Binary Risk Analysis

License

License Summary

Copyright Holder

Ben Sapiro, Toronto - ben@sapiro.net

Getting started

Here's a three step process to using the Binary Risk Analysis tool:

1. Print out the Work Card, preferably in colour and double sided
2. Spend ten minutes and run a practice analysis
3. Use it during your next conversation about risk

Optional step: if you want, read this document, but it is not a requirement that you do so. In fact, doing so will take away time that you could have been using the tool.

Bonus points: Once you've printed the Work Card, get it laminated so you can keep using it without having to reprint it. Not only does it save trees, but it makes it clear this is the tool and there are no other parts to it.

Acknowledgements

A tool like this would not be possible without the existence of other methodologies or the hard work of their creators. In developing this tool, multiple methodologies were examined, some providing inspiration and others guidance on the treatment of various topics. The methodologies include, but are not limited to:

- OCTAVE
- SOMAP
- FAIR
- NIST SP800-30
- OSSTMM
- FRAP
- CICRAM

If this tool serves to advance risk management practices then it is because of them, if it fails to advance risk management practices, then it is not because of them.

Table of Contents

Overview

Binary Risk Analysis is a lightweight qualitative risk assessment tool that is openly licensed. The tool is easy to use, enables quick structured conversations about risk and works with existing risk management frameworks.

While the tool was developed for use in the IT security arena, it can be used in other risk domains (risk is, after all, risk) with some trivial adjustments to the language.

This document provides context on the tool but is not essential for its use, in fact, anyone can use the tool successfully without ever reading this document.

Design objectives

The design objectives were to provide a tool that satisfies the following requirements:

- presents a decomposed view of risk
- does not ask anyone to guess on event frequency in the absence of statistical data
- can be printed on a single piece of paper
- does not require a computer to complete
- is fast (can be completed in under five minutes)
- can be handed out to anyone with relatively little explanation
- is freely distributable and modifiable
- does not require a training course
- does not require much in the way of supporting documentation
- can serve as input into existing frameworks and methodologies

Rationale

Why build yet another tool for risk analysis? Binary Risk Analysis was created to:

- **Make structured risk discussions easier and more common** - people are more likely to do something if it takes less effort (either in training or during the actual task); simple works for most people and most situations.
- **Provide a stepping stone to more robust methodologies** - get organizations to start on the path to proper risk analysis and risk management. Starting small is more likely to have long term positive outcomes.

In a nutshell, everything about the tool is for the purposes of removing objections to improving the understanding of our risks. It's easy to object to a complicated methodology on the grounds it takes too long or that the risk is, in someone's opinion, subjectively obvious so why bother with analysis. Big methods will overwhelm people and are more likely to result in failure.

Providing the tool with an open license means there are no barriers of any sort to its use and broad adoption.

Uses

Binary Risk Analysis is good for:

- **Quick risk conversations** - be able to discuss a specific risk in just a few minutes
- **Highlighting subjectivity** - helping identify where perceptions about risk elements differ

Binary Risk Analysis is not:

- **A full risk management methodology** - you will still need a process to catalogue and monitor risks
- **A quantitative analysis** - if you need hard statistics, monetary values or want to eliminate subjectivity completely from the analysis, look to the larger and more complex methodologies
- **A threat discovery technique** - if you need to discover threats to your assets, look to threat modelling or threat risk assessment techniques

The Tool

Common terms

There are many texts that do a complete job of defining and explaining ris. For the purposes of the tool, risk is defined:

> *A composite qualitative measurement on the likelihood of a bad event occurring to an asset and how much damage it will cause to the asset and its owner.*

More simply put, risk is the answer to the question “how much should I worry about this?”.

There are other terms used by this tool such as threat, threat agent, vulnerability and attacker, their use is consistent with industry norms and for the purposes of brevity will not be defined in this document.

Binary risk

The central tenant to this tool is that risk analysis is based exclusively on yes or no responses to ten questions, a binary response. By forcing the tool user to choose one of two mutually exclusive answers the tool ensures speed and simplicity in its approach.

