Zero Day Risks and Probabilistic Risk Prioritization

Dr. Hale

University of Nebraska at Omaha

Information Security and Policy– Lecture 3

Today's topics:

Last time recap

Homework Discussion

Zero Day Risk Prioritization

- Definition
- Examples
- What to do

Risk Prioritization Probability Theory

- Decision Trees: Strategic thinking
- Risk Attitude Preference & Risk Premiums
- Decision Rules
- Utility Theory & Multiple Attribute Optimization
- Examples

(My dog in a top hat)

Say what?

It will be ok, we will break it all down.

Previously…on IA 3600…

$$ATLE_{threat} = L_{rate} \times L_{cost}$$

$$SLE_{threat,\ asset} = \text{Asset Value (AV)} \times \text{Percentage Lost (PL)}$$

$$ETI_{threat} = \sum_{i=1}^{n} SLE_{threat,i}$$

$$ATLE_{threat} = L_{rate} \times ETI_{threat}$$

Recap

Full Example Summary

Threats:

$ETI_{theft} = SLE_{theft,\ device} + SLE_{theft,\ companydata}$

$= \$1000 + \$10{,}000 = \$11{,}000$

(occurs 10 times a year) => $ATLE_{theft} = 10 \times \$11{,}000 = \$110{,}000$/year

$ETI_{dos} = SLE_{dos,\ pos}$

$= \$5000$

(occurs 20 times a year) => $ATLE_{dos} = 20 \times \$5{,}000 = \$100{,}000$/year

$ETI_{hacks} = SLE_{hacks,\ webservers} + SLE_{hacks,\ workstations} + SLE_{hacks,\ reputation}$

$= \$50000 + \$1000 + \$100{,}000 = \$151{,}000$

(occurs once every 5 years [.2 times/year]) => $ATLE_{hacks} = .2 \times \$151{,}000 = \$30{,}200$/year

$ETI_{phishing} = SLE_{phishing,\ personneldata} + SLE_{phishing,\ workstations}$

$= \$500 + \$100 = \$600$

(occurs 100 times a year) => $ATLE_{phishing} = 100 \times \$600 = \$60{,}000$/year

Recap

Full Example (Decision time)
Allocate $10,000 to Info. Sec.

Option 1: Encrypt laptops

(reduces $SLE_{theft, companydata}$ to 0) => $ATLE_{theft}$ reduced by $100,000

Option 2: Buy a firewall

(reduces rate of hack success by 50% and dos by 50%[e.g. ddos still works])
=> DoS L_{rate} drops to 10 (from 20) and $ATLE_{dos}$ reduced by $50,000
=> hack L_{rate} drops to .1 (from .2) and $ATLE_{hacks}$ reduced by $15100
for a total of $65,100

Option 3: Train staff against phishing

(reduces rate of phishing attack success by 40%)
=> reduces Phishing L_{rate} to 60 (from 100) and $ATLE_{phishing}$ reduced by $24000

~~Homework Discussion Time~~

(next time)

What do we do about threats we don't know about?

“There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.”

– Donald Rumsfeld, on Iraq Evidence

"There are also unknown knowns. These are things we don't know that we know"

– Me (for completion sake)

Zero Days are unknown unknowns or known unknowns

And/or this quote is silly

Definition

Zero Day threats are previously un-encountered events that threaten an organization in potentially unknown ways.

Despite sounding like the title of the next Micheal Bay film, zero-days account for billions of dollars of lost revenue yearly.

Famous Examples

Feb. 2013 Acrobat Reader 10 and 11 sandbox bypass

allowed malicious entity to operate arbitrary code

April 2014 Heartbleed

OpenSSL exploitation for buffer over-read (allowed theft of private keys and session tokens on about17% of the worlds webservers)

The 2014-2015 Sony Hack

Apache Struts 2017

Apache Struts 2 Aug 23, 2018

There is a BIG market for selling zero-day vulnerabilities.

The average exploit sells for 35-160k. MS, Apple, NSA, and foreign governments are main clientele.

see

http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

What can you do to combat them?

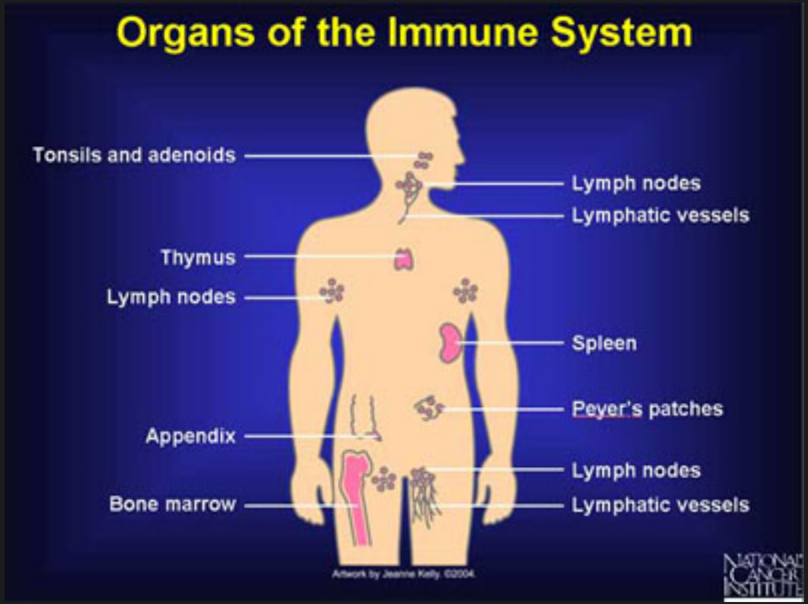
Zero days are a type of *residual risk* that can’t be eliminated.

What can you do to combat them?

Best bet: Follow best practices, defense-in-depth, monitor your assets, and look to past exploits for insight.

What can you do to combat them?

Analogy: Immune System Architecture



Defense in depth

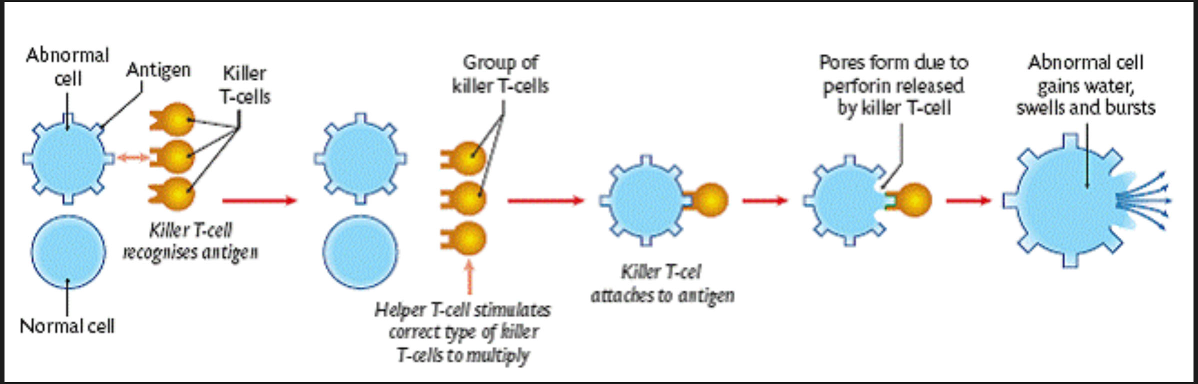
What can you do to combat them?

Analogy: Immune System

Monitoring & Audit

Incident Response Plans

Mitigation & Assessment for next time



Zero Day Risk

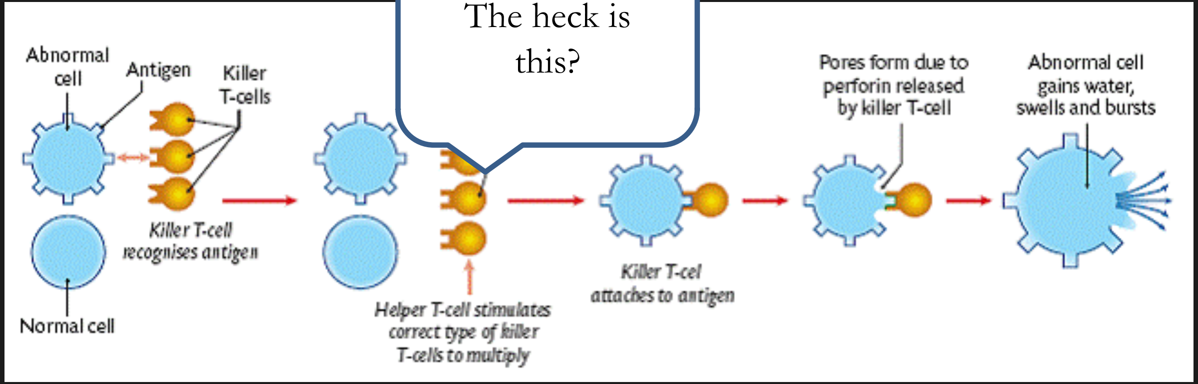
What can you do to combat them?

Analogy: Immune System

Monitoring & Audit

Incident Response Plans

Mitigation & Assessment for next time



The heck is this?

