

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 }

Even the simplest  
change results in  
resistance



Why?

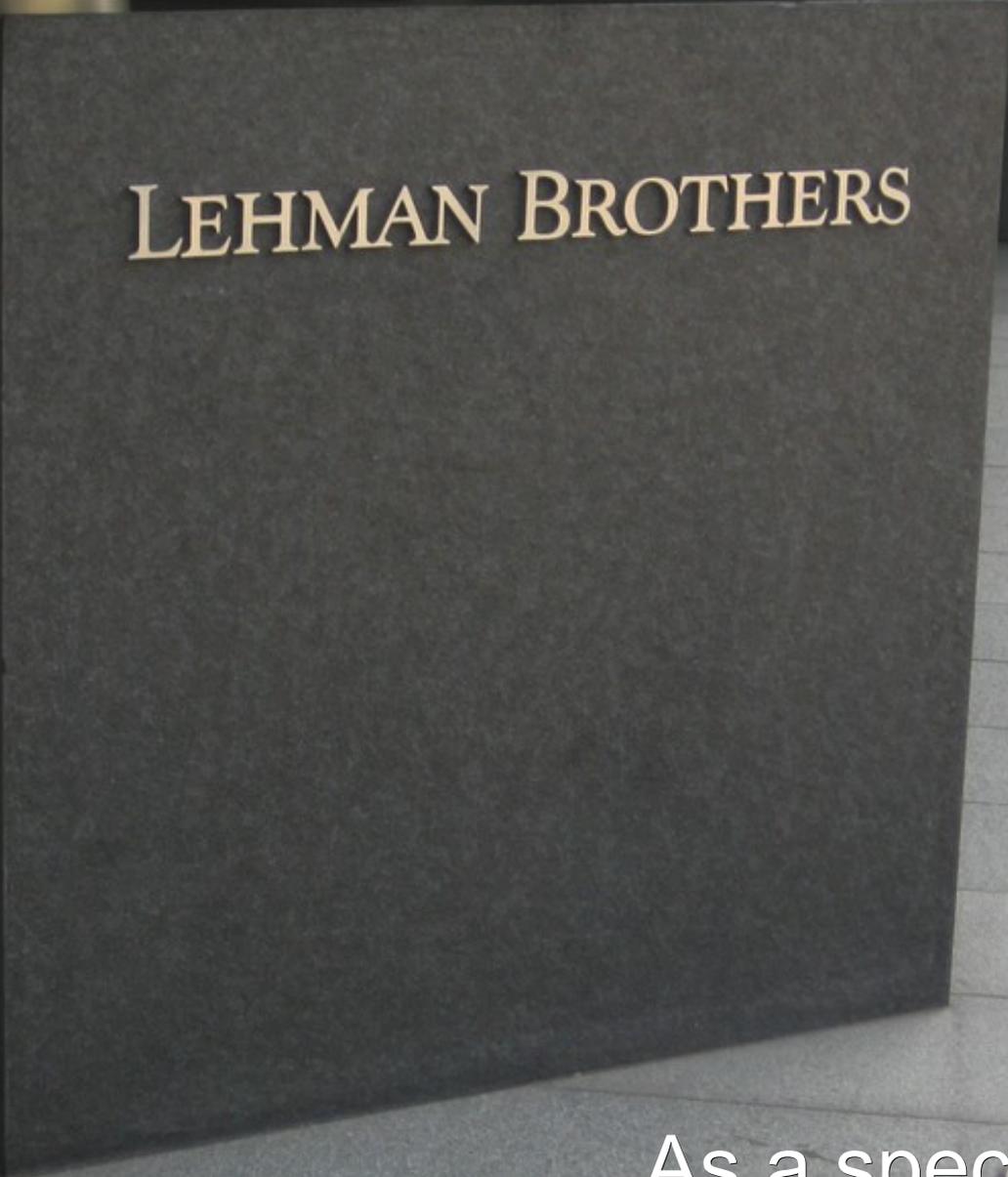
It's something intrinsic to  
how we see and respond to the world



“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



Is our understanding  
of risk hardwired?

