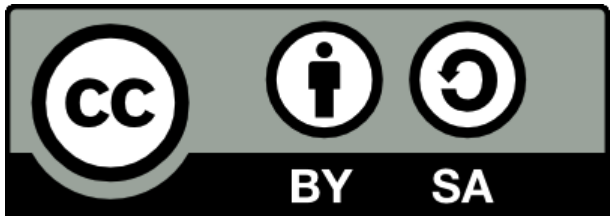
this talk is about a new risk assessment tool

This presentation is




(except if it's someone else's content)

latest version at

https://binary.protect.io

# Binary Risk Assessment

me = Ben Sapiro

email = ben @ protect.io

“why don't we do security?”

- Dan Jones

# Is it a resourcing problem?


{budget | education | process }

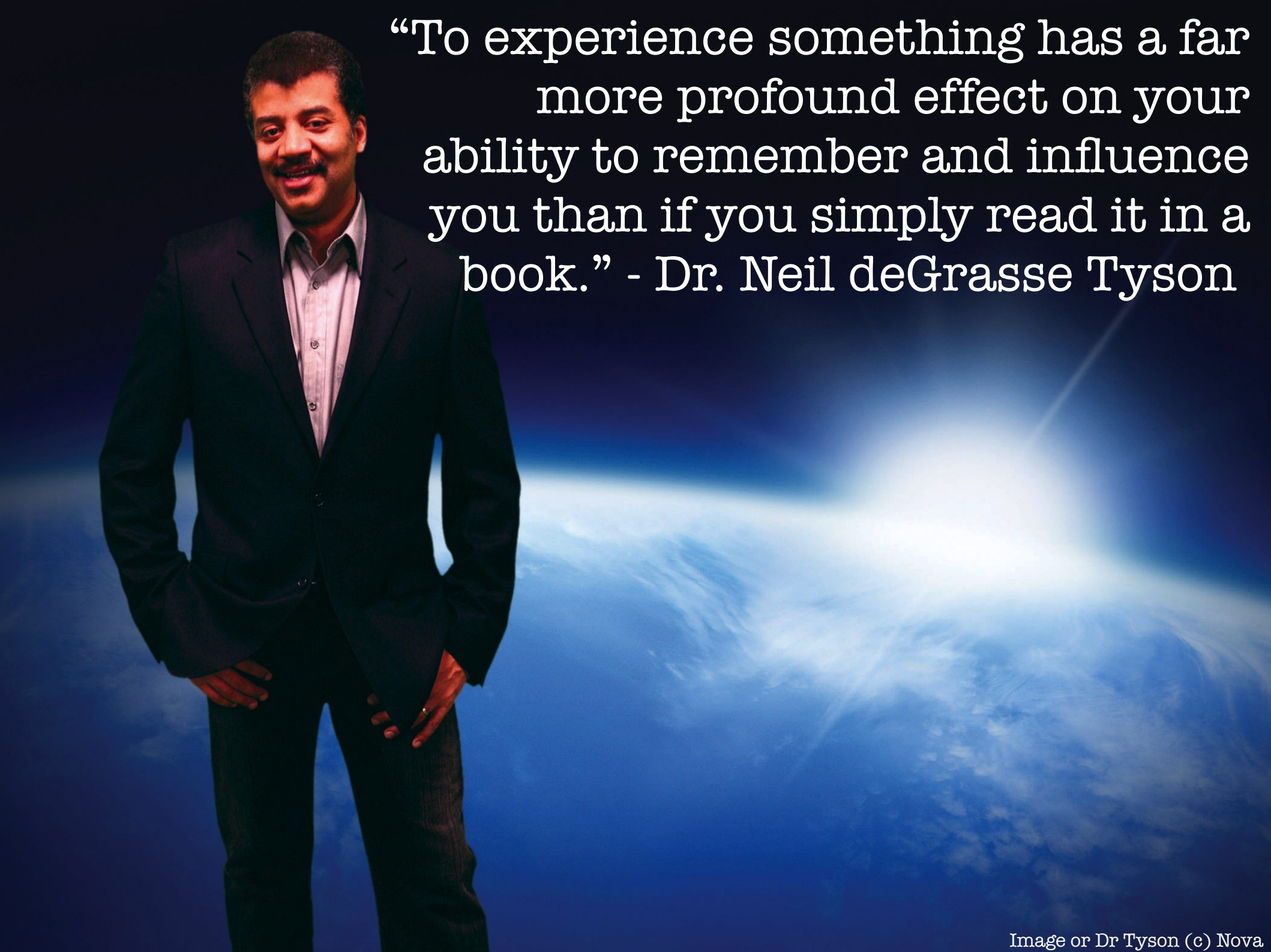
Money Image (cc) Amagill @ Flickr

Even the simplest change results in resistance


Protest Image (cc) soukup @ Flickr

Why?