Using the tool

The tool is provided to you in the form of a work card, designed to be printed out and used (although you could do this on the back of a napkin if needed, the work card is just a convenience).

Once you’ve determine the asset and the threat it must be protected from, you can use tool by following these steps:

1. Answer the ten questions
2. Map the answers to each of the 2x2 matrices
3. Use the results from the 2x2 matrices to select results from the 3x3 matrices. The final 3x3 matrix will compute the risk

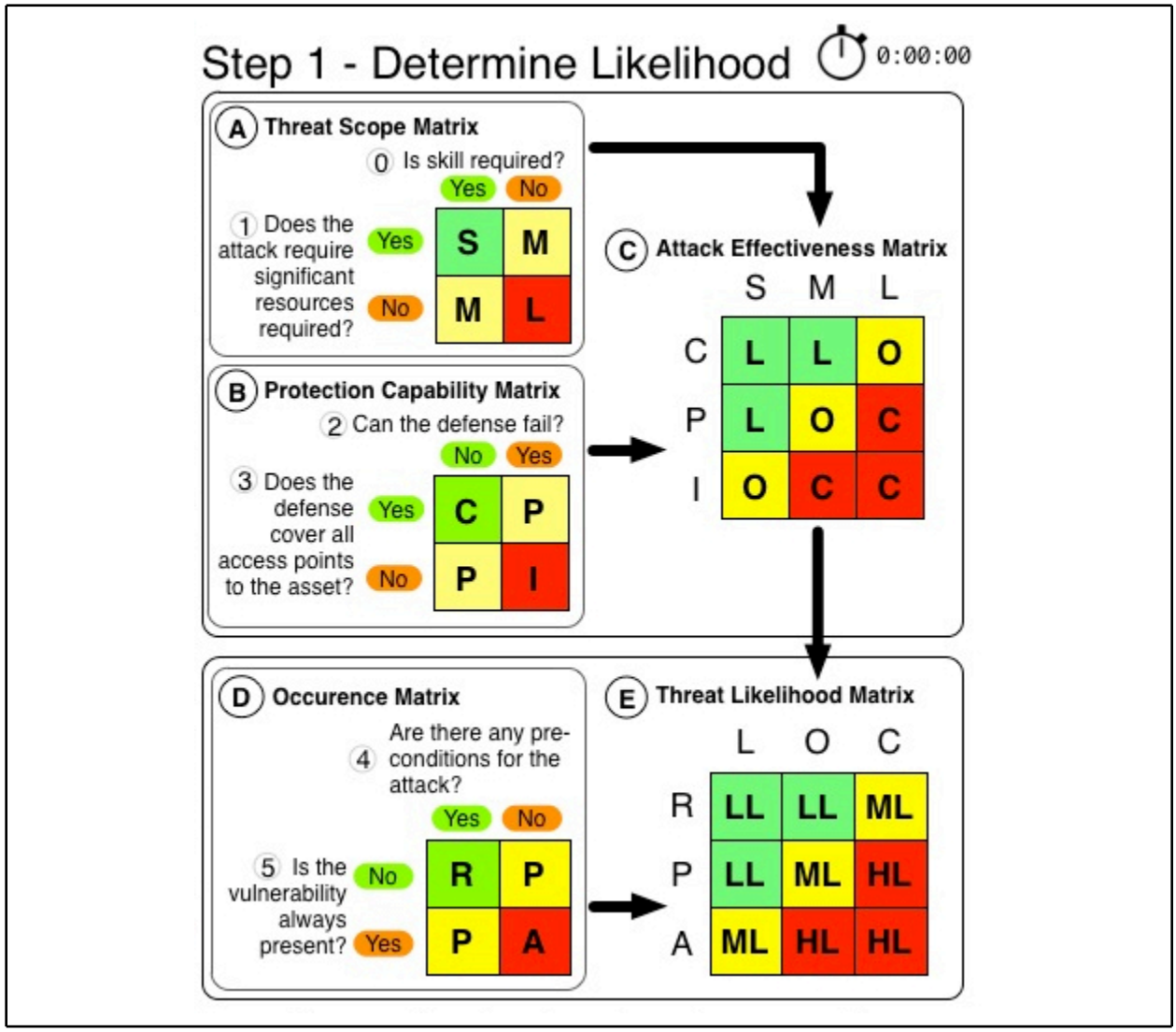
While you answer the questions in any order you want, it’s faster to answer them in pairs and then map the results to the relevant matrix.

