Flip over for instructions and an example

AN OVERVIEW

Binary Risk Analysis is a lightweight risk tool designed to help information security professionals and business people quickly come to agreement on the severity of an identified risk. This first release focuses on attack based risk.

Binary Risk Analysis asks the user to answer exactly 10 questions and from that risk is derived. Users can complete a single risk assessment in under five minutes but with far more clarity (and meaning) than the classic approaches used today.

While the tool (and its supporting methodology) still produces the classical outputs of likelihood and impact (making it compatible with existing practices) the structured approach allows parties debating risk to quickly identify differing perceptions of risk inputs (and thereby eliminate implicit assumptions).

The methodology and tool is freely licensed for commercial use under the Creative Commons Attribution-ShareAlike license (version 3.0).

If you find this document without the work card attached, you can download a copy of this work card, supporting methodology documentation and a community app at **https://binary.protect.io.**

?

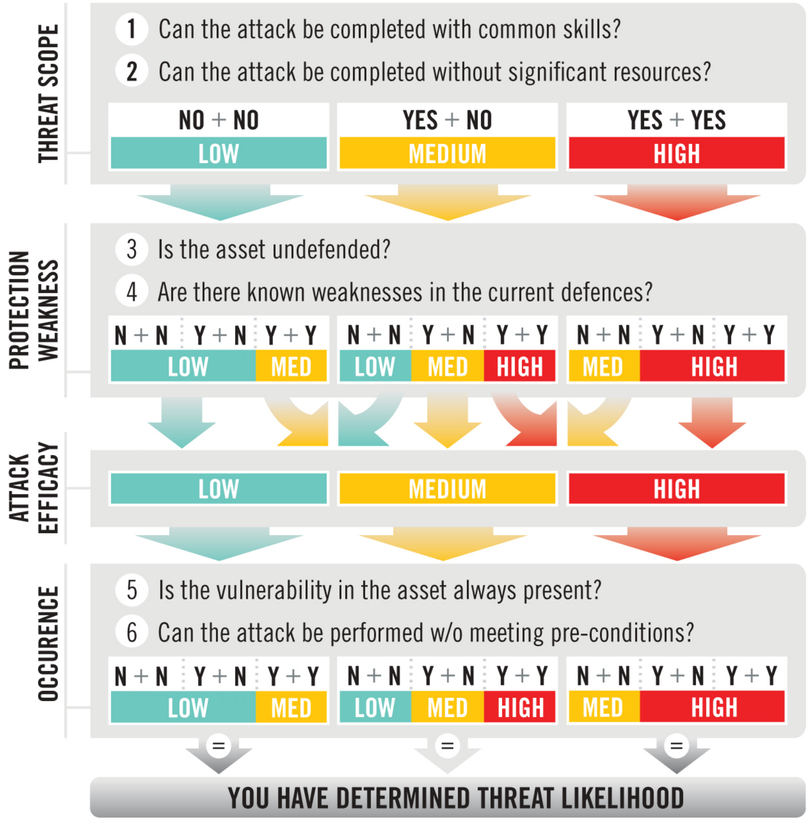
Get the CC licensed methodology and copies of this work card at **https://binary.protect.io**

To begin, name the asset and threat event

BINARY **RISK** ANALYSIS

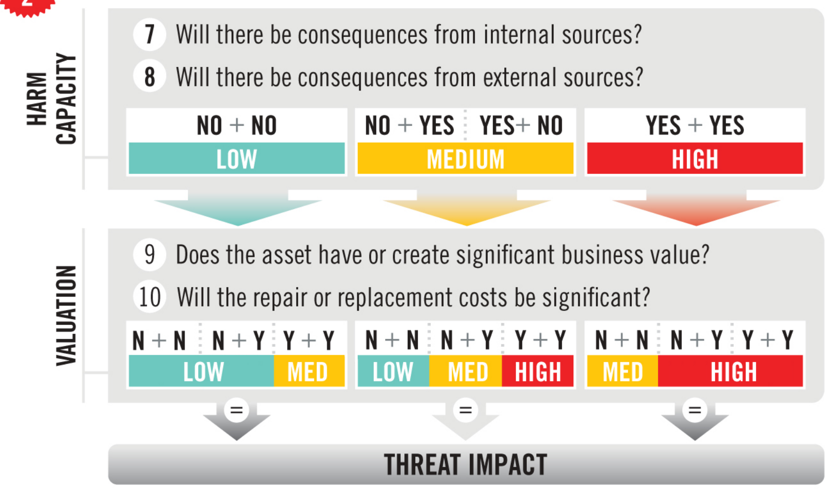
STEP 1 DETERMINE LIKELIHOOD

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
LOW
YES + NO
MEDIUM
YES + YES
HIGH
PROTECTION WEAKNESS
3 Is the asset undefended?
4 Are there known weaknesses in the current defences?
N + N
Y + N
Y + Y
LOW
MED
N + N
Y + N
Y + Y
LOW
MED
HIGH
N + N
Y + N
Y + Y
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
LOW
MED
N + N
Y + N
Y + Y
LOW
MED
HIGH
N + N
Y + N
Y + Y
MED
HIGH
=
=
=
YOU HAVE DETERMINED THREAT LIKELIHOOD

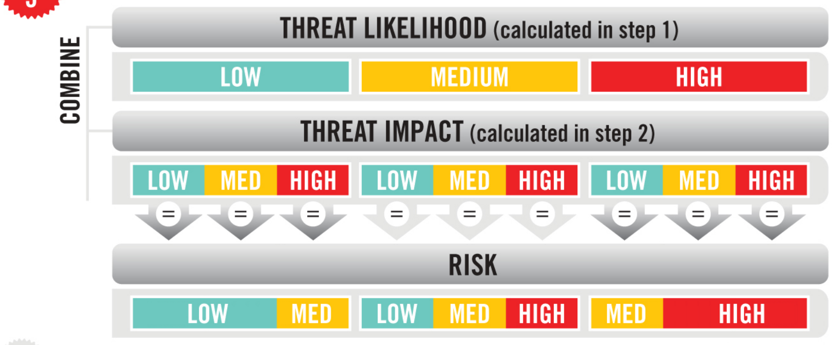
Write down the above result and turn the card over

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



SAVE A TREE Get the app at **https://binary.protect.io**

BINARY **RISK** ANALYSIS

INSTRUCTIONS

A Identify the asset to subject the risk analysis to

B Identify the threat event the asset will be subject to

C Answer the ten questions (there are six on this side of the work card and four on the other side) with a **YES** or **NO**

D For every pair of questions you answer, you will determine a component of the risk analysis by mapping it to the columns below

E Once you complete *step 1* (this side of the work card) you'll know the likelihood of the threat event occurring

F Next complete *step 2* (the other side of the work card) and you will know the impact of the threat event should it occur

G Finally, *step 3* (also on the other side) will determine the risk of the threat event

A BRIEF EXAMPLE

You answer **YES** to question 1, **YES** to the second question - so you get a **HIGH** in the first row (Threat Scope). You answer **YES** to the third question and **NO** to the forth - you get a **MEDIUM** in the second row (Protection Weakness). Which means the third row (Attack Efficacy) rates as a **MEDIUM**. **NO** to the fifth and sixth questions means that Threat Likelihood is **LOW**.

In Step 2, you answer **YES** to questions 7 and 8 making the harm capacity **HIGH**. Question 9 is **YES** and question 10 is **NO** so Threat Impact is calculated as **HIGH** .With a Threat Likelihood of **LOW** (calculated in step #1) and a Threat Impact of **HIGH** (calculated in step #2), we calculate Risk as **MEDIUM**.