It's something intrinsic to
how we see and respond to the world

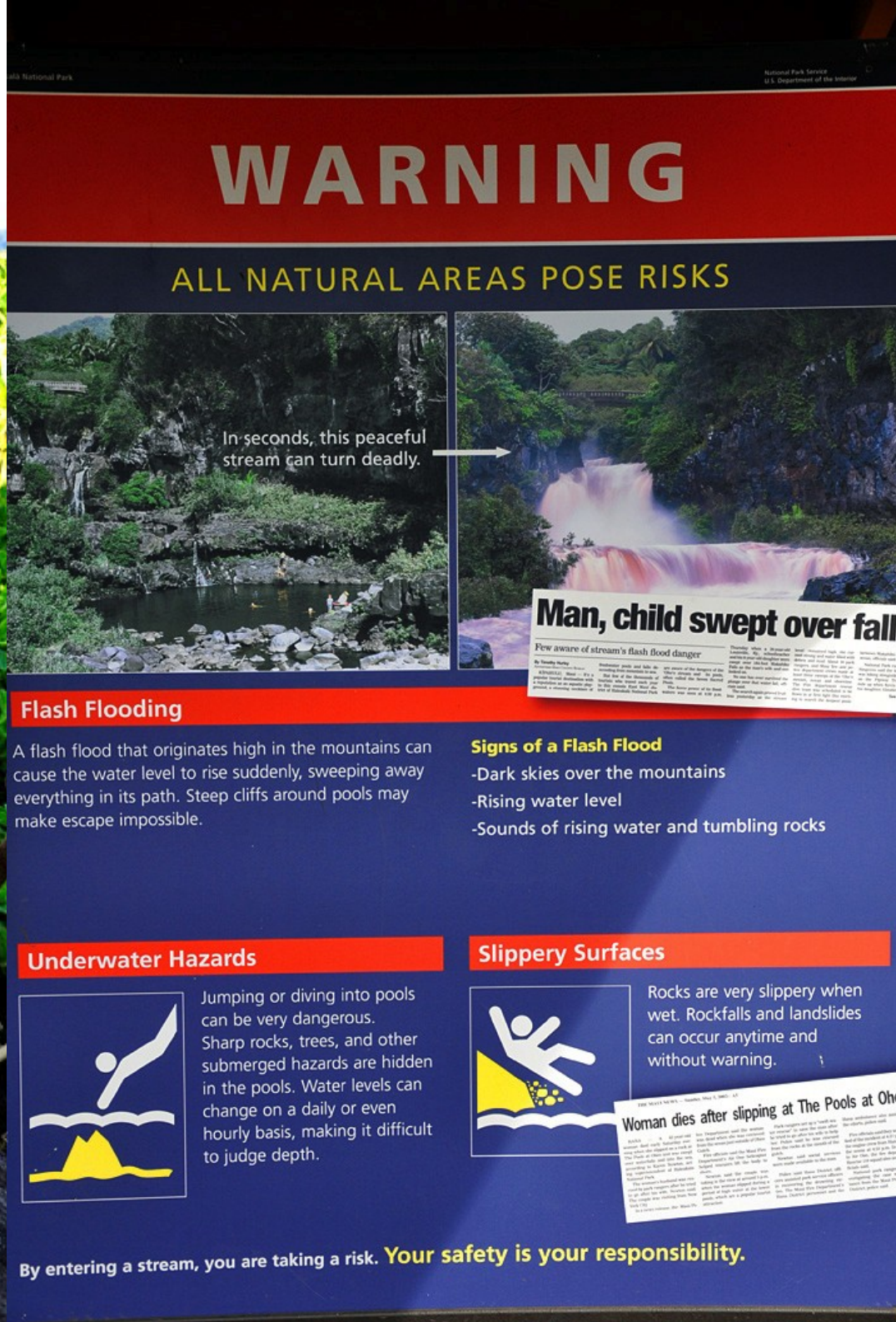

“To experience something has a far more profound effect on your ability to remember and influence you than if you simply read it in a book.” - Dr. Neil deGrasse Tyson
Image or Dr Tyson (c) Nova

Sabre tooth image (c) skills4life.com.au

Is our understanding of risk hardwired?


As a species we're bad at processing abstract risk

Lehman Brothers (cc) williacw @ flickr

# Cautionary tales are ignored in IT

WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW-

Sign In | RSS Feeds

## Exclusive: Computer Virus Hits U.S. Drone Fleet

A computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones.

“What's the risk of THAT happening to us?”

Dice image (cc) photography-andreas @ flickr

Ok, so what's the problem again?


Two people image (cc) pietroizzo @ Flickr

Can we have better risk conversations?

Is it a poor workmen who blames their tools?

Risk = Likelihood x Impact

"Do not place hope in finding a secret technique, Polish the mind through ceaseless training; that is the key to effective techniques."

- Kyuzo Mifune.

"Do not place hope in finding a secret technique, Polish the mind through ceaseless training; that is the key to effective techniques."

- Kyuzo Mifune.

"Do not place hope in finding a secret technique, Polish the mind through ceaseless training; that is the key to effective techniques."

- Kyuzo Mifune.