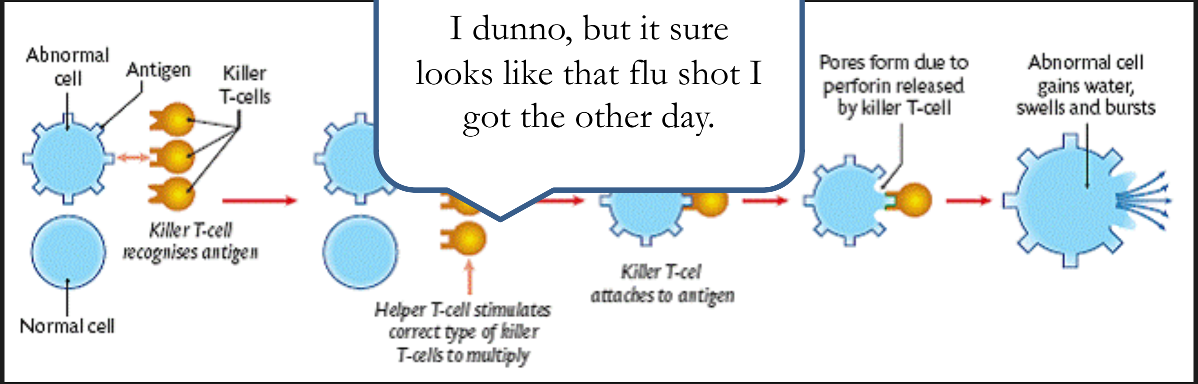
Zero Day Risk

What can you do to combat them?

Analogy: Immune System

Monitoring & Audit | Incident Response Plans | Mitigation & Assessment for next time

I dunno, but it sure looks like that flu shot I got the other day.



What can you do to combat them?

Takeaway – You can't perfectly protect against Zero-days, but by understanding what you've fought in the past and generalizing you can do your best against new things in the future.

Analogy Sad truth

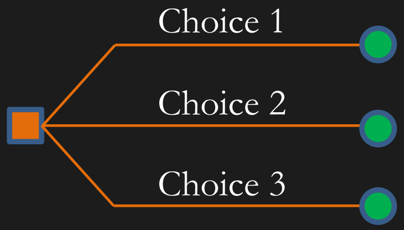
Decisions about Info. Sec. Spending (governance) are made with uncertainty.

Risk Probability Theory

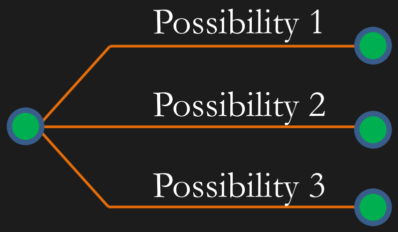
Risk probability theory can help quantify uncertainty and structure the decision making process.

Decision Trees

- Decision Node (choice)



- Event Nodes (different possibilities)



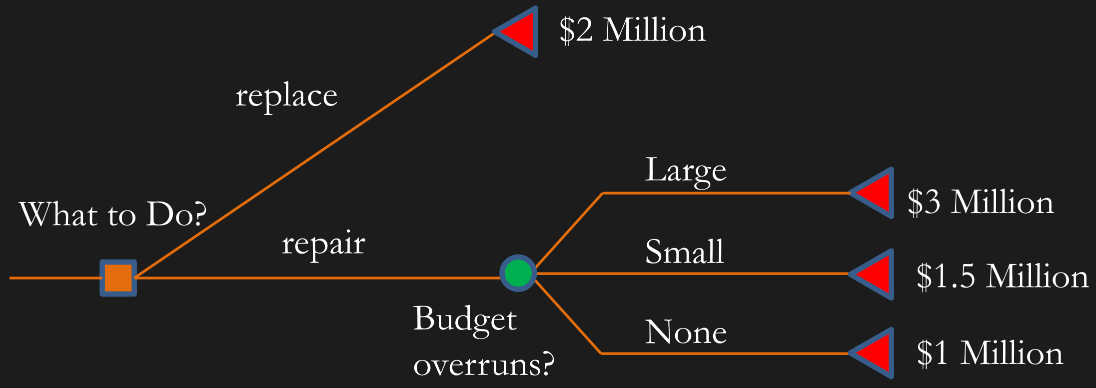
- Outcome Leaf Node (results)

Decision Trees

- Provide illustrative clarity for decision making
- Build Quantitative reasoning beyond ATLE
- Can represent uncertainty

Decision Trees: Simple example (e.g. leaky roof)

(probabilities unknown)

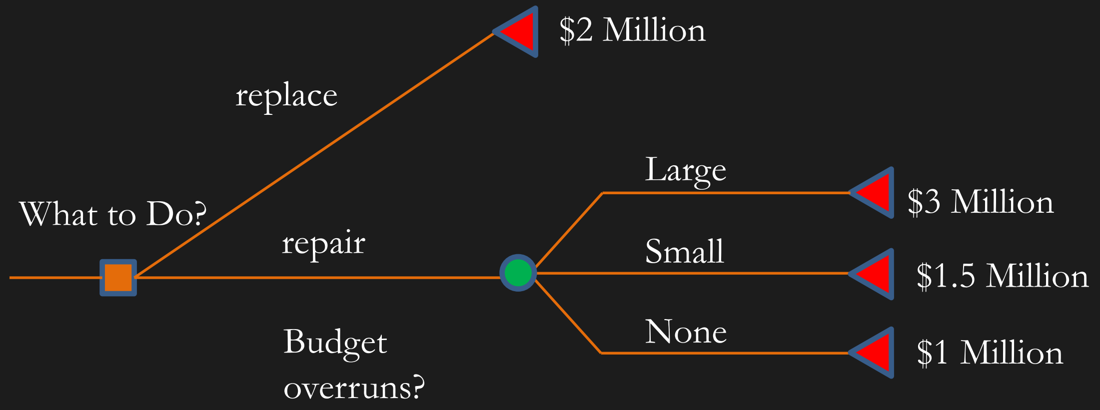


Decision Tree: Optimization Rules

- Pessimism (maximin or minimax)
  - Conservative decision maker will
    - maximize the minimum gain (if outcome = payoff)
    - minimize the maximum loss (if outcome = loss, risk)
- Optimism
  - The risk seeker will maximize the maximum gain (maximax)
  - or choose the cheapest and hope that the maximum loss doesn’t occur (minimin)
- Compromise (Hurwitz rule)
  - Maximize ($\alpha(\min) + (1-\alpha)\max$), $0 \leq \alpha \leq 1$
    - $\alpha = 1$ => pessimism
    - $\alpha = 0.5$ => neutral
    - $\alpha = 0$ => optimism
  - or Minimize ($\alpha(\min) + (1-\alpha)\max$)
    - $\alpha = 1$ => optimism
    - $\alpha = 0.5$ => neutral
    - $\alpha = 0$ => pessimism

Decision Trees: Simple example (construction)

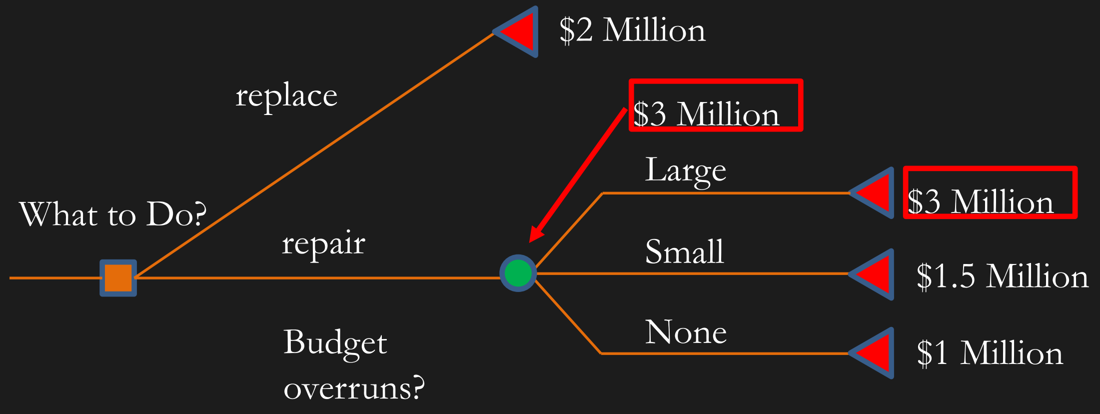
(probabilities unknown)



Pessimism:
minimize the maximum loss

Decision Trees: Simple example (construction)

(probabilities unknown)



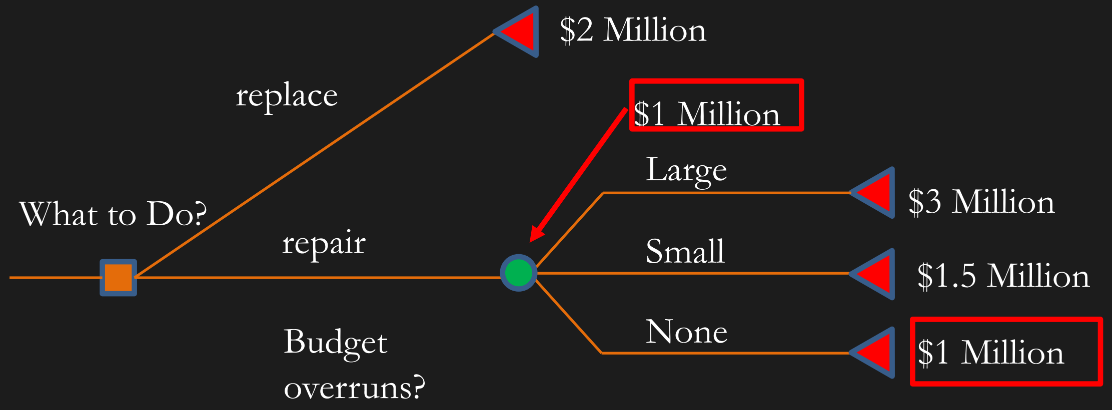
Pessimism:

minimize the maximum loss

= min (2, 3) =2 => replace

Decision Trees: Simple example (construction)

