, as an Overall Program Update

- The Number of Unacceptable Risks is trending down (Risk Quantity)
- The Sum Current Risk Scores is trending down (Risk Magnitude)
- We are On Track with an Effective Security Program

Program Health Trending

| | |
|---|---|
| Quantity ↓ Magnitude ↓ — On Target Effective Program | Quantity ↑ Magnitude ↑ — More Resources are Needed |
| Quantity ↑ Magnitude ↓ — Effective Program More Resources are Needed | Quantity ↓ Magnitude ↑ — A Different Focus Is Needed |

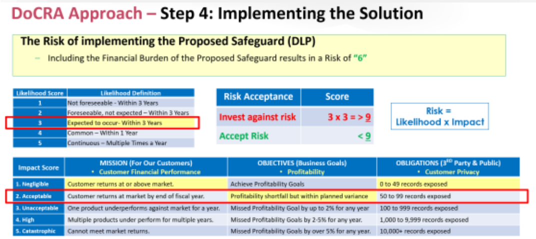


## DoCRA Approach – Step 2 and 3: Level of Discontinuity

Second, a list of our Highest Risks is provided below:

- The red line represents our Acceptable Risk Level (a "9"), below which we "accept" the risk and at or above which we must do something to "mitigate" the risk.
- Personally Identifiable Information (PII) leaving the perimeter is the Highest Risk in our Risk Register

| ID | Score | Description | Likelihood | MISSION (For Our Customers) | OBJECTIVES (Business Goals) | OBLIGATIONS (3RD Party & Public) |
|---|---|---|---|---|---|---|
| 12 | 20 | PII leaving the perimeter unintentionally | 4 | 3 | 1 | 5 |
| 2 | 15 | Network architecture does not support business continuity requirements | 3 | 3 | 1 | 5 |
| 24 | 8 | Lack of MFA on Web application | 2 | 3 | 4 | 3 |
| 5 | 6 | Passwords for privileged accounts not adequately managed | 2 | 2 | 3 | 2 |
| 9 | 6 | Employee onboarding lacks access roles | 3 | 2 | 1 | 2 |



## DoCRA Approach – Step 4: Implementing the Solution

The Risk of implementing the Proposed Safeguard (DLP)

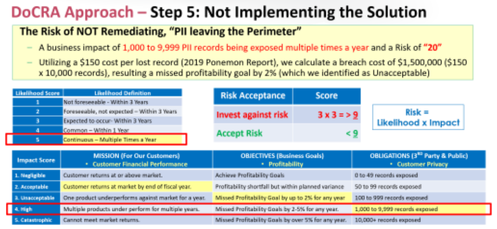
- Including the Financial Burden of the Proposed Safeguard results in a Risk of "6"

| Likelihood Score | Likelihood Definition |
|---|---|
| 1 | Not foreseeable - Within 3 Years |
| 2 | Foreseeable, not expected – Within 3 Years |
| 3 | Expected to occur- Within 3 Years |
| 4 | Common – Within 1 Year |
| 5 | Continuous – Multiple Times a Year |

| Risk Acceptance | Score |
|---|---|
| Invest against risk | 3 x 3 = > 9 |
| Accept Risk | < 9 |

Risk = Likelihood x Impact

| Impact Score | MISSION (For Our Customers) • Customer Financial Performance | OBJECTIVES (Business Goals) • Profitability | OBLIGATIONS (3RD Party & Public) • Customer Privacy |
|---|---|---|---|
| 1. Negligible | Customer returns at or above market. | Achieve Profitability Goals | 0 to 49 records exposed |
| 2. Acceptable | Customer returns at market by end of fiscal year. | Profitability shortfall but within planned variance | 50 to 99 records exposed |
| 3. Unacceptable | One product underperforms against market for a year. | Missed Profitability Goal by up to 2% for any year | 100 to 999 records exposed |
| 4. High | Multiple products under perform for multiple years. | Missed Profitability Goals by 2-5% for any year. | 1,000 to 9,999 records exposed |
| 5. Catastrophic | Cannot meet market returns. | Missed Profitability Goals by over 5% for any year. | 10,000+ records exposed |



## DoCRA Approach – Step 5: Not Implementing the Solution

The Risk of NOT Remediating, "PII leaving the Perimeter"