What if we could make risk discussions faster and simpler but with more clarity?

| | FAIR | COBRA | OCTAVE | SOMAP |
|---|---|---|---|---|
| Proprietary licensing | ◐ | ● | | |
| Complex | ● | ● | ● | ● |
| Training required | ● | | | |
| Limited transparency | | ● | | |
| Part of a full framework | | ● | ● | ● |

| | FAIR | COBRA | OCTAVE | SOMAP |
|---|---|---|---|---|
| Open license | ◐ | | ● | ● |
| Simple | | | | |
| Quick to learn | | | | |
| Transparent | ● | | ● | ● |
| Standalone | ● | | | |

| | |
|---|---|
| Open license | Lowers barriers to adoption |
| Simple | Fast to complete |
| Quick to learn | Can be used by the business |
| Transparent | Accounts for subjectivity |
| Standalone | Integrate with current practices |

Open license

Simple

Quick to learn

Transparent

Standalone

Make the world a safer place by sharing tools and techniques freely and openly.

Open license

Simple

Quick to learn

Transparent

Standalone

The 5 minute rule:
Learn it in 5
Use is in 5
Discuss in 5 minutes

(endless practice)

Open license

Simple

Quick to learn

Transparent

Standalone

The napkin rule:

Be able to do it on the back of a napkin, no computer required.

Open license

Simple

Quick to learn

Transparent

Standalone

Highlight subjectivity and provide a framework for consensus.

Be better than R = I x L

Open license

Simple

Quick to learn

Transparent

Standalone

Businesses are trained to think in Impact and Likelihood when defining Risk; be compatible and avoid religious wars.

Open license

Simple

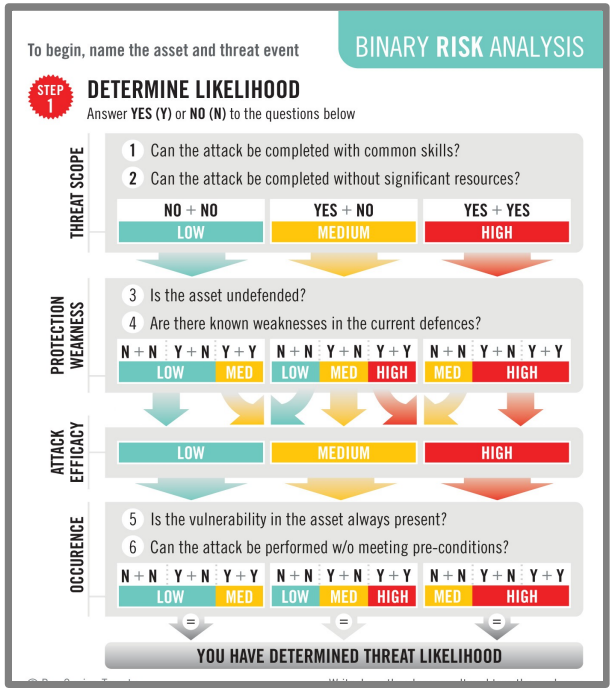
Quick to learn

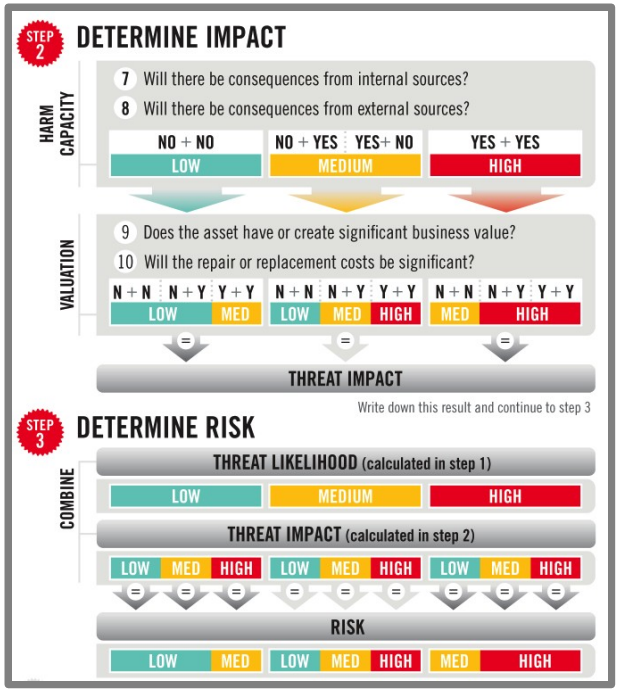
Transparent

Standalone

Limit the inputs to a set number of queries (10).

Constrain the analysis, collect only yes or no responses.




# Binary Risk Analysis

The work card is available at https://binary.protect.io

First release has a technical focus

(Binary Risk Analysis - Technical)

# Risk

Likelihood | Impact

10 questions

Risk

Likelihood Impact

6+4

10 questions

# Risk

Name the asset

Name the threat event

Likelihood Impact

10 questions

# Can my pilot haz virus?


RQ-1 drone iImage (cc) JimNTexas @ Flickr

Risk

Drone ground station | asset

Get infected by a virus | threat event

Likelihood | Impact

10 questions

## Question 0001

Can the attack be completed with common skills?