A large, dark grey rectangular sign with the words "LEHMAN BROTHERS" in gold, serif, all-caps lettering. The sign is positioned on a light-colored, tiled sidewalk. In the background, there are several large, cylindrical columns and a planter with red flowers. Two people are walking away from the camera on the sidewalk to the right.

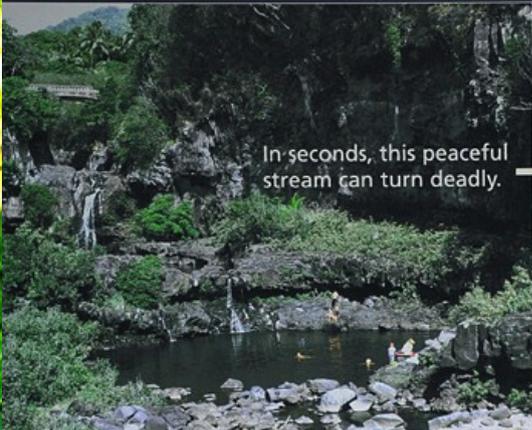
LEHMAN BROTHERS

As a species we're bad at  
processing abstract risk



# WARNING

## ALL NATURAL AREAS POSE RISKS



In seconds, this peaceful stream can turn deadly.



**Man, child swept over fall**

Few aware of stream's flash flood danger

### Flash Flooding

A flash flood that originates high in the mountains can cause the water level to rise suddenly, sweeping away everything in its path. Steep cliffs around pools may make escape impossible.

### Signs of a Flash Flood

- Dark skies over the mountains
- Rising water level
- Sounds of rising water and tumbling rocks

### Underwater Hazards



Jumping or diving into pools can be very dangerous. Sharp rocks, trees, and other submerged hazards are hidden in the pools. Water levels can change on a daily or even hourly basis, making it difficult to judge depth.

### Slippery Surfaces



Rocks are very slippery when wet. Rockfalls and landslides can occur anytime and without warning.

**By entering a stream, you are taking a risk. Your safety is your responsibility.**

# 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?”



Ok, so what's the problem again?



Few of us can  
have good risk  
conversations



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

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  $R = I \times L$

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

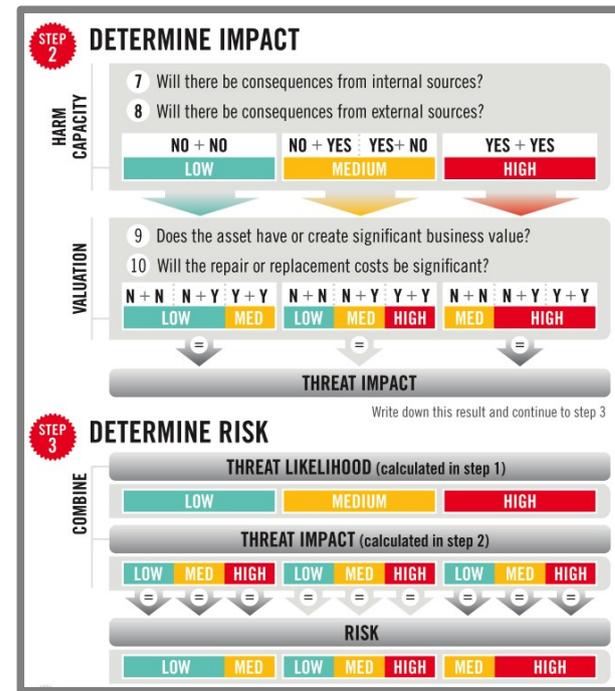
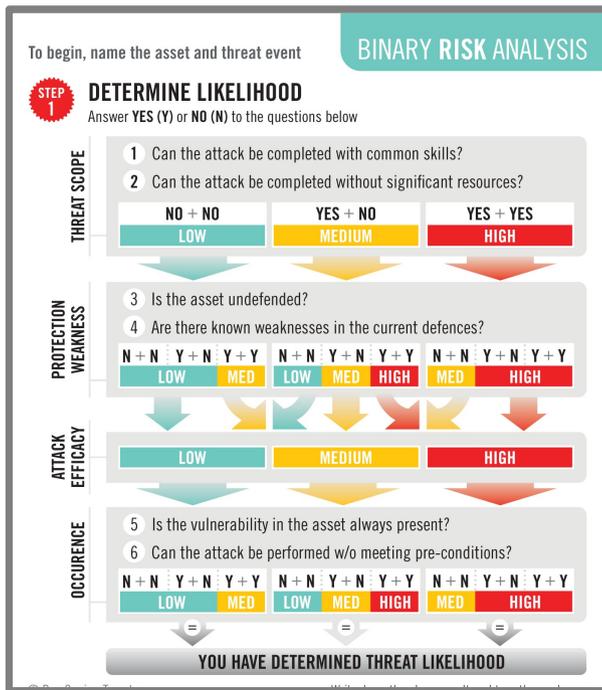
Quick to learn