(probabilities unknown)



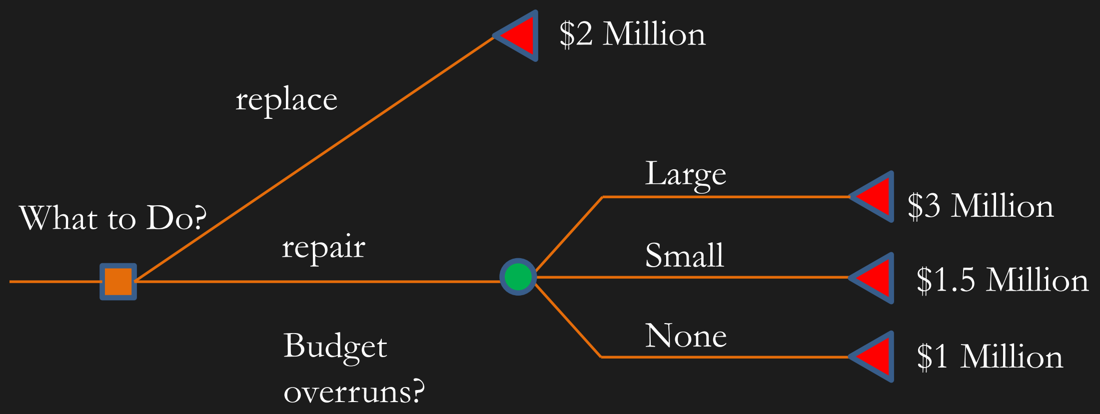
Optimism:

minimin -> pick the cheapest and hope for the best

min (2, 1) => repair and hope the budget doesn't overrun

Decision Trees: Simple example (construction)

(probabilities unknown)



Neutral:

pick the minimum of the medians of each

min (2, [0.5*3+0.5*1]) = min (2, 2) => repair or replace

or assume equal probability

min (2, [0.33*3 + 0.33*1.5 + 0.33*1]) = min (2, 1.83) => repair

Decision Trees: When to use each rule

- Pessimism
  - (maximin) Good for established organizations that want to provide quarterly gains that meet expectations
  - (minimax) Good for establish organizations that want to minimize catastrophic loss such as loss of reputation or huge data loss
- Optimism
  - Good for startups and risk seekers that want to make money quickly or bust (maximax)
  - Good for startups that prefer to devote money towards core functionality rather than security (minimin)

Risk Preference

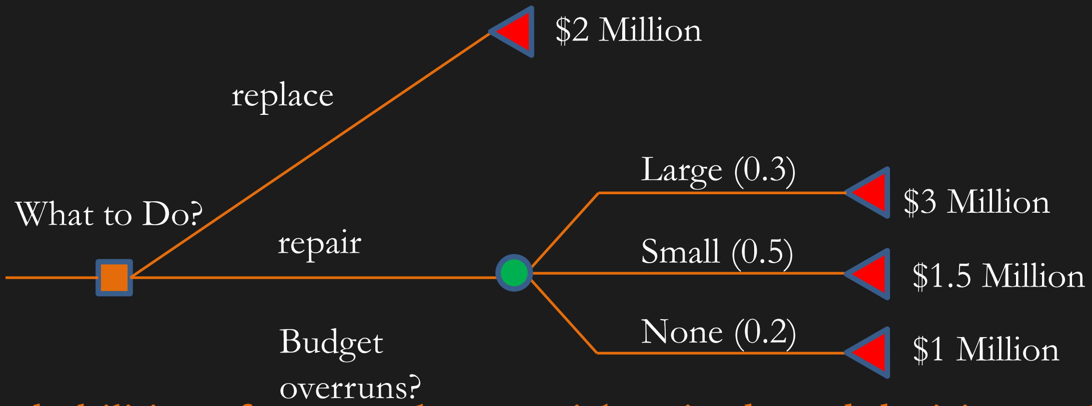
- Groups prefer different types of uncertainty
  - Some prefer risk aversion
  - others seek risks
  - E.g. Gamblers value gaining $x more than they disvalue losing $x
- Risk averse groups will pay *risk premiums* to avoid uncertainty
  - a risk premium is an amount of money that pins down risks, but may be higher than the expected cost of accepting the risks
  - e.g. insurance premiums are risk premiums that individuals pay to avoid the risk of footing high medical bills, most people never have medical bills though – so non risk averse entities (like insurance companies can profit)

Risk Preference: Categories

- Risk attitude is a general way of classifying risk preferences
- Classes
  - *risk averse* – fear loss and seek sureness (individuals who pay for health insurance)
  - *risk neutral* – indifferent to uncertainty (insurance companies)
  - *risk lovers* – don't fear loss and seek large payoffs (startups, day traders)
- Attitudes change with time and by circumstances for companies and individuals

Decision Trees: Simple example (leaky roof)

(now with known probabilities)



Knowing the probabilities of events changes <u>risk attitude and decision making</u>

Expected Cost of repair = 0.3*3 + 0.5*1.5 + 0.2*1 = $1.85 million

relaxed Pessimism -> min (2, 1.85) => repair instead of replace

relaxed optimism -> min (2, 1.85) => repair, we don't have to hope as much

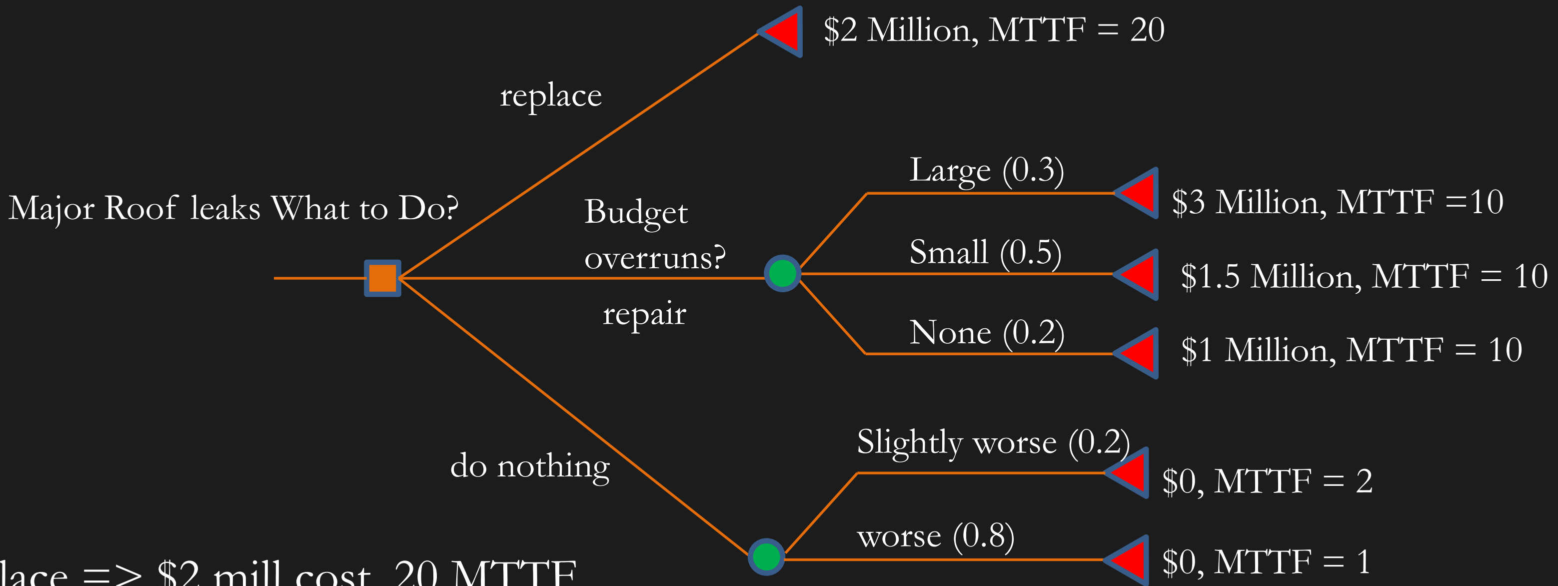
Decision Trees can have multiple terminal attributes

- Makes decision making depend on optimizing all attributes
- Can affect risk attitude differently.
- Requires decision makers to quantify all attributes
- Also requires decision makers to make trade-offs between attributes
  - can be examined using *value functions*
  - value functions can equate attributes into a single number (i.e. the value) so that you can compare two unlike attributes
  - without valuations, tradesoffs must just be made qualitatively

Decision Trees: Simple example (leaky roof)

(now with multiple attributes)