The Work Card

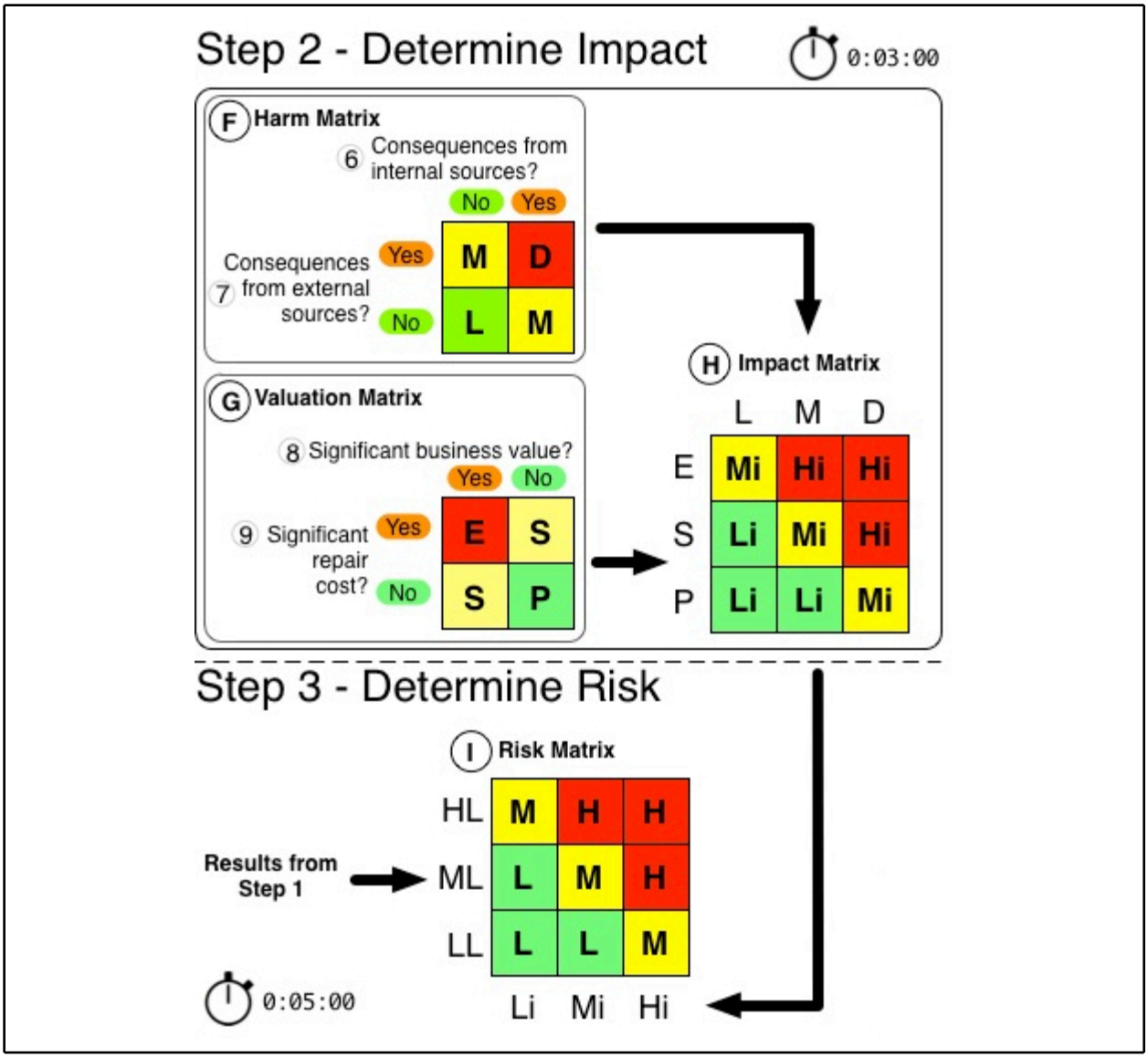
Images of the work card (front and back) are provided below but a fully printable version of the work card is available along with this document. The images below are just the working part of the tool; instructions and guidance are included with the work card in a condensed format.