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?



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

00000000 1 1

## Question 0011

Is the asset undefended?

NO

0000000011

## Question 0100

Are there known weaknesses in the current defences?

YES

0000001011

## Question 0101

Is the vulnerability in the asset always present?

YES

0000011011

## Question 0110

Can the attack be performed without meeting pre-conditions?

NO

0000011011

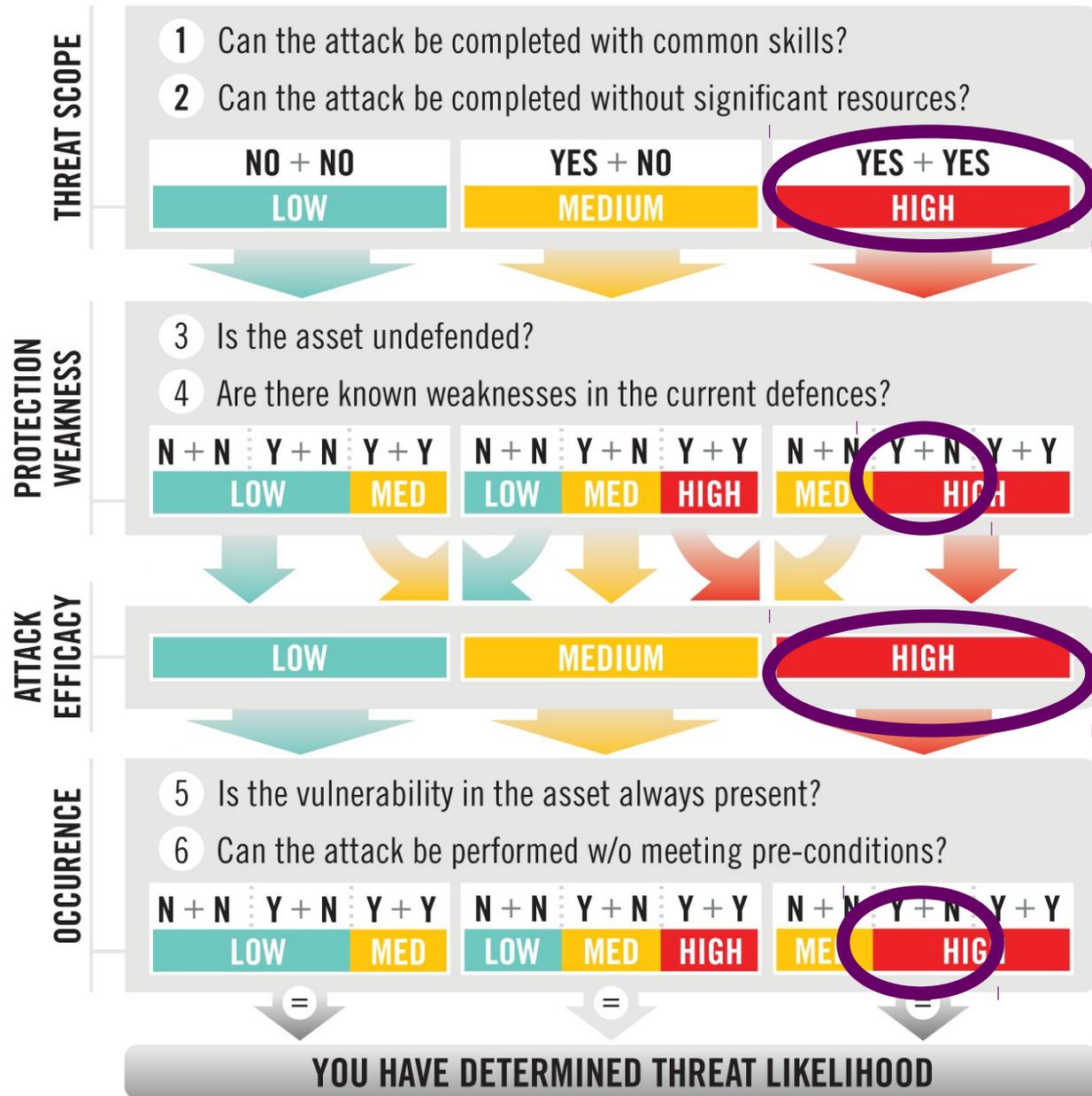
# BINARY RISK ANALYSIS

To begin, name the asset and threat event

**STEP 1**

## DETERMINE LIKELIHOOD

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



## Question 0111

Will there be **consequences** from internal sources?

YES

0001011011

## Question 1000

Will there be **consequences** from external sources?

YES

0011011011

## 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

1111011011

**STEP 2**

# DETERMINE IMPACT

HARM CAPACITY

- 7 Will there be consequences from internal sources?
- 8 Will there be consequences from external sources?

NO + NO	NO + YES	YES + NO	YES + YES
LOW	MEDIUM		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	N + N	N + Y	Y + Y	N + N	N + Y	Y + Y
LOW	MED		LOW	MED	HIGH	MED		HIGH



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	MED	HIGH
-----	-----	------	-----	-----	------	-----	-----	------

**RISK**

LOW	MED	LOW	MED	HIGH	MED	HIGH