MTTF = mean time to failure



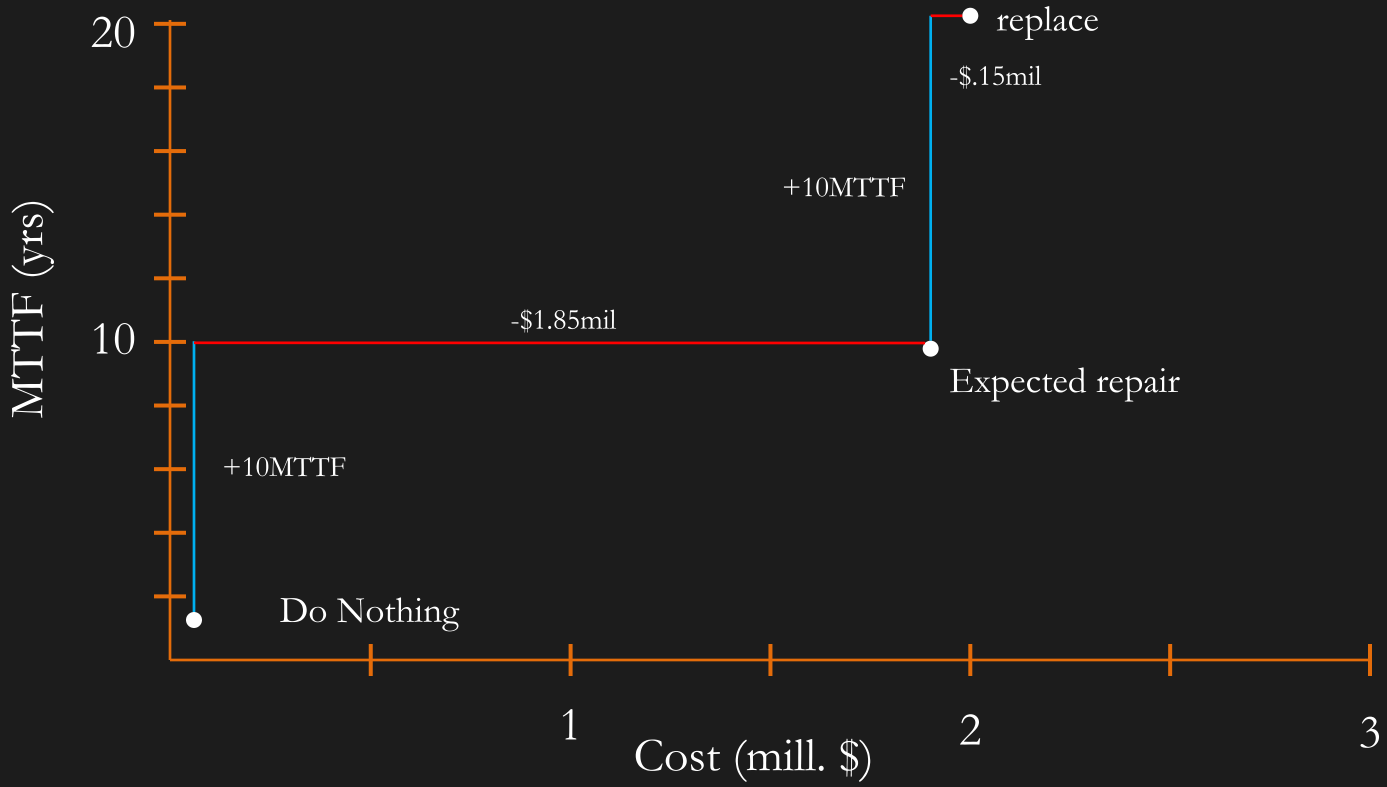
Replace => $2 mill cost, 20 MTTF

Repair => $1.85 mill cost, 10MTTF

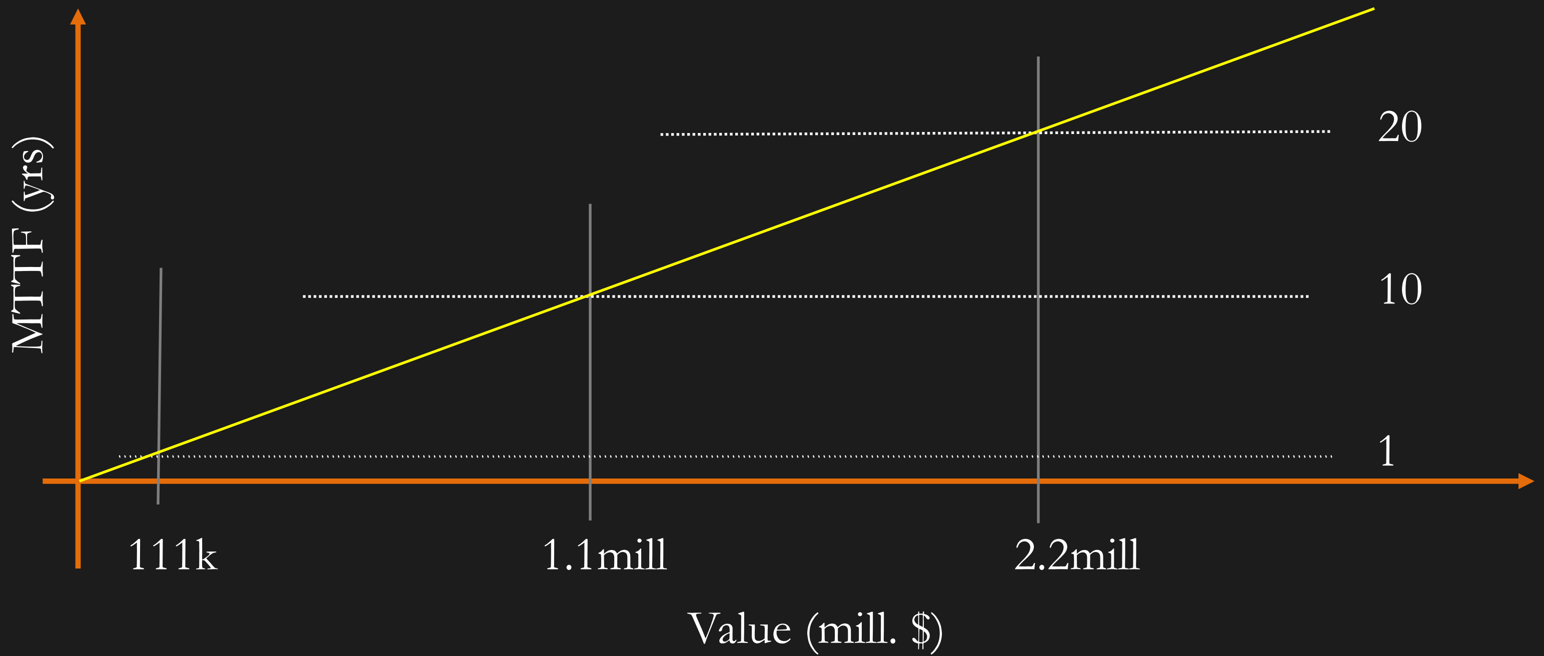
Do nothing => $0, 0.8*1 + .2*2 = 1.2 MTTF

Risk Probability Theory

Decisions, Decisions



Valuation Function (utility theory)