YES

0000000001

## Question 0010

Can the attack be completed without significant resources?

YES

0 0 0 0 0 0 0 0 1 1

# Question 0011

Is the asset undefended?

NO

0 0 0 0 0 0 0 0 1 1

## Question 0100

Are there known weaknesses in the current defences?

YES

0 0 0 0 0 0 1 0 1 1

## Question 0101

Is the vulnerability in the asset always present?

YES

0 0 0 0 0 1 1 0 1 1

## Question 0110

Can the attack be performed without meeting pre-conditions?

NO

0 0 0 0 0 1 1 0 1 1

To begin, name the asset and threat event

# BINARY **RISK** ANALYSIS

STEP 1

## DETERMINE LIKELIHOOD

Answer **YES (Y)** or **NO (N)** to the questions below

### THREAT SCOPE

1 Can the attack be completed with common skills?

2 Can the attack be completed without significant resources?

| NO + NO | YES + NO | YES + YES |
|---|---|---|
| LOW | MEDIUM | HIGH |

### PROTECTION WEAKNESS

3 Is the asset undefended?

4 Are there known weaknesses in the current defences?

| N + N | Y + N | Y + Y | N + N | Y + N | Y + Y | N + N | Y + N | Y + Y |
|---|---|---|---|---|---|---|---|---|
| LOW | | MED | LOW | MED | HIGH | MED | HIGH | |

### ATTACK EFFICACY

| LOW | MEDIUM | HIGH |
|---|---|---|

### OCCURENCE

5 Is the vulnerability in the asset always present?

6 Can the attack be performed w/o meeting pre-conditions?

| N + N | Y + N | Y + Y | N + N | Y + N | Y + Y | N + N | Y + N | Y + Y |
|---|---|---|---|---|---|---|---|---|
| LOW | | MED | LOW | MED | HIGH | MED | HIGH | |

=

**YOU HAVE DETERMINED THREAT LIKELIHOOD**

# Question 0111

Will there be consequences from internal sources?

YES

0 0 0 1 0 1 1 0 1 1

## Question 1000

Will there be consequences from external sources?

YES

0 0 1 1 0 1 1 0 1 1

# Question 1001

Does the asset have or create significant business value?