-----	-----	-----	-----	------	-----	------

infosec pro

1111011011 =

High

stakeholder

0001010010 =

Low

consequences from external sources  
has or creates significant business value  
repair or replacement costs are significant  
known weaknesses  
common skills

The correct conversation with the business

# Step 1 - Determine Likelihood 🕒 0:00:00

**A Threat Scope Matrix**

0 Is skill required? Yes No

1 Does the attack require significant resources? Yes No

S	M
M	L

**C Attack Effectiveness Matrix**

	S	M	L
C	L	L	O
P	L	O	C
I	O	C	C

**B Protection Capability Matrix**

2 Can the defense fail? No Yes

3 Does the defense cover all access points to the asset? Yes No

C	P
P	I

**E Threat Likelihood Matrix**

	L	O	C
R	LL	LL	ML
P	LL	ML	HL
A	ML	HL	HL

**D Occurrence Matrix**

4 Are there any pre-conditions for the attack? Yes No

5 Is the vulnerability always present? No Yes

R	P
P	A

Proceed to step 2 on the of reverse side

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

<b>THREAT SCOPE</b>	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		
<b>PROTECTION WEAKNESS</b>	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	HIGH	MED	HIGH
<b>ATTACK EFFICACY</b>	LOW	MEDIUM	HIGH		
<b>OCCURENCE</b>	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	HIGH	MED	HIGH
=      =      =					
<b>YOU HAVE DETERMINED THREAT LIKELIHOOD</b>					