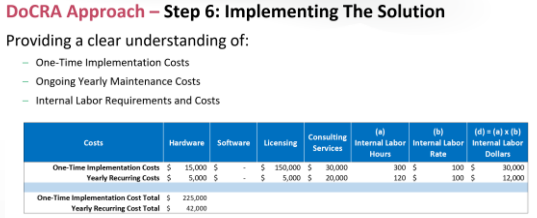
- A business impact of 1,000 to 9,999 PII records being exposed multiple times a year and a Risk of "20"
- Utilizing a $150 cost per lost record (2019 Ponemon Report), we calculate a breach cost of $1,500,000 ($150 x 10,000 records), resulting a missed profitability goal by 2% (which we identified as Unacceptable)

| Likelihood Score | Likelihood Definition |
|---|---|
| 1 | Not foreseeable - Within 3 Years |
| 2 | Foreseeable, not expected – Within 3 Years |
| 3 | Expected to occur- Within 3 Years |
| 4 | Common – Within 1 Year |
| 5 | Continuous – Multiple Times a Year |

| Risk Acceptance | Score |
|---|---|
| Invest against risk | 3 x 3 = > 9 |
| Accept Risk | < 9 |

Risk = Likelihood x Impact

| Impact Score | MISSION (For Our Customers) • Customer Financial Performance | OBJECTIVES (Business Goals) • Profitability | OBLIGATIONS (3RD Party & Public) • Customer Privacy |
|---|---|---|---|
| 1. Negligible | Customer returns at or above market. | Achieve Profitability Goals | 0 to 49 records exposed |
| 2. Acceptable | Customer returns at market by end of fiscal year. | Profitability shortfall but within planned variance | 50 to 99 records exposed |
| 3. Unacceptable | One product underperforms against market for a year. | Missed Profitability Goal by up to 2% for any year | 100 to 999 records exposed |
| 4. High | Multiple products under perform for multiple years. | Missed Profitability Goals by 2-5% for any year. | 1,000 to 9,999 records exposed |
| 5. Catastrophic | Cannot meet market returns. | Missed Profitability Goals by over 5% for any year. | 10,000+ records exposed |

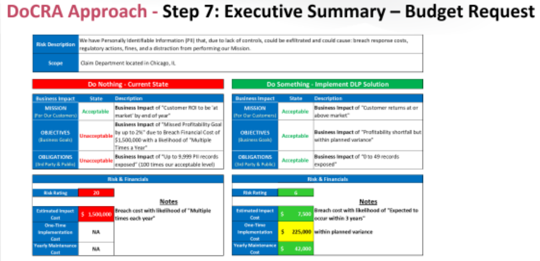


## DoCRA Approach – Step 6: Implementing The Solution

Providing a clear understanding of:

- One-Time Implementation Costs
- Ongoing Yearly Maintenance Costs
- Internal Labor Requirements and Costs

| Costs | Hardware | Software | Licensing | Consulting Services | (a) Internal Labor Hours | (b) Internal Labor Rate | (d) = (a) x (b) Internal Labor Dollars |
|---|---|---|---|---|---|---|---|
| One-Time Implementation Costs | $ 15,000 | $ - | $ 150,000 | $ 30,000 | 300 | $ 100 | $ 30,000 |
| Yearly Recurring Costs | $ 5,000 | $ - | $ 5,000 | $ 20,000 | 120 | $ 100 | $ 12,000 |
| | | | | | | | |
| One-Time Implementation Cost Total | $ 225,000 | | | | | | |
| Yearly Recurring Cost Total | $ 42,000 | | | | | | |



## DoCRA Approach - Step 7: Executive Summary – Budget Request

| | |
|---|---|
| Risk Description | We have Personally Identifiable Information (PII) that, due to lack of controls, could be exfiltrated and could cause: breach response costs, regulatory actions, fines, and a distraction from performing our Mission. |
| Scope | Claim Department located in Chicago, IL |

Do Nothing - Current State

| Business Impact | State | Description |
|---|---|---|
| MISSION (For Our Customers) | Acceptable | Business Impact of "Customer ROI to be 'at market' by end of year" |
| OBJECTIVES (Business Goals) | Unacceptable | Business Impact of "Missed Profitability Goal by up to 2%" due to Breach Financial Cost of $1,500,000 with a likelihood of "Multiple Times a Year" |
| OBLIGATIONS (3rd Party & Public) | Unacceptable | Business Impact of "Up to 9,999 PII records exposed" (100 times our acceptable level) |

Risk & Financials

| | | Notes |
|---|---|---|
| Risk Rating | 20 | |
| Estimated Impact Cost | $ 1,500,000 | Breach cost with likelihood of "Multiple times each year" |
| One-Time Implementation Cost | NA | |
| Yearly Maintenance Cost | NA | |