A suggestion: It is strongly recommended that you print out a copy of the work card and use it as an aid while reading the rest of document.

Front side



Back side


Step 2 - Determine Impact
0:03:00
F Harm Matrix
6 Consequences from internal sources?
No
Yes
Consequences from external sources? 7
Yes
No
M
D
L
M
G Valuation Matrix
8 Significant business value?
Yes
No
9 Significant repair cost?
Yes
No
E
S
S
P
H Impact Matrix
L M D
E Mi Hi Hi
S Li Mi Hi
P Li Li Mi
Step 3 - Determine Risk
I Risk Matrix
Results from Step 1
HL M H H
ML L M H
LL L L M
Li Mi Hi
0:05:00

The 1010 (ten) questions

Each question must be answered with a yes or no; in cases where it is not possible to answer to the question (for example no defenses exist), choose the answer that is the worse outcome.

Question 0

Are unique skills required to complete the attack successfully?

Question 1

Are significant resources required to complete the attack successfully?

Question 2

Is it possible that the defense fails to protect against the attack?

Question 3

Does the defense cover all access points to the asset?

Question 4

Is the vulnerability always present in the asset?

Question 5

Are there significant prerequisites to completing the attack successfully?

Question 6

Is there a significant cost to repair or replace this asset?

Question 7

Does the asset have significant value to the asset owner?

Question 8

Will there be consequences to the attack from internal sources?

Question 9

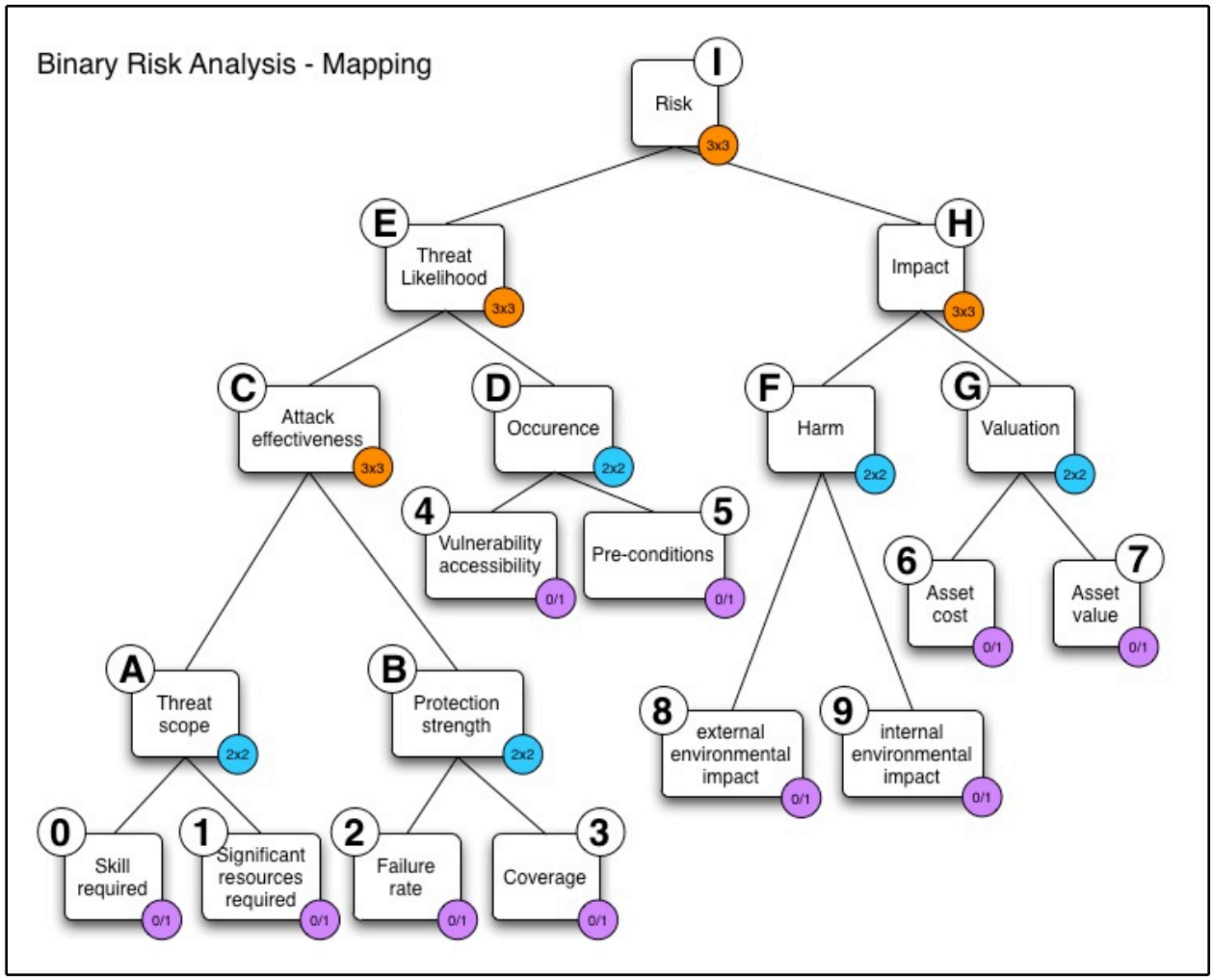
Will there be consequences to the attack from external sources?