# The back story

Question 1

Yes	Med	High
No	Low	Med
	No	Yes

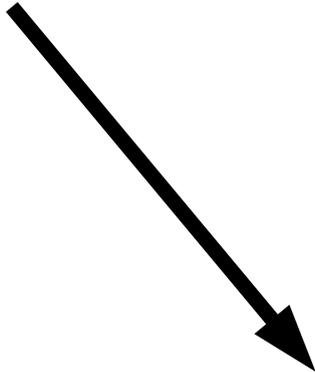
Question 2

Med	High	Yes
Low	Med	No
No	Yes	

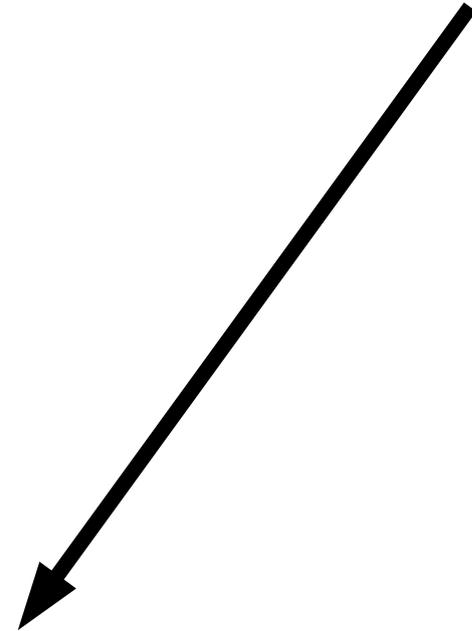
Question 3

Question 4

Pair A

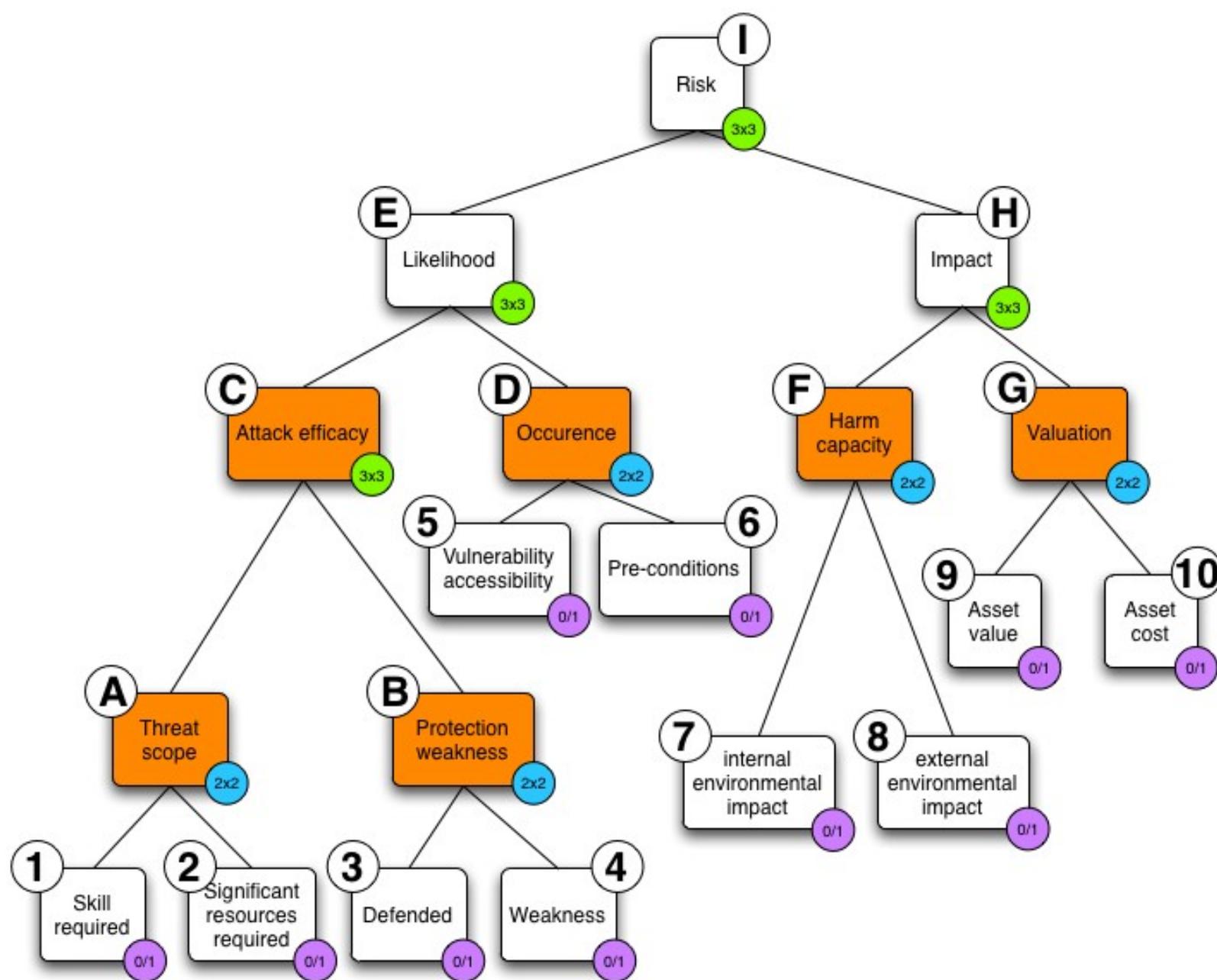