Do Something - Implement DLP Solution

| Business Impact | State | Description |
|---|---|---|
| MISSION (For Our Customers) | Acceptable | Business Impact of "Customer returns at or above market" |
| OBJECTIVES (Business Goals) | Acceptable | Business Impact of "Profitability shortfall but within planned variance" |
| OBLIGATIONS (3rd Party & Public) | Acceptable | Business Impact of "0 to 49 records exposed" |

Risk & Financials

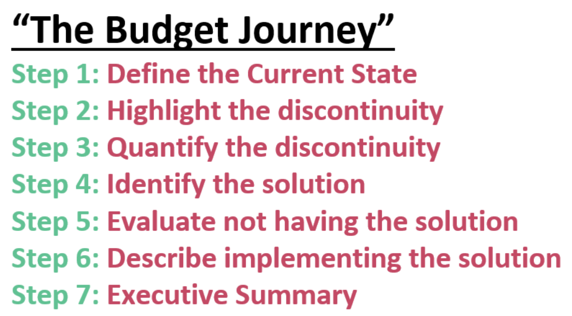
| | | Notes |
|---|---|---|
| Risk Rating | 6 | |
| Estimated Impact Cost | $ 7,500 | Breach cost with likelihood of "Expected to occur within 3 years" |
| One-Time Implementation Cost | $ 225,000 | within planned variance |
| Yearly Maintenance Cost | $ 42,000 | |

# Putting It All Together….

## Level 1 - *Immediate*

**Proven Storyline**

(Business Case Templates)



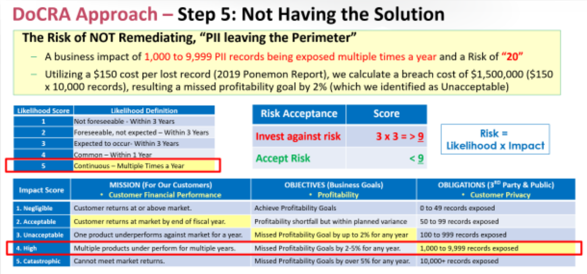
### "The Budget Journey"

Step 1: Define the Current State
Step 2: Highlight the discontinuity
Step 3: Quantify the discontinuity
Step 4: Identify the solution
Step 5: Evaluate not having the solution
Step 6: Describe implementing the solution
Step 7: Executive Summary

## Level 2 – *3 Months*

**DoCRA Language**

(Terminology)



### DoCRA Approach – Step 5: Not Having the Solution

**The Risk of NOT Remediating, "PII leaving the Perimeter"**

- A business impact of 1,000 to 9,999 PII records being exposed multiple times a year and a Risk of "20"
- Utilizing a $150 cost per lost record (2019 Ponemon Report), we calculate a breach cost of $1,500,000 ($150 x 10,000 records), resulting a missed profitability goal by 2% (which we identified as Unacceptable)

| Likelihood Score | Likelihood Definition |
|---|---|
| 1 | Not foreseeable - Within 3 Years |
| 2 | Foreseeable, not expected – Within 3 Years |
| 3 | Expected to occur- Within 3 Years |
| 4 | Common – Within 1 Year |
| 5 | Continuous – Multiple Times a Year |

| Risk Acceptance | Score |
|---|---|
| Invest against risk | 3 x 3 = > 9 |
| Accept Risk | < 9 |

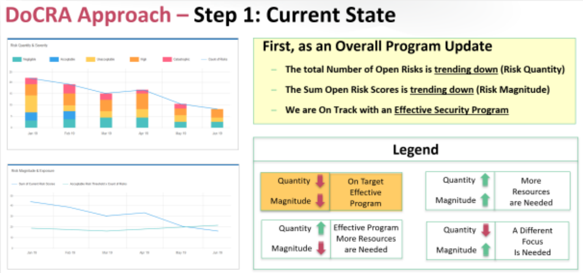
Risk = Likelihood x Impact

| Impact Score | MISSION (For Our Customers)<br>• Customer Financial Performance | OBJECTIVES (Business Goals)<br>• Profitability | OBLIGATIONS (3$^{RD}$ Party & Public)<br>• Customer Privacy |
|---|---|---|---|
| 1. Negligible | Customer returns at or above market. | Achieve Profitability Goals | 0 to 49 records exposed |
| 2. Acceptable | Customer returns at market by end of fiscal year. | Profitability shortfall but within planned variance | 50 to 99 records exposed |
| 3. Unacceptable | One product underperforms against market for a year. | Missed Profitability Goal by up to 2% for any year | 100 to 999 records exposed |
| 4. High | Multiple products under perform for multiple years. | Missed Profitability Goals by 2-5% for any year. | 1,000 to 9,999 records exposed |
| 5. Catastrophic | Cannot meet market returns. | Missed Profitability Goals by over 5% for any year. | 10,000+ records exposed |