Structure

The relationship between ten questions is shown below in a tree diagram. The diagram maps the ten questions to nine matrices (two-by-two and three-by-three). The diagram is annotated with icons that read as follows:

- 0/1 is question (there are ten of them)
- 2x2 is a two-by-two matrix (there are five of them)
- 3x3 is a three-by-three matrix (there are four of them)

Additionally the questions are numbered (0 through 9) and the matrices are labelled (A-I). You can answer the question in any order but the matrices must be processed in order.



The Matrices

There are nine matrices on the work card. Each matrix helps compute a part of the risk. The quadrants in each matrix are coloured with green, yellow and red:

- Green indicates a result that will contribute to a lower overall risk
- Yellow indicates a result that will contribute to a moderate overall risk
- Red indicate a result that will contribute to a higher overall risk

Each quadrant is marked by one of three letter symbol, the ordered set of which (such as {S,M,L} in the threat scope matrix or {P,S,E} in the valuation matrix) is unique to that matrix. Each of the letter symbols is the short form identifier for a risk quality.

(A) Threat Scope Matrix

Threat scope is the size of the pool of potential attackers (threat agents). The more attackers, the more likely it is the threat will occur.

The 2x2 matrix can return one of the following results based on questions 0 and 1 as input:

- (S) small
- (M) medium
- (L) large

(B) Protection Capability Matrix

Protection strength is the effectiveness of the defense against the threat. The better the defenses the less likely it is the attacker will succeed.

The 2x2 matrix can return one of the following results based on questions 2 and 3 as input:

- (C) complete
- (P) partial
- (I) incomplete

(C) Attack Effectiveness Matrix

Attack effectiveness is the likelihood that the attack will be effective. This is a composite measure that indicates the threat is more likely to occur if the defenses are weak and there is a larger pool of potential attackers.

The 3x3 matrix can return one of the following results based on matrices A and B as input:

- (L) limited basis
- (O) occasionally
- (C) consistently

(D) Occurrence Matrix

Occurrence is the frequency the threat agent can attempt an attack. If the vulnerability is always reachable and there are not prerequisites that must be fulfilled to gain access, the easier it is for the attacker to can access to the vulnerable asset.

The 2x2 matrix can return one of the following results based on questions 4 and 5 as input:

- (R) rarely
- (P) periodically
- (A) always

(E) Threat Likelihood Matrix

Threat likelihood is the probability of a successful attack occurring. This is the derived outcome of the following matrices:

- Threat Scope
- Protection Capability
- Attack Effectiveness
- Occurrence

The 3x3 matrix can return one of the following results based on matrices C and D as input:

- (LL) low
- (ML) moderate
- (HL) high

(F) Harm Matrix

Harm is the damage an attack will cause to the asset owner. Harm (or consequences) come from internal and external sources. If there are harm sources both inside and outside the organization, the resultant impact of successful attack it likely to be higher.