YES

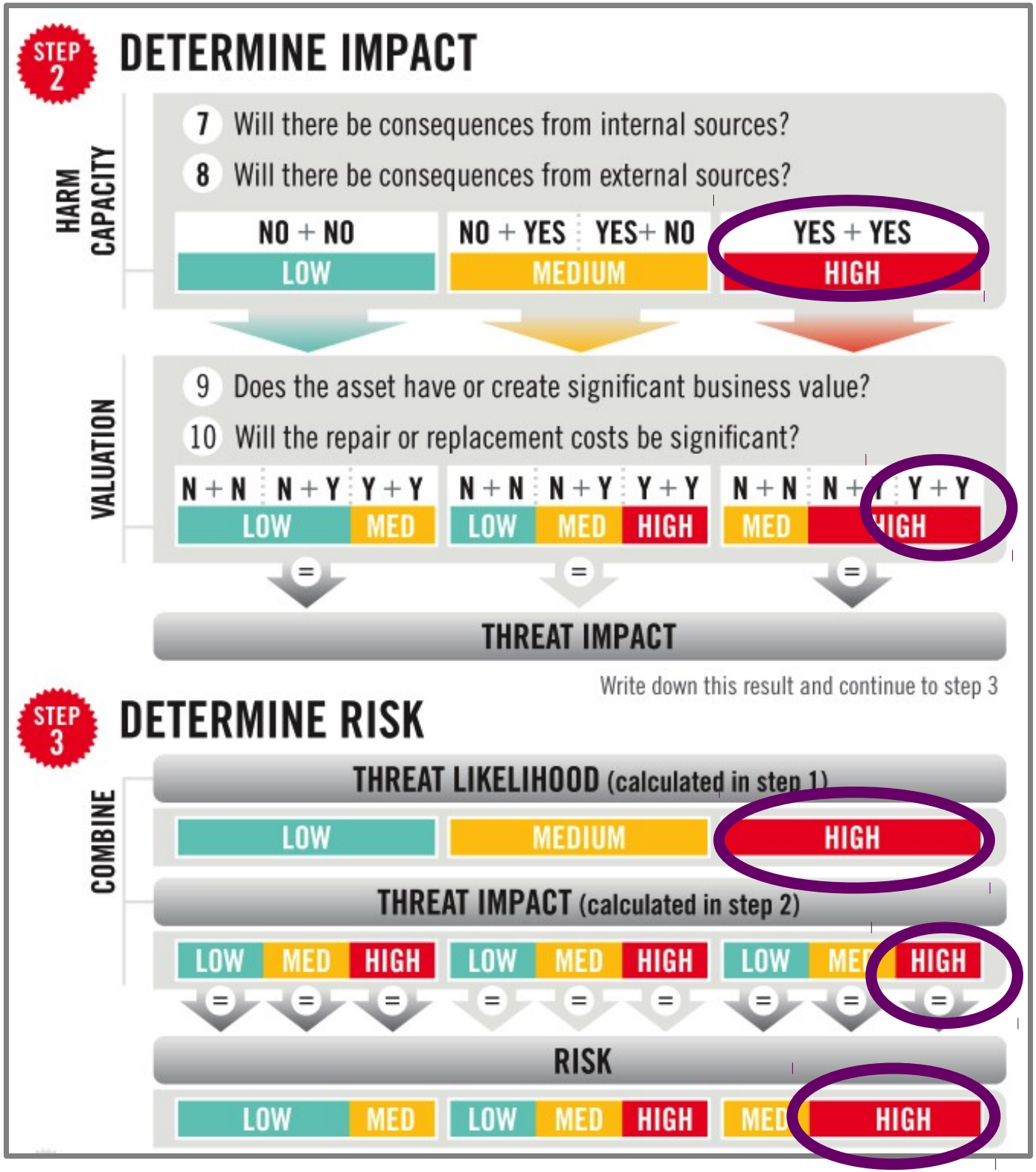
0 1 1 1 0 1 1 0 1 1

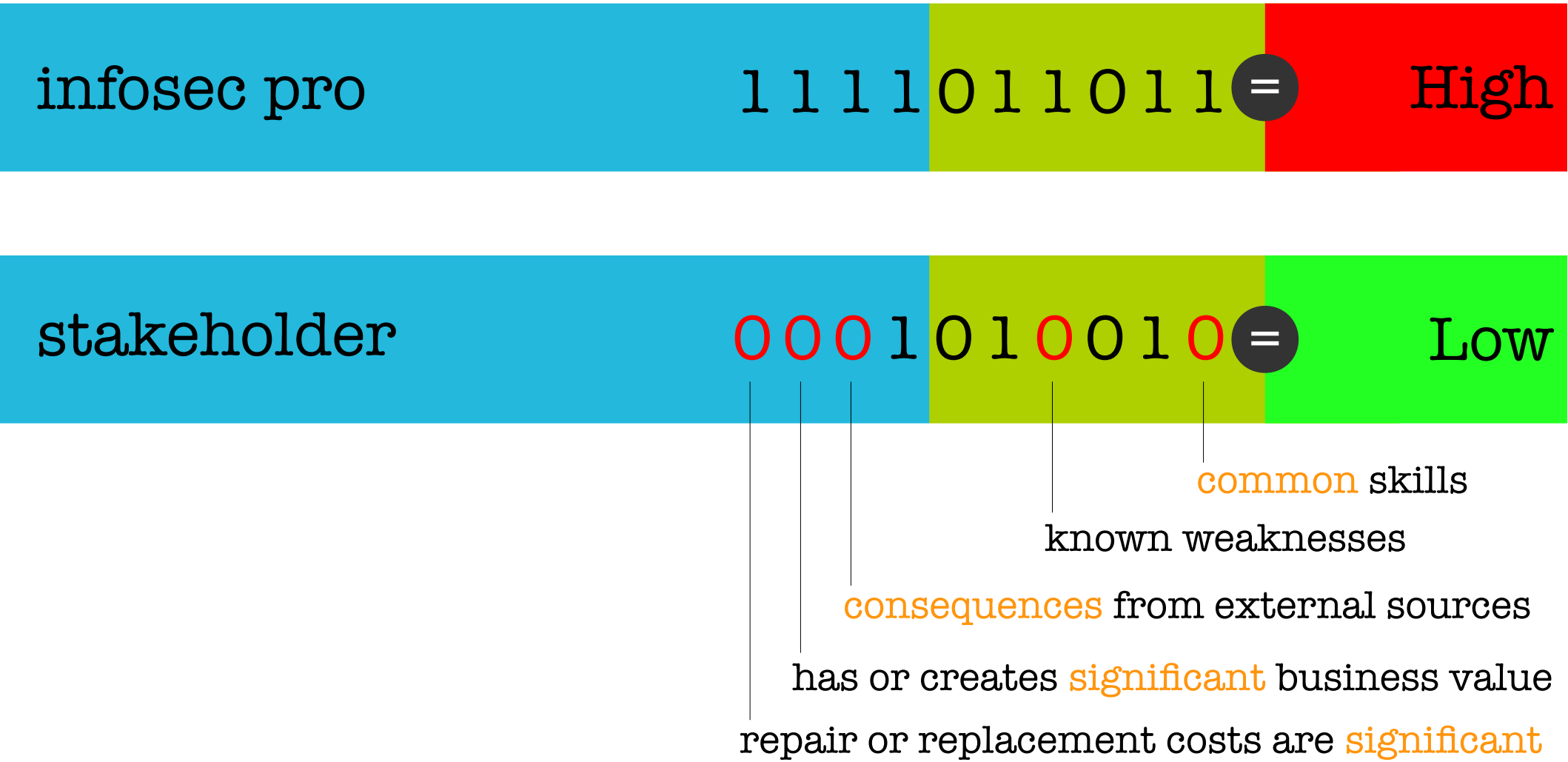
# Question 1010

Will the repair or replacement costs be significant?