## Level 3 - *6 Months*

**DoCRA Management**

(Process)



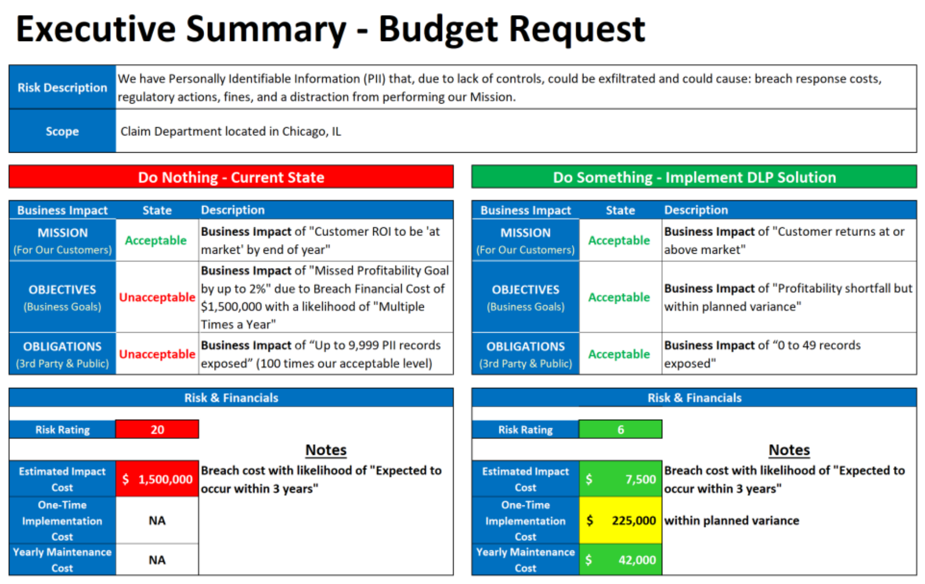
### DoCRA Approach – Step 1: Current State

**First, as an Overall Program Update**

- The total Number of Open Risks is trending down (Risk Quantity)
- The Sum Open Risk Scores is trending down (Risk Magnitude)
- We are On Track with an Effective Security Program

**Legend**

| | |
|---|---|
| Quantity ↓<br>Magnitude ↓ | On Target Effective Program |
| Quantity ↑<br>Magnitude ↑ | More Resources are Needed |
| Quantity ↑<br>Magnitude ↓ | Effective Program More Resources are Needed |
| Quantity ↓<br>Magnitude ↑ | A Different Focus Is Needed |



### Executive Summary - Budget Request

| | |
|---|---|
| Risk Description | We have Personally Identifiable Information (PII) that, due to lack of controls, could be exfiltrated and could cause: breach response costs, regulatory actions, fines, and a distraction from performing our Mission. |
| Scope | Claim Department located in Chicago, IL |

**Do Nothing - Current State**

| Business Impact | State | Description |
|---|---|---|
| MISSION (For Our Customers) | Acceptable | **Business Impact** of "Customer ROI to be 'at market' by end of year" |
| OBJECTIVES (Business Goals) | Unacceptable | **Business Impact** of "Missed Profitability Goal by up to 2%" due to Breach Financial Cost of $1,500,000 with a likelihood of "Multiple Times a Year" |
| OBLIGATIONS (3rd Party & Public) | Unacceptable | **Business Impact** of "Up to 9,999 PII records exposed" (100 times our acceptable level) |

**Risk & Financials**

| | | Notes |
|---|---|---|
| Risk Rating | 20 | |
| Estimated Impact Cost | $ 1,500,000 | Breach cost with likelihood of "Expected to occur within 3 years" |
| One-Time Implementation Cost | NA | |
| Yearly Maintenance Cost | NA | |

**Do Something - Implement DLP Solution**

| Business Impact | State | Description |
|---|---|---|
| MISSION (For Our Customers) | Acceptable | **Business Impact** of "Customer returns at or above market" |
| OBJECTIVES (Business Goals) | Acceptable | **Business Impact** of "Profitability shortfall but within planned variance" |
| OBLIGATIONS (3rd Party & Public) | Acceptable | **Business Impact** of "0 to 49 records exposed" |

**Risk & Financials**

| | | Notes |
|---|---|---|
| Risk Rating | 6 | |
| Estimated Impact Cost | $ 7,500 | Breach cost with likelihood of "Expected to occur within 3 years" |
| One-Time Implementation Cost | $ 225,000 | within planned variance |
| Yearly Maintenance Cost | $ 42,000 | |