The 2x2 matrix can return one of the following results based on questions 6 and 7 as input:

- (L) limited
- (M) material
- (D) damaging

(G) Valuation Matrix

Valuation measures the importance of the asset to the owner. The asset owner will experience higher impact if the asset delivers higher value to the owner or costs more to repair in the event of a successful attack.

The 2x2 matrix can return one of the following results based on questions 8 and 9 as input:

- (P) peripheral
- (S) supporting
- (E) essential

(H) Impact Matrix

Impact is the damage of a successful attack to the asset and the asset owner. This matrix is the derived outcome of the of the following matrices:

- Harm
- Valuation

The 3x3 matrix can return one of the following results based on matrices F and G as input:

- (Li) low
- (Mi) moderate
- (Hi) high

(I) Risk Matrix

Risk is the probability the threat event is likely to happen and the degree of harm it will cause. This matrix is the outcome of the following matrices:

- Threat Likelihood
- Impact

The 3x3 matrix can return one of the following results based on matrices E and H as input:

- (L) low
- (M) moderate
- (H) high

Determining risk

Once you've answered the ten questions, use the work card to map the answers to the associated 2x2 matrices and follow the arrows to continue mapping the results to the larger 3x3 matrices. The last 3x3 matrix you complete provides the risk estimate.

A note on subjectivity

The tool is not designed to eliminate subjectivity, that's not possible given the requirements for speed and near-zero training. However, the tool is designed to highlight and decompose subjectivity. You may not agree on a particular risk rating, but at least you will quickly know why.

A note on risk management

To reduce the identified risk, users should propose corrective measures that shift the 2x2 matrices to lower risk contribution states (turn red to yellow or yellow to green).

An Example

Let's analyse the risk of an attacker stealing an unencrypted USB key containing sensitive business data from your desk drawer:

Question number	Question	Answer	Rationale
0	Are unique skills required to complete the attack successfully?	No	Opening a desk drawer is easy and so is walking into an office.
1	Are significant resources required to complete the attack successfully?	No	No, at most a suit and good haircut.
2	Is it possible that the defense fails to protect against the attack?	Yes	There's no defense implemented to protect against this.
3	Does the defense cover all access points to the asset?	No	There's no defense implemented to protect against this.
4	Is the vulnerability always present in the asset?	Yes	Yes, you can always steal something small and unguarded.
5	Are there significant prerequisites to completing the attack successfully?	Yes	You need to gain access to the office.
6	Is there a significant cost to repair or replace this asset?	Yes	The data contains information about new products; it would require significant engineering effort to replace with newer or better designs if competitors were provided a copy of the data.
7	Does the asset have significant value to the asset owner?	Yes	Yes, it's sensitive company data.
8	Will there be consequences to the attack from internal sources?	Yes	The company will need to explain to the board.
9	Will there be consequences to the attack from external sources?	Yes	The company will need to disclose the data theft

			to regulators.

Let's map the answers to the 2x2 matrices:

Matrix reference	**Inputs**	**Matrix name**	**Result**
A	(0) No (1) No	Threat Scope	(L) Large
B	(2) Yes (3) No	Protection Capability	(B) Incomplete
D	(4) Yes (5) Yes	Occurrence	(P) Periodically
F	(6) Yes (7) Yes	Harm	(D) Damaging
G	(8) Yes (9) Yes	Valuation	(E) Essential

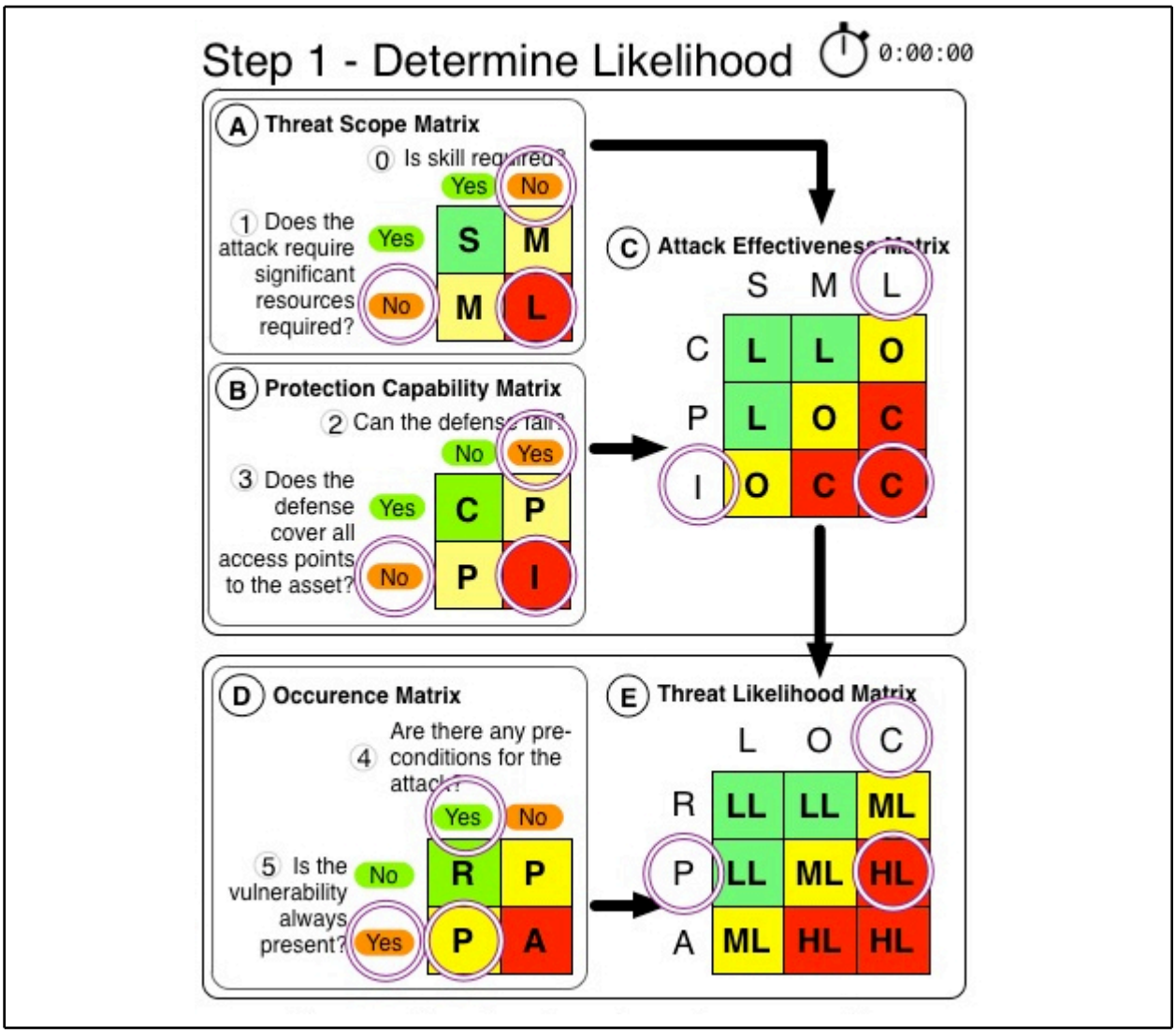
Let's map the answers to the 3x3 matrices:

Matrix reference	**Inputs**	**Matrix name**	**Result**
C	(A) L (B) I	Attack Effectiveness	(C) Consistently
E	(C) C (D) P	Threat Likelihood	(HL) High Likelihood
H	(F) D (G) E	Impact	(Hi) High Impact
I	(E) HL (H) Hi	Risk	(H) High

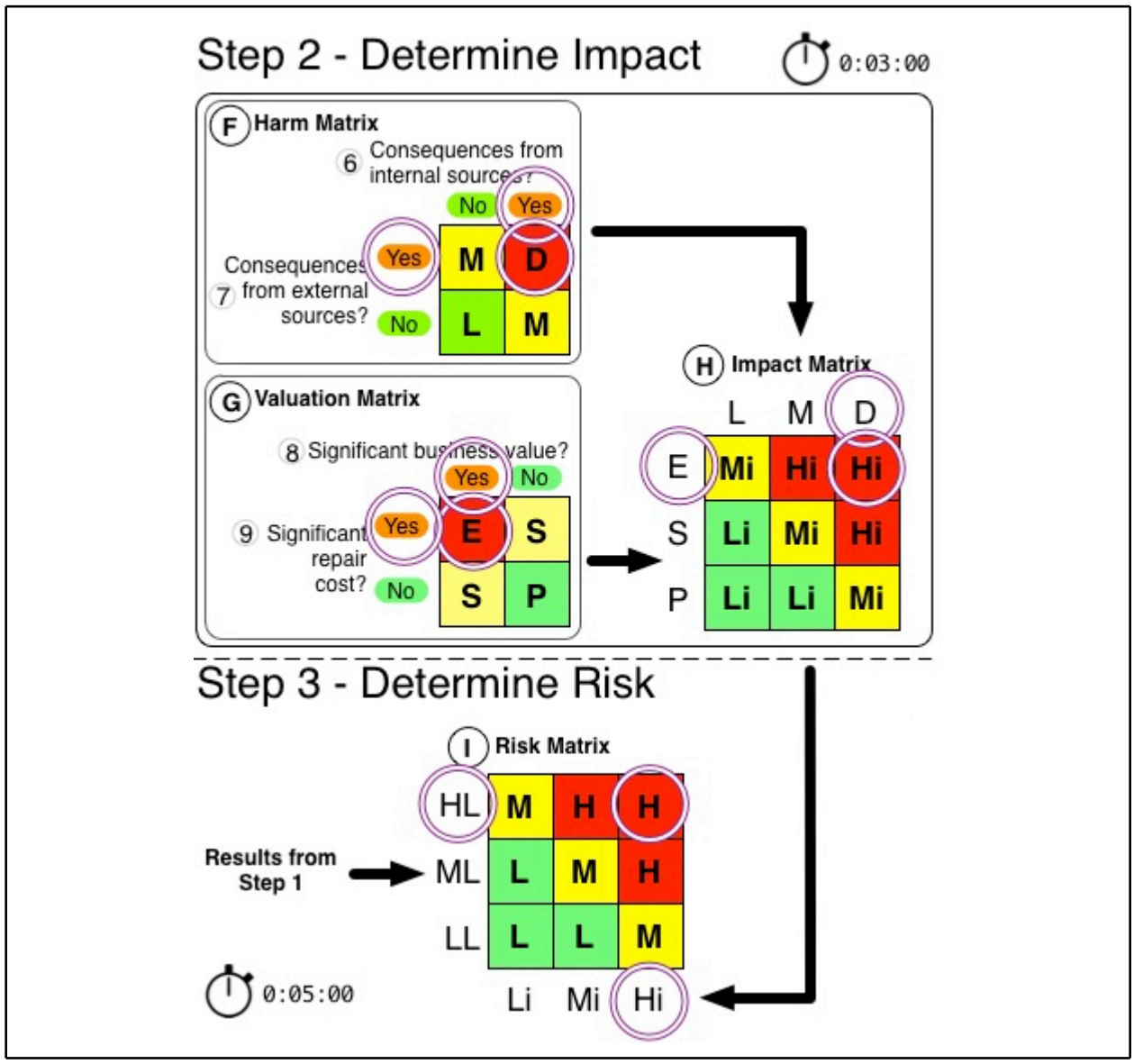
The risk for this threat has been assessed as high.

A completed work card is provided as well. The answers to questions and results from the matrices are highlighted by a purple double edged ring.

Here is the front of complete work card:



Here is the back of the completed work card:



You have probably noticed that some of the answers are subjective (in part because of context). When you run this example, you might get a different answer but at least you can quickly highlight where and why your answers are different from the example.

Version History

Version	Date	Released By
1.0	May 29, 2011	Ben Sapiro