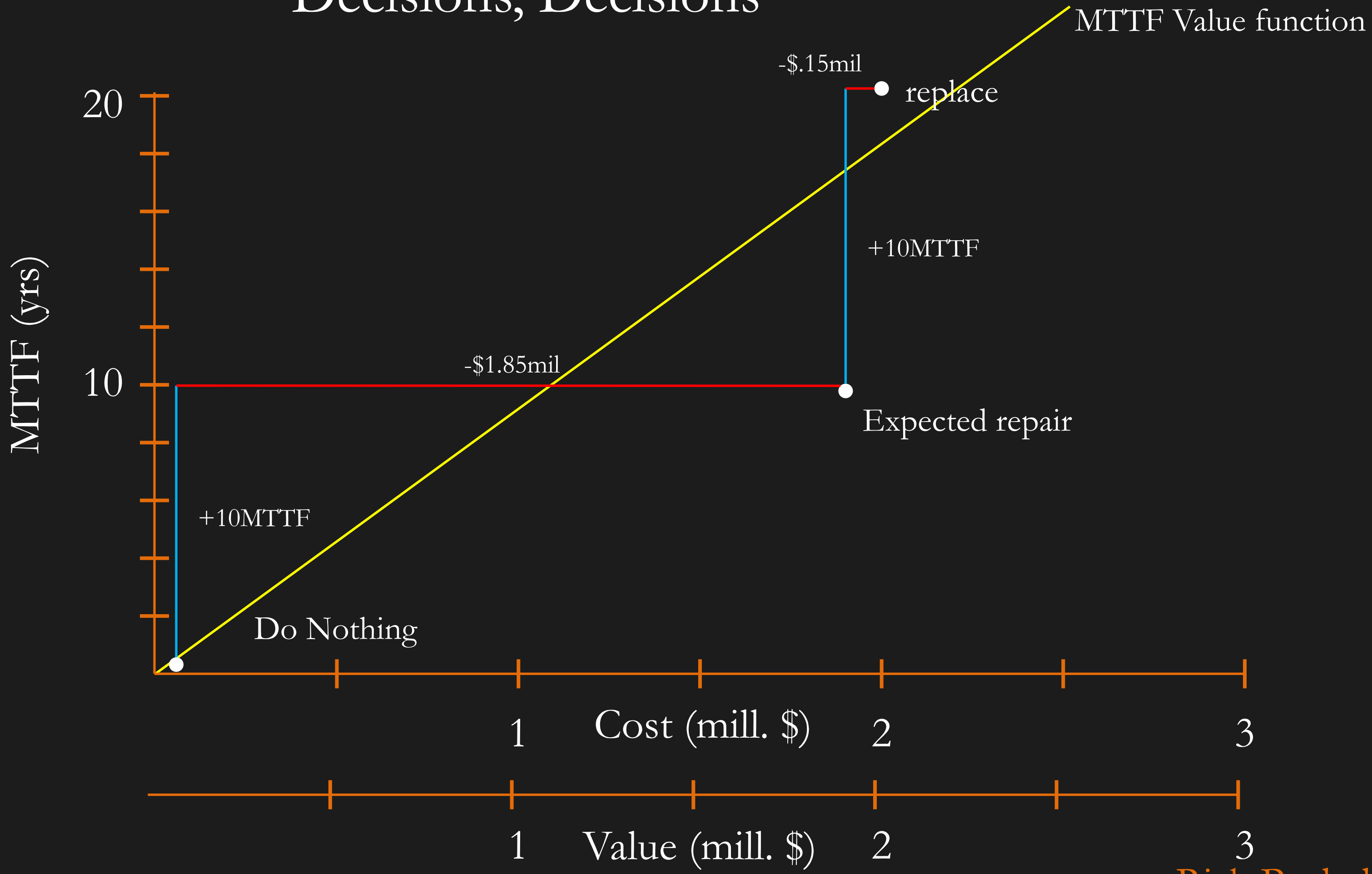
f(y) = 110000*y

Risk Probability Theory

Value Function

- Good for quantitative analysis with multiple attributes
- Compares apples to apples using money (or utility)
- Isn't always easy to determine or define
    - especially for intangibles like reputation or brand recognition

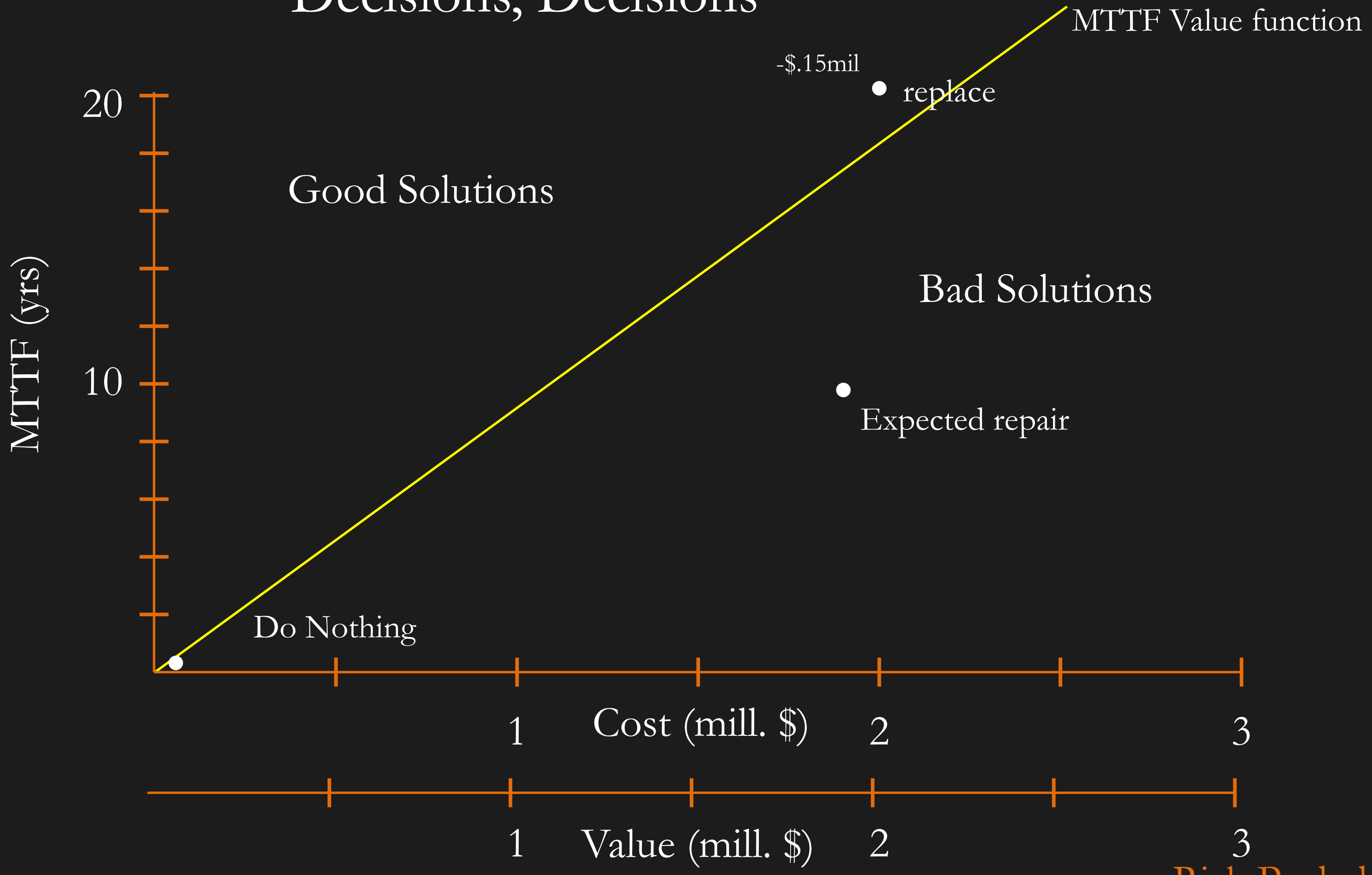
Decisions, Decisions



Value Function (leaky roof)

- Willing to trade <=110k for 1 MTTF
- If we can get 1MTTF for <110k – we are doing well
- Otherwise its not worthwhile (not valuable to the organization)

Decisions, Decisions



Value Function (leaky roof)

- Replace gets 20 MTTF at a cost of 100k per
- Repair (no overruns) gets 10 MTTF at a cost of 100k per
- Repair (small overruns) gets 10 MTTF at a cost of 150k per
- Repair (large overruns) gets 10 MTTF at a cost of 300k per
- Repair (expected) gets 10 MTTF at a cost of 185K per
- Do nothings get 1-2 MTTF at a cost of 0

So is doing nothing the best option?

No, look at overall return on investment.

Replace Valuation = -2M + 2.2M = 200k
Repair Valuation (no overruns) = -1M + 1.1M = 100k
Repair Valuation (small overrun) = -1.5M + 1.1M = -400k
Repair Valuation (Large overrun) = -3M + 1.1M = -1.9M
Repair Valuation (expected = -1.85M +1.1M = -.75M
Do Nothing (slightly worse) = 220k
Do Nothing (worse) = 110K
Do Nothing (expected) = 132K

Clearly replacing is the best for pessimists (or realists),
for cheap optimists doing nothing could work for 1-2 years

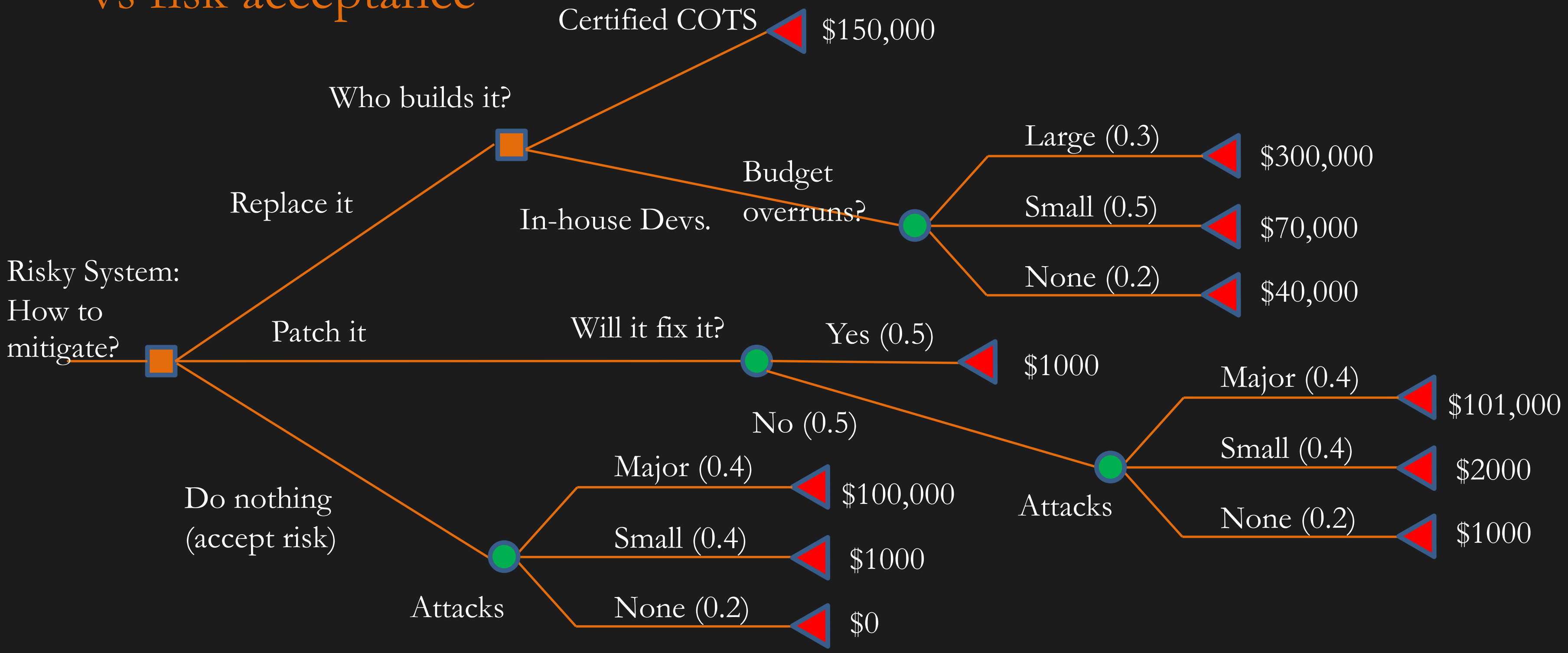
Takeaway: Multiple attribute functions involve tradeoffs.
If tradeoffs can be directly compared, the best solution is the option that maximizes utility across attributes and satisfies a group's risk attitude preferences.

So how does all of this affect Info. Sec. Governance?

A: It visually represents decision making and helps select an ‘optimal’ decision, given assumptions and risk perspective.

-> Switch to Example

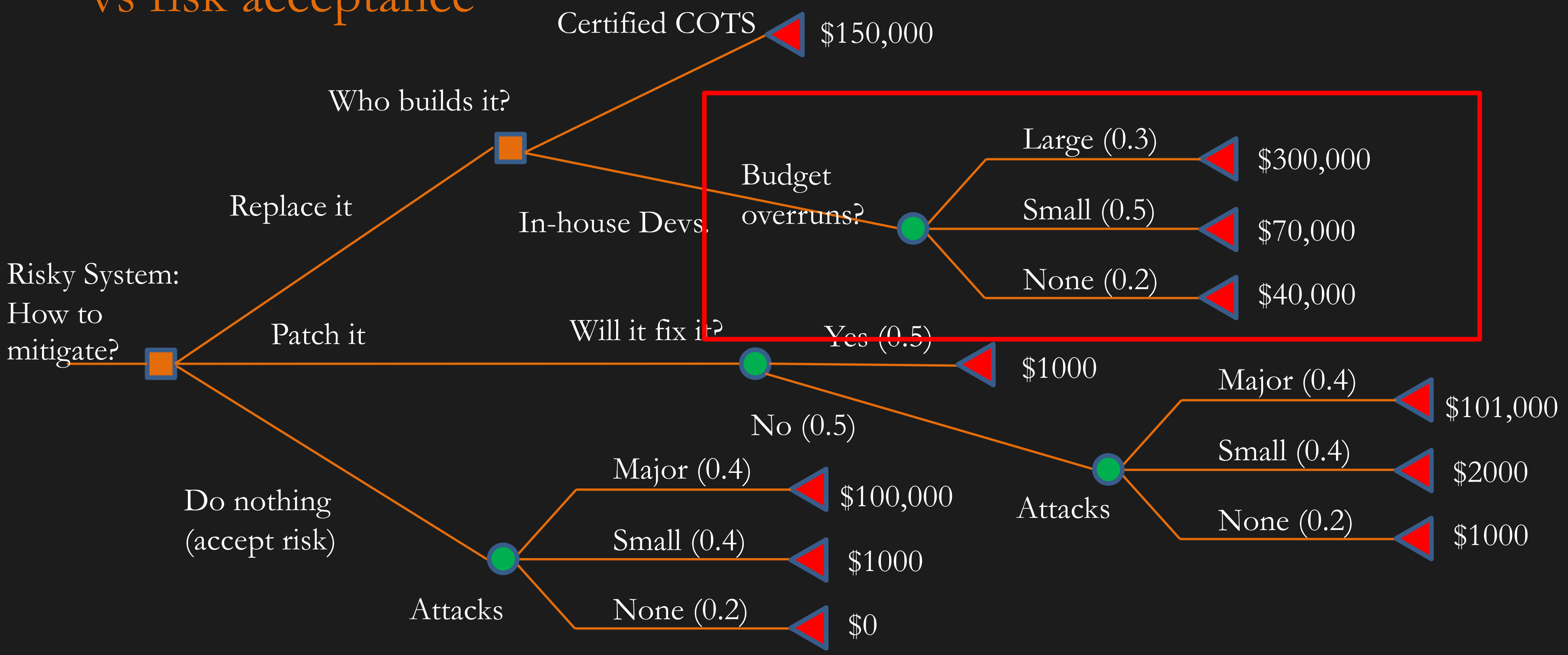
Ex. Security spending vs risk acceptance



Decision Trees: Propagation

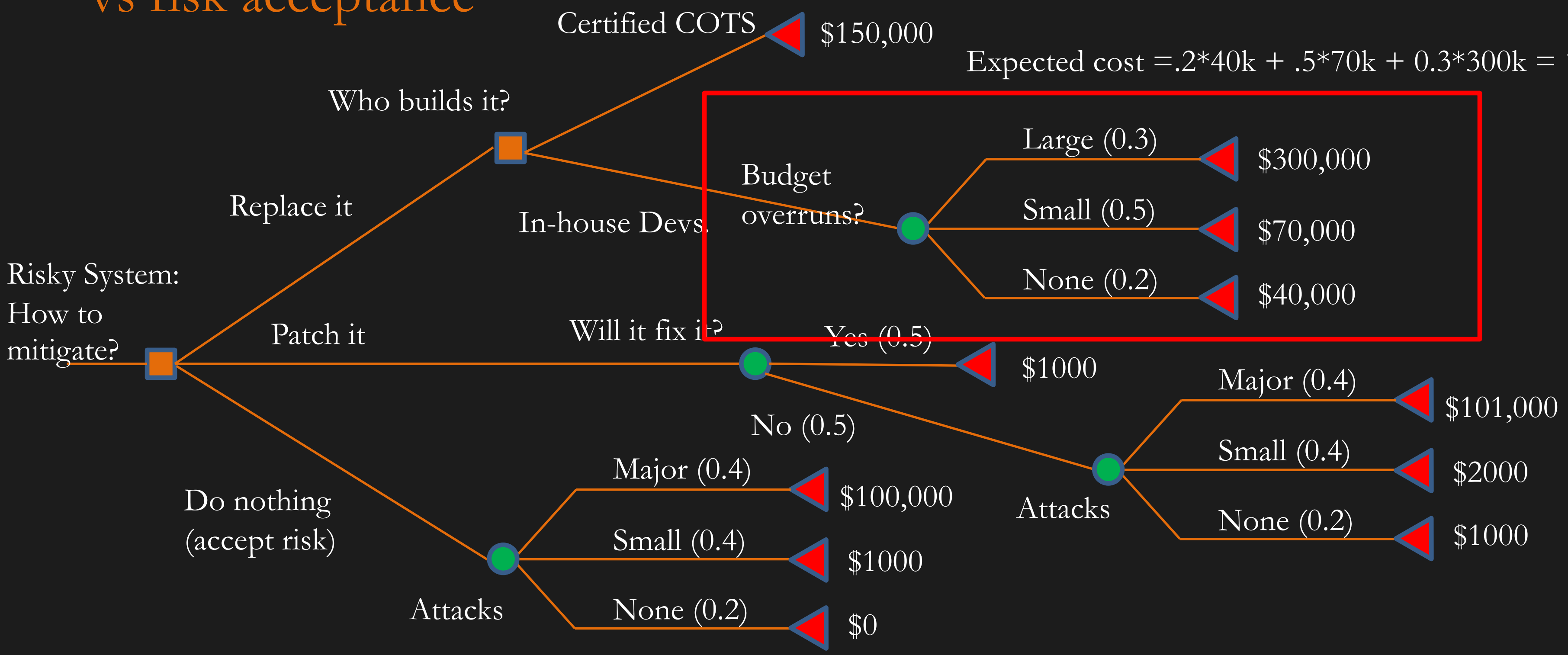
Min/maxing can propagate up a tree to resolve choices at each node
This is how (most) chess playing programs work.
Fun Fact: Some games, like checkers, are fully solved decision trees.