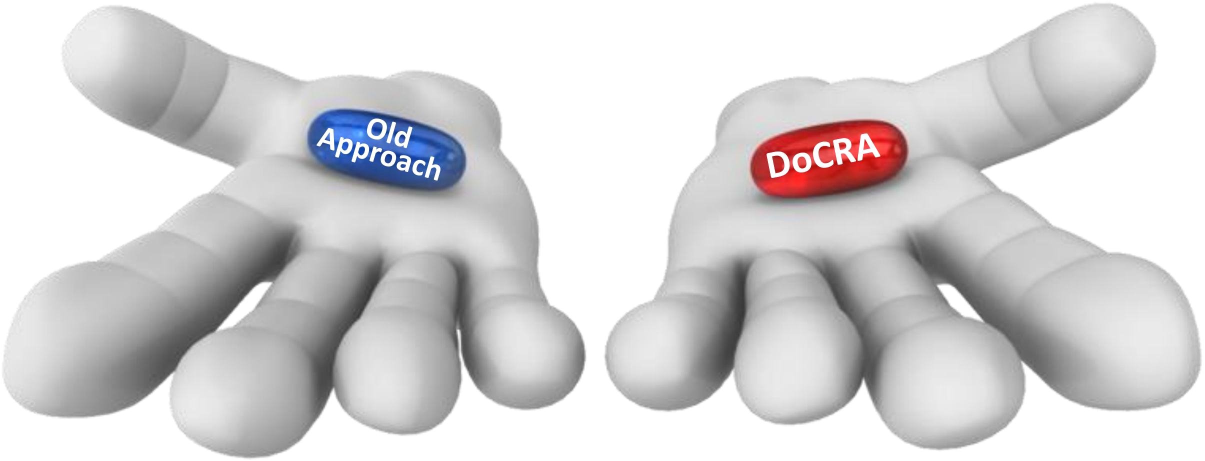
# Now That You Have Seen A More Powerful Approach…

- You have a choice to make:

A. Continue using the **old approach** for budget approval

or

B. Utilize something new and more powerful (**DoCRA**).



# Some Potential Questions or Concerns At This Point…

- How do we fill out the business impact scores?
- Are there templates we can use?
- How do we get the business buy-in?
- It seems daunting and difficult.

# Success Strategies To Address Questions and Concerns

- Many worthwhile endeavors are difficult the first time through it!
  - We all learned to drive cars - that was difficult at first but now it’s second nature!
- **Senior leadership participates** in defining and approving the Acceptable Risk Definition.
- Many organizations **perform Level 2 and Level 3 (implementing DoCRA) as one project.**
- Seek out **experienced talent inside or outside your organization** that have the right skills to lead you through this initiative.

# Thank You

# Now Go Get Your Budgets Approved!

**Jim Mirochnik,** MBA, PMP, PCI QSA, ISO 27001 Auditor
CEO, Senior Partner
**HALOCK** Security Labs
jmirochnik@halock.com
847.221.0205 office

A link to download a free copy of the tools and templates for this RSA Presentation is provided here: www.halock.com/rsa2020

# Appendix A - “The Budget Journey”

## Level 1: A Proven Storyline for Requesting Budget

1. The seven steps of the “Budget Journey”
2. A financial cost template
3. An Executive Summary – Budget Request template

A link to download a free copy of the above tools and templates is provided here: www.halock.com/rsa2020

# Appendix B - Terminology

## Level 2: Resources for Implementing DoCRA Terminology

1. Sample Business Impact Level Matrixes
2. Sample Likelihood Level Matrixes

A link to download a free copy of the above tools and templates is provided here: www.halock.com/rsa2020

# Appendix C – Process

## Level 3: Resources for Implementing DoCRA Management

1. Samples of Risk Trending Charts
2. DoCRA Checklist – To make sure your Risk Assessment meets DoCRA

A link to download a free copy of the above tools and templates is provided here: www.halock.com/rsa2020

# Appendix D – Supplementary Exhibits

## What is a DoCRA Risk Assessment?

- **What it's Not**
  - It's not a list of "what keeps you up at night"
  - It's not a brainstorming session with the executives
  - It's not a automated vulnerability scan
  - It's not a maturity assessment or gap assessment
- **What it Is**
  - Comprehensive Inventory of your information assets
  - Comprehensive review for each information asset
    - Threat
    - Vulnerability
    - Impact definitions for Mission, Objectives and Obligations
    - Likelihood
  - An Acceptable Risk Level Definition
  - A process to assess the burden of proposed safeguards