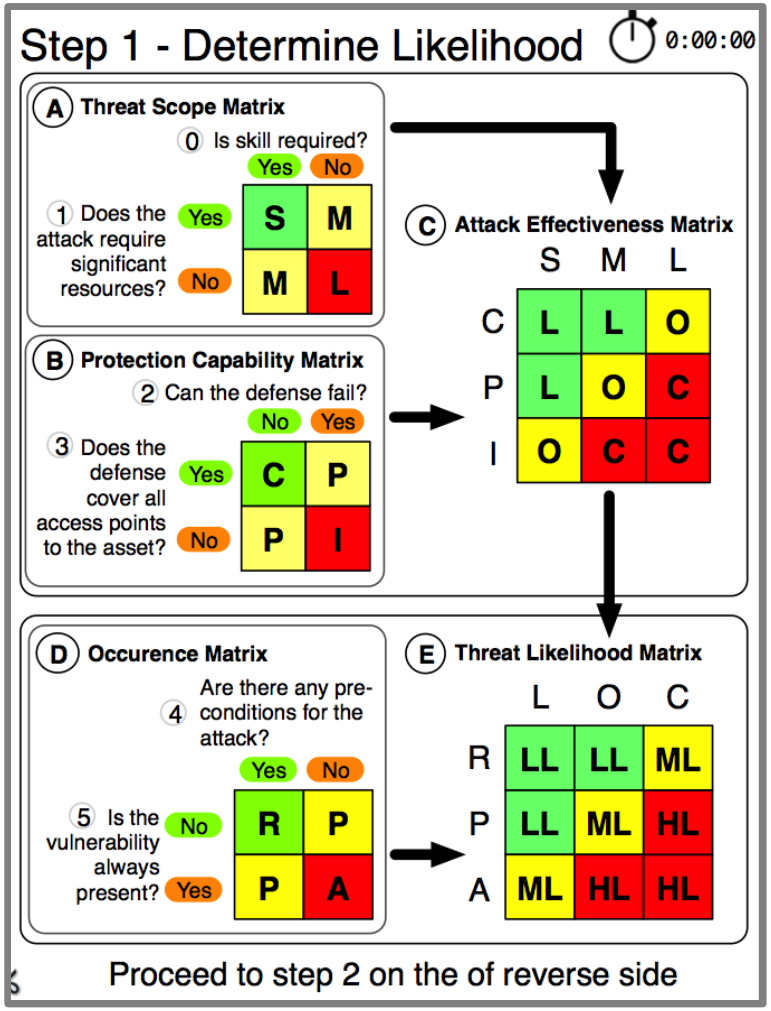
YES

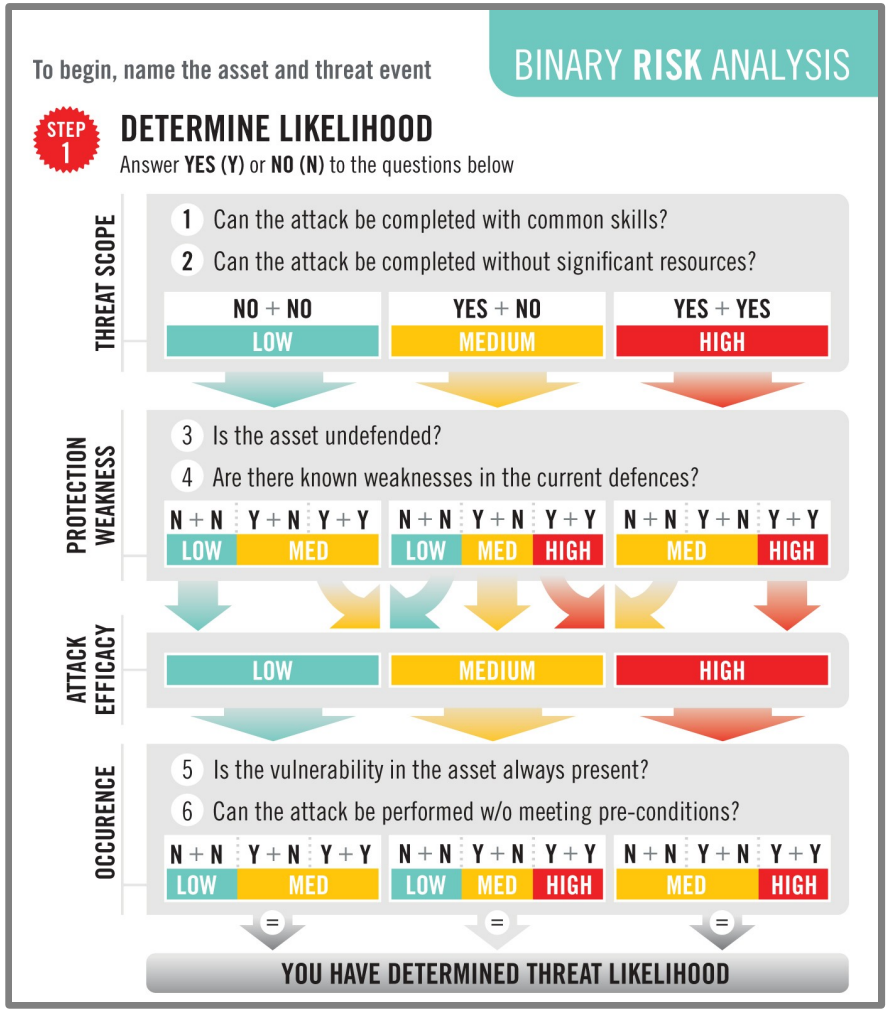
1 1 1 1 0 1 1 0 1 1


STEP 2
DETERMINE IMPACT
HARM CAPACITY
7 Will there be consequences from internal sources?
8 Will there be consequences from external sources?
NO + NO
LOW
NO + YES
YES + NO
MEDIUM
YES + YES
HIGH
VALUATION
9 Does the asset have or create significant business value?
10 Will the repair or replacement costs be significant?
N + N
N + Y
Y + Y
LOW
MED
N + N
N + Y
Y + Y
LOW
MED
HIGH
N + N
N + Y
Y + Y
MED
HIGH
=
THREAT IMPACT
Write down this result and continue to step 3
STEP 3
DETERMINE RISK
COMBINE
THREAT LIKELIHOOD (calculated in step 1)
LOW
MEDIUM
HIGH
THREAT IMPACT (calculated in step 2)
LOW
MED
HIGH
LOW
MED
HIGH
LOW
HIGH
=
RISK
LOW
MED
LOW
MED
HIGH
HIGH