Pair B



High	Med	High	High
Med	Low	Med	High
Low	Low	Low	Med
	Low	Med	High

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

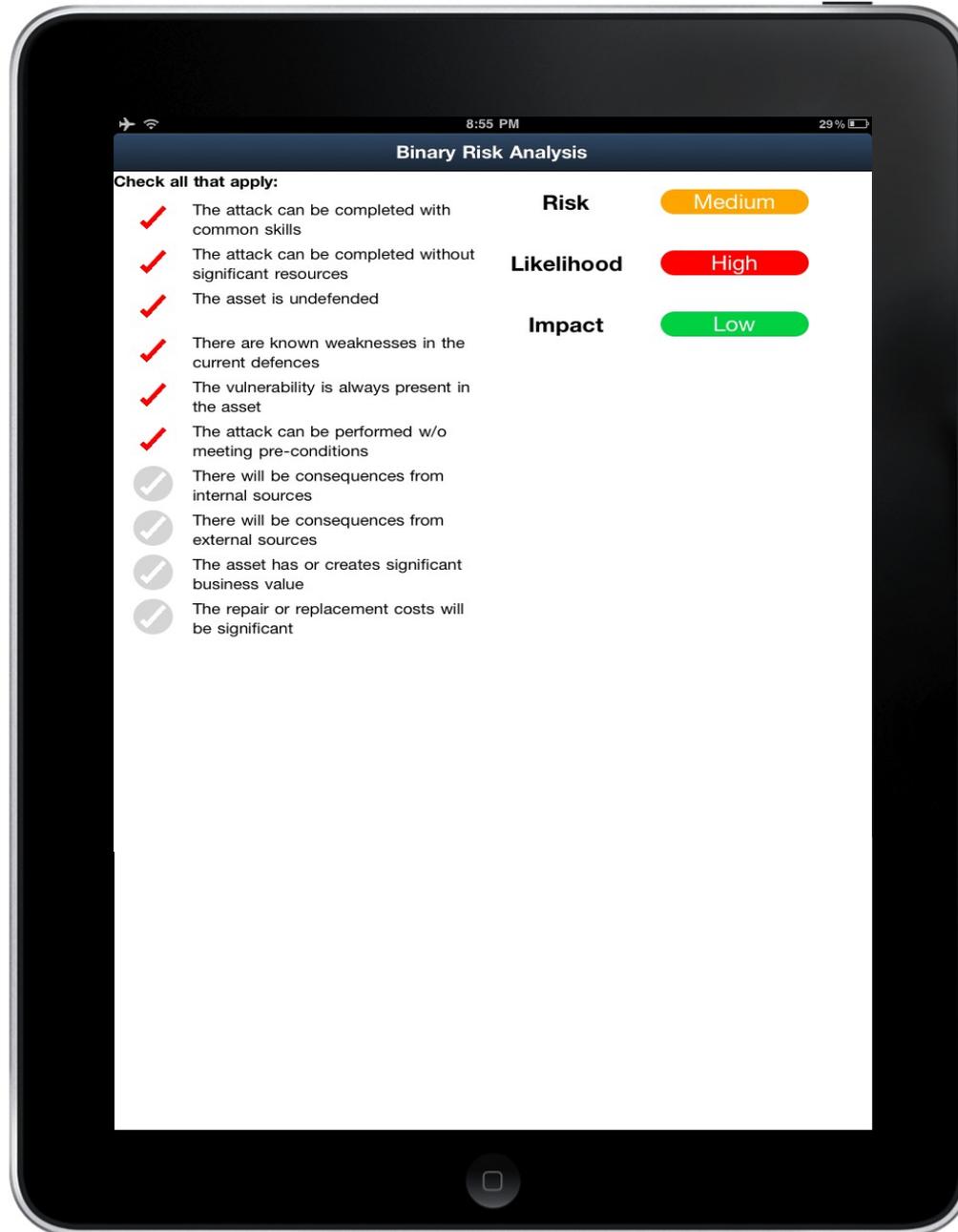
(Send me feedback)

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)