Ex. Security spending vs risk acceptance



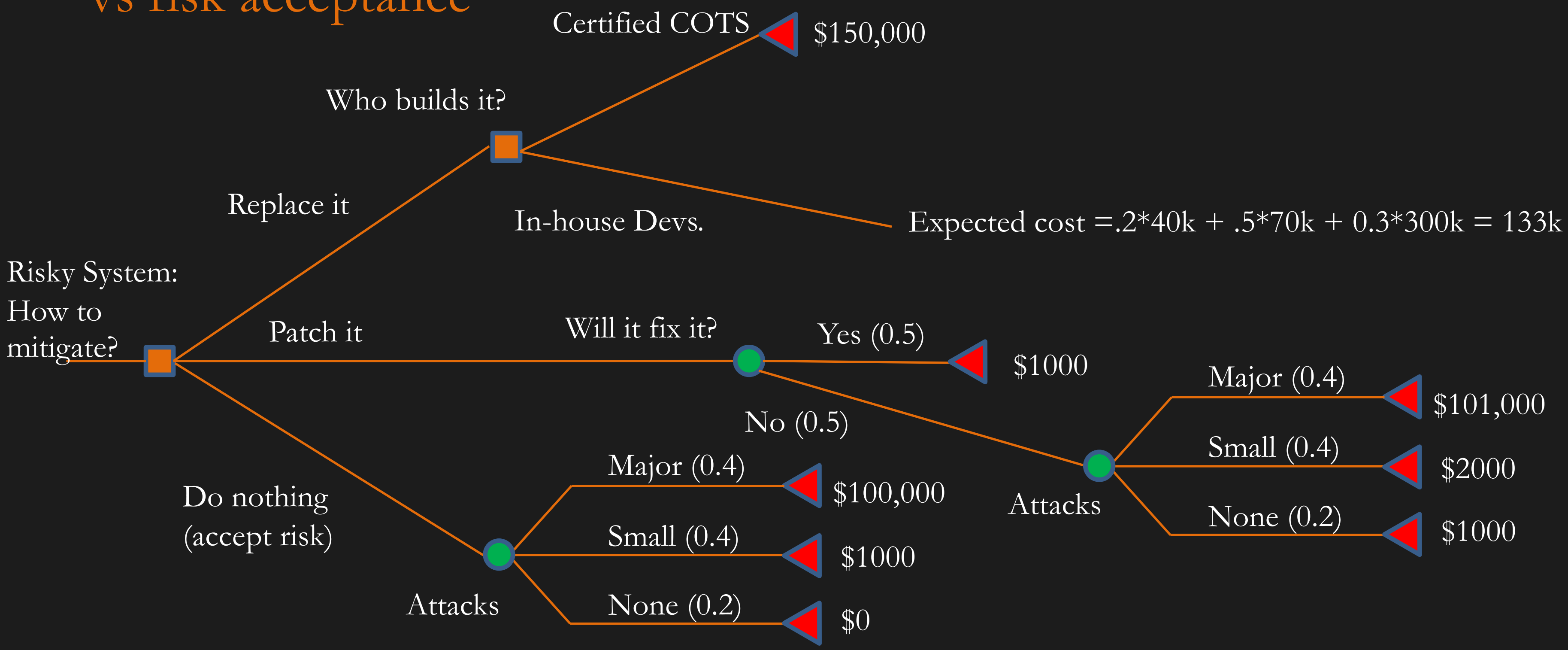
Ex. Security spending vs risk acceptance

Expected cost =.2*40k + .5*70k + 0.3*300k = 133k

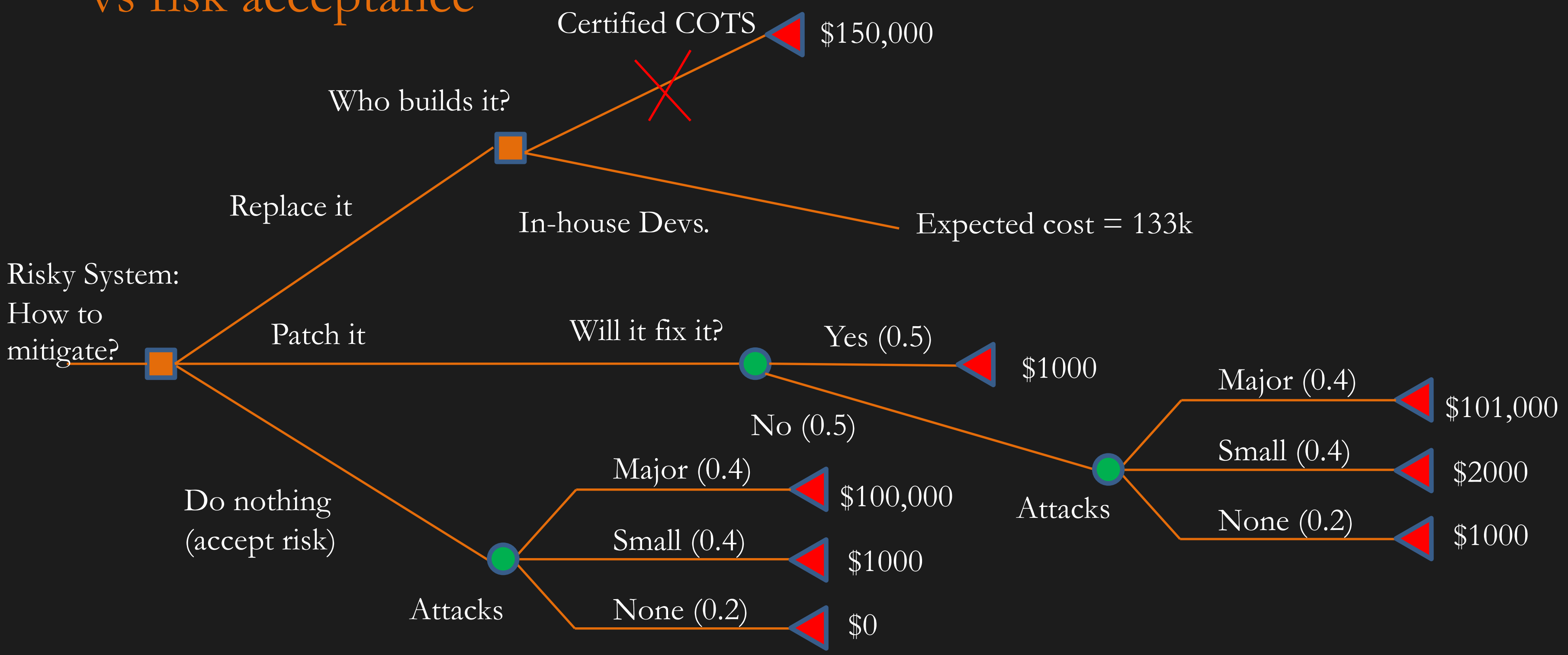


Risk Probability Theory

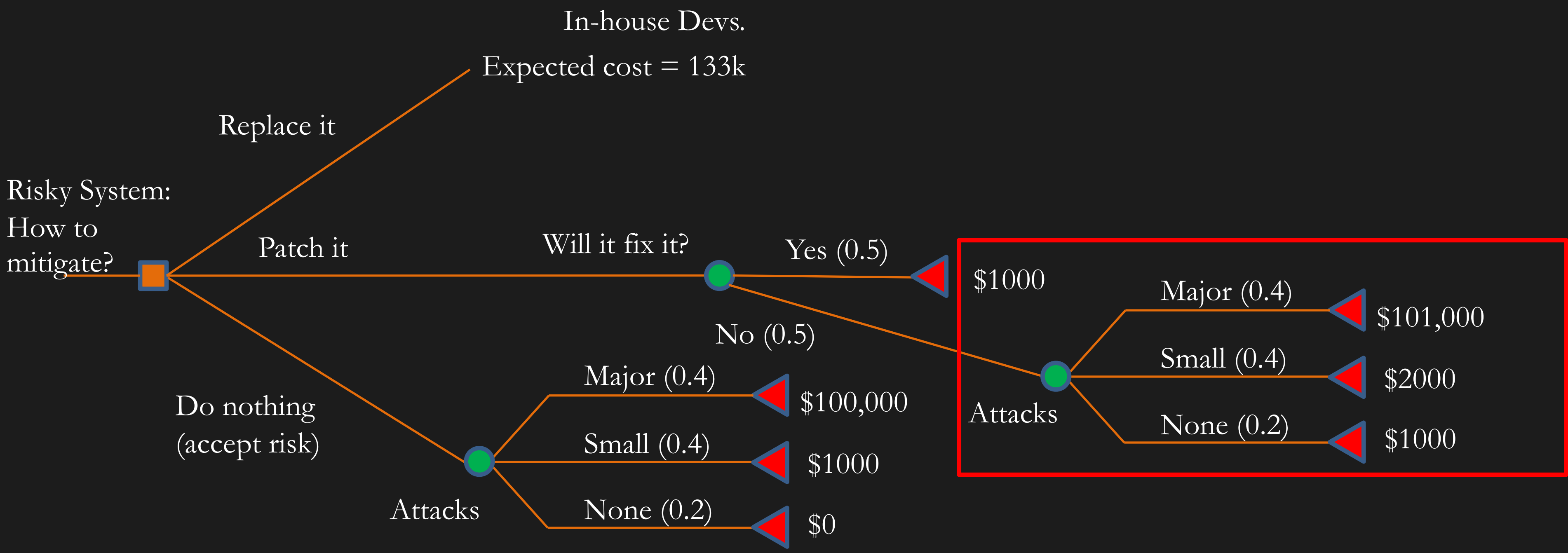
Ex. Security spending vs risk acceptance



Ex. Security spending vs risk acceptance

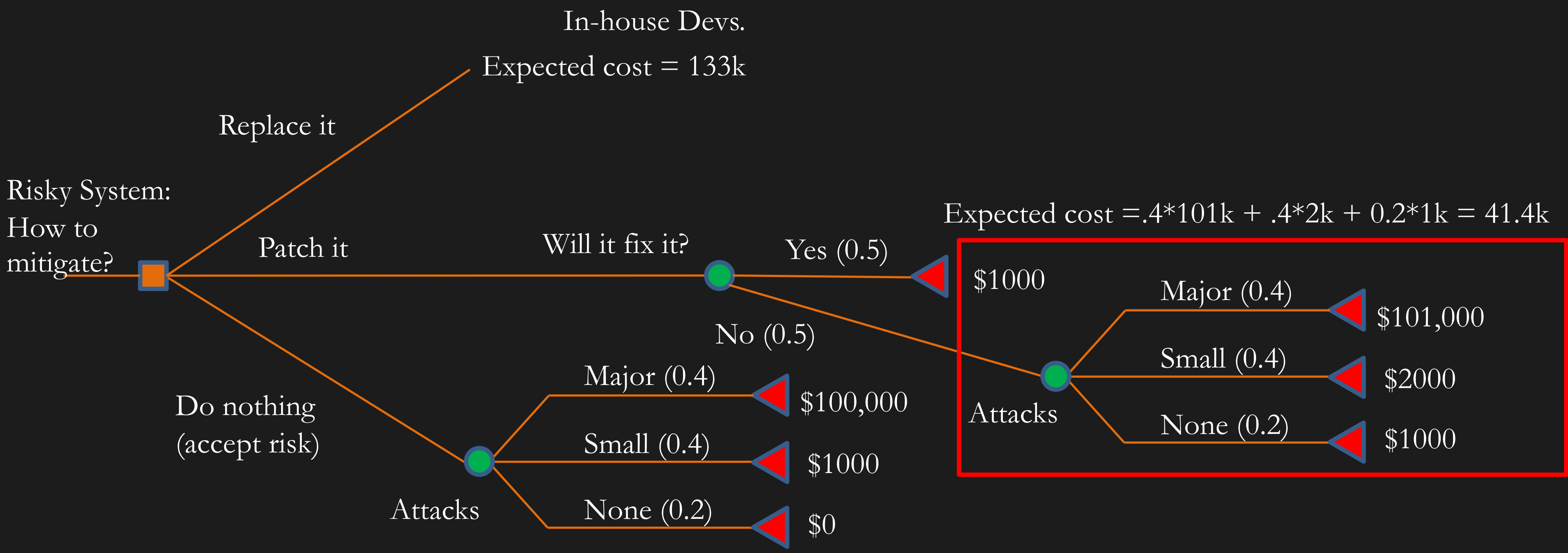


Ex. Security spending vs risk acceptance

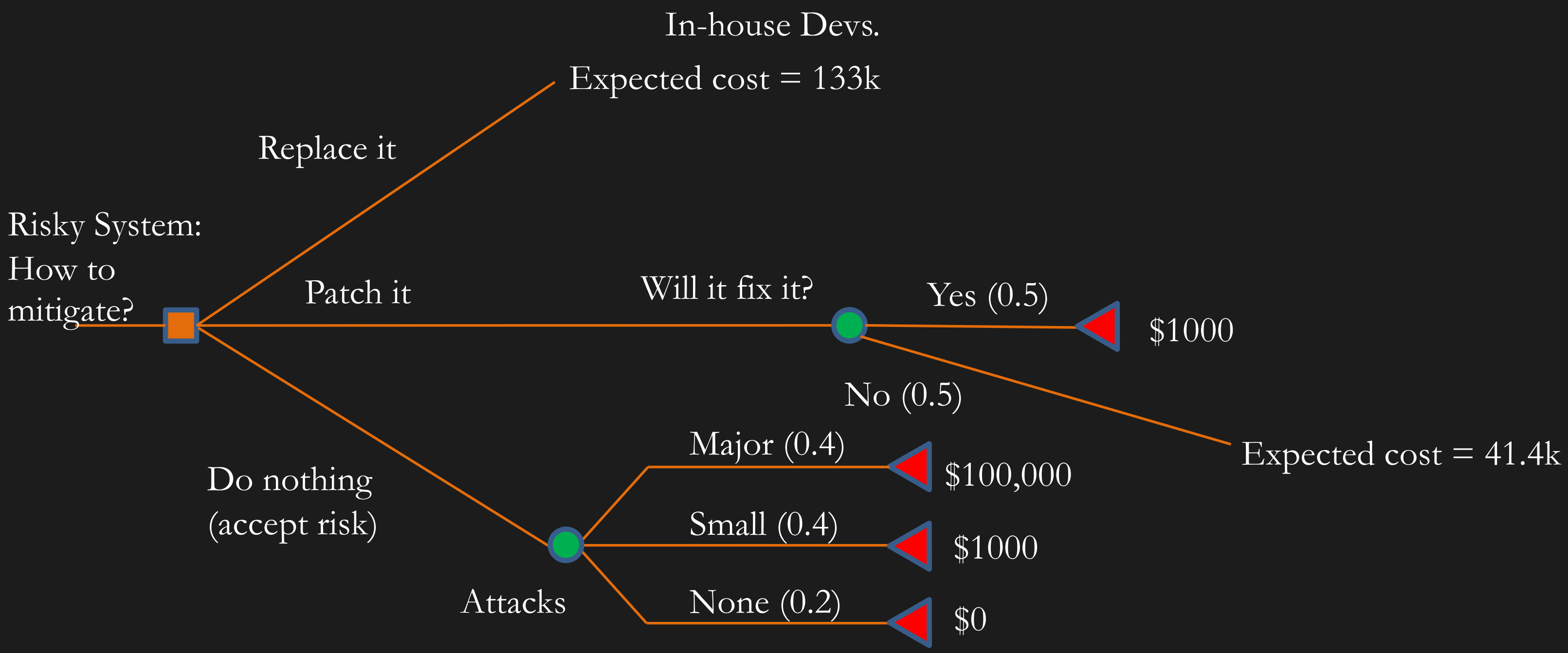


Risk Probability Theory

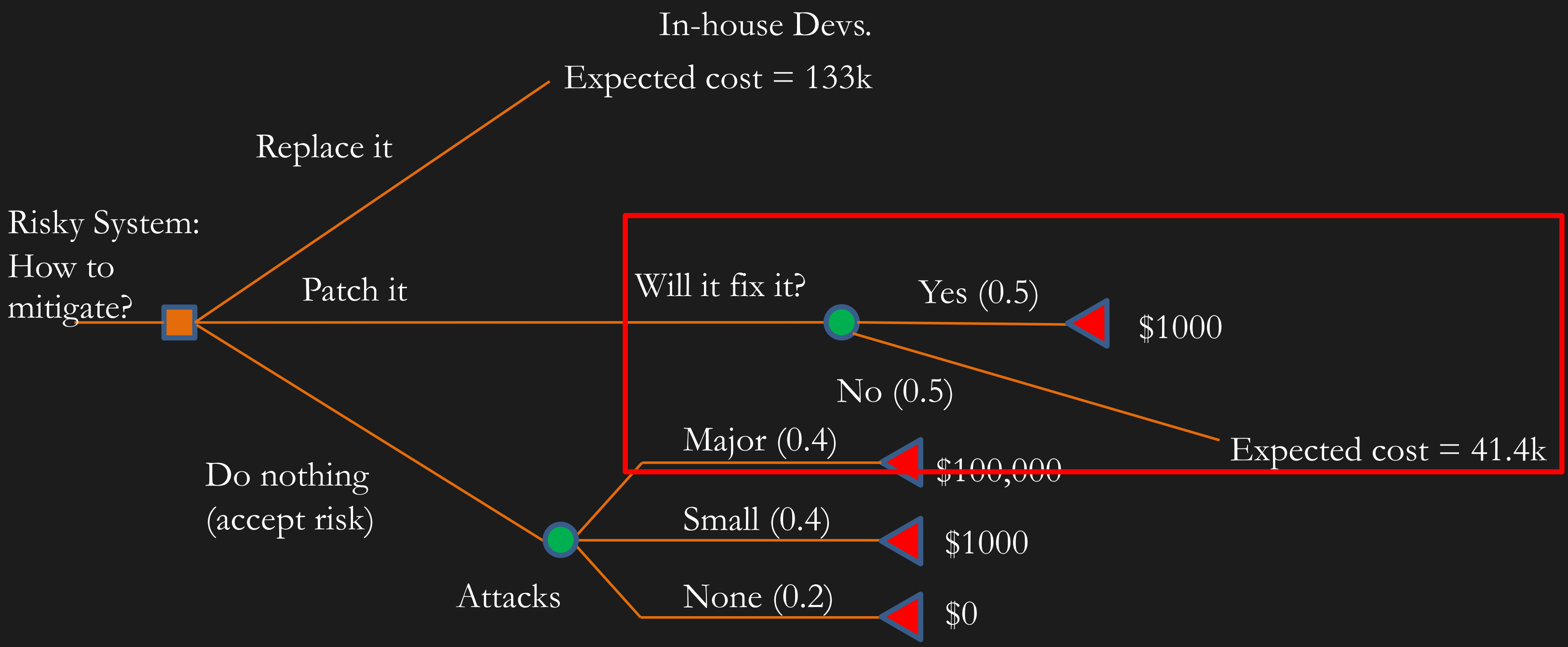
Ex. Security spending vs risk acceptance