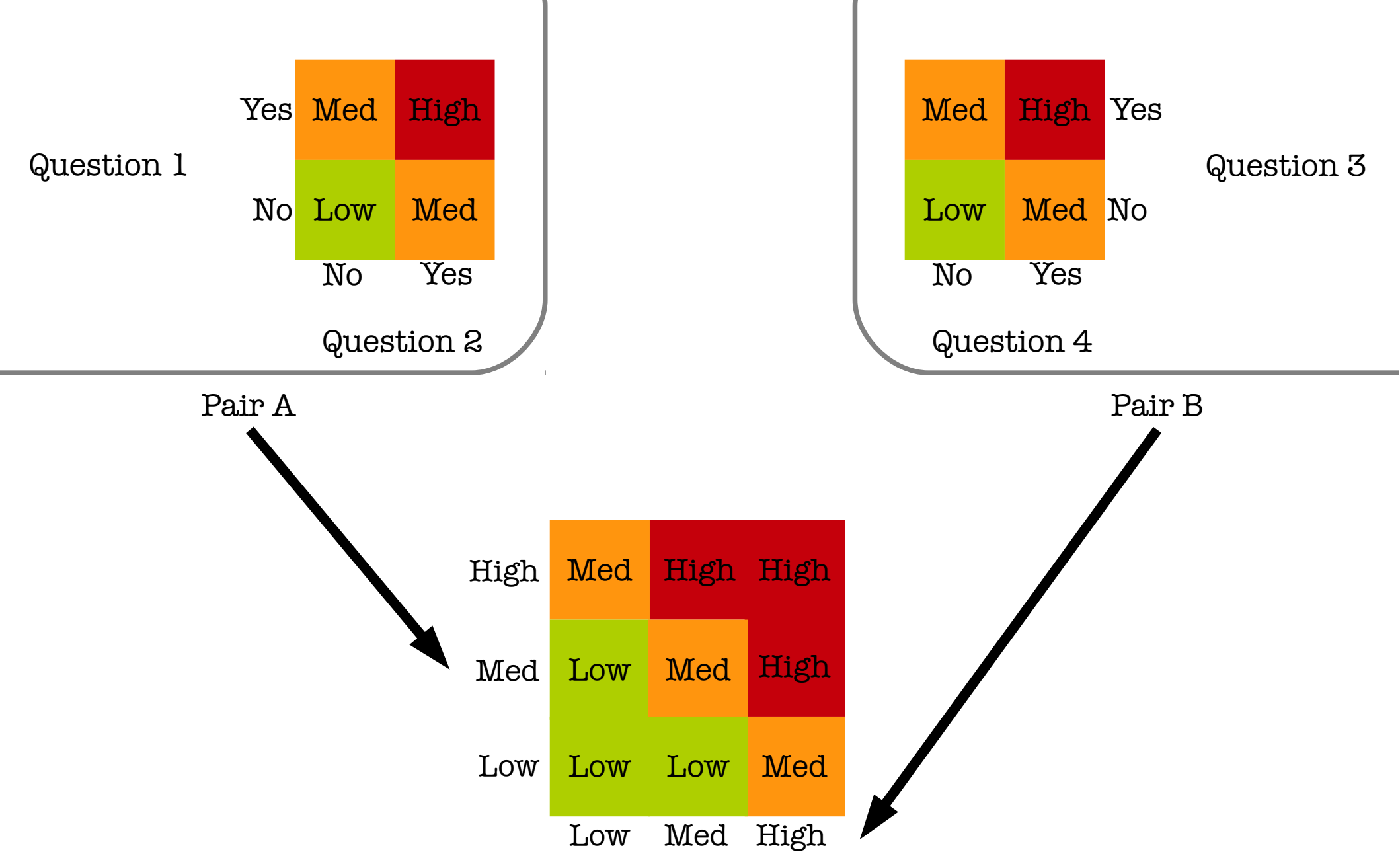



The correct conversation with the business

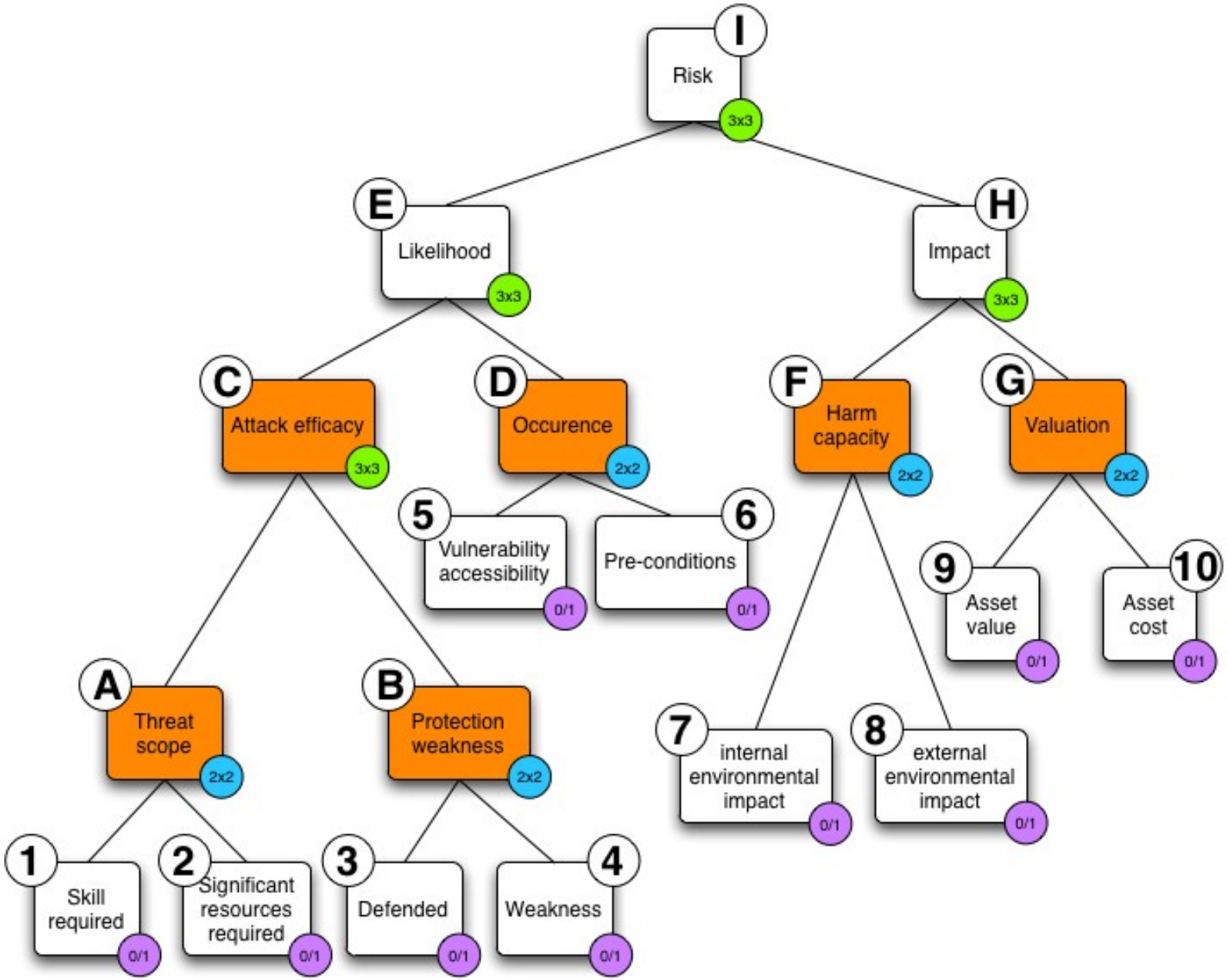



# The back story




# The underlying logic




More than just High, Medium and Low


# Wrapping it up

# BRA

| | |
|---|---|
| Open license | Lowers barriers to adoption |
| Simple | Fast to complete |
| Quick to learn | Can be used by the business |
| Transparent | Accounts for subjectivity |
| Standalone | Integrate with current practices |

# A possible future

What happens if we're all having brief but effective conversations about risk?

# My ask

Print the work card
Carry it with you
Use it in your risk discussions
Give it to colleagues, vendors & partners
Critique it

(Send me feedback)

# tl;dr

Answer the 10 questions
Map each answer against the work card to calculate risk

# “Make this an app”

# Thank you

Download the community iPad app at
https://binary.protect.io

(there's also a paper and other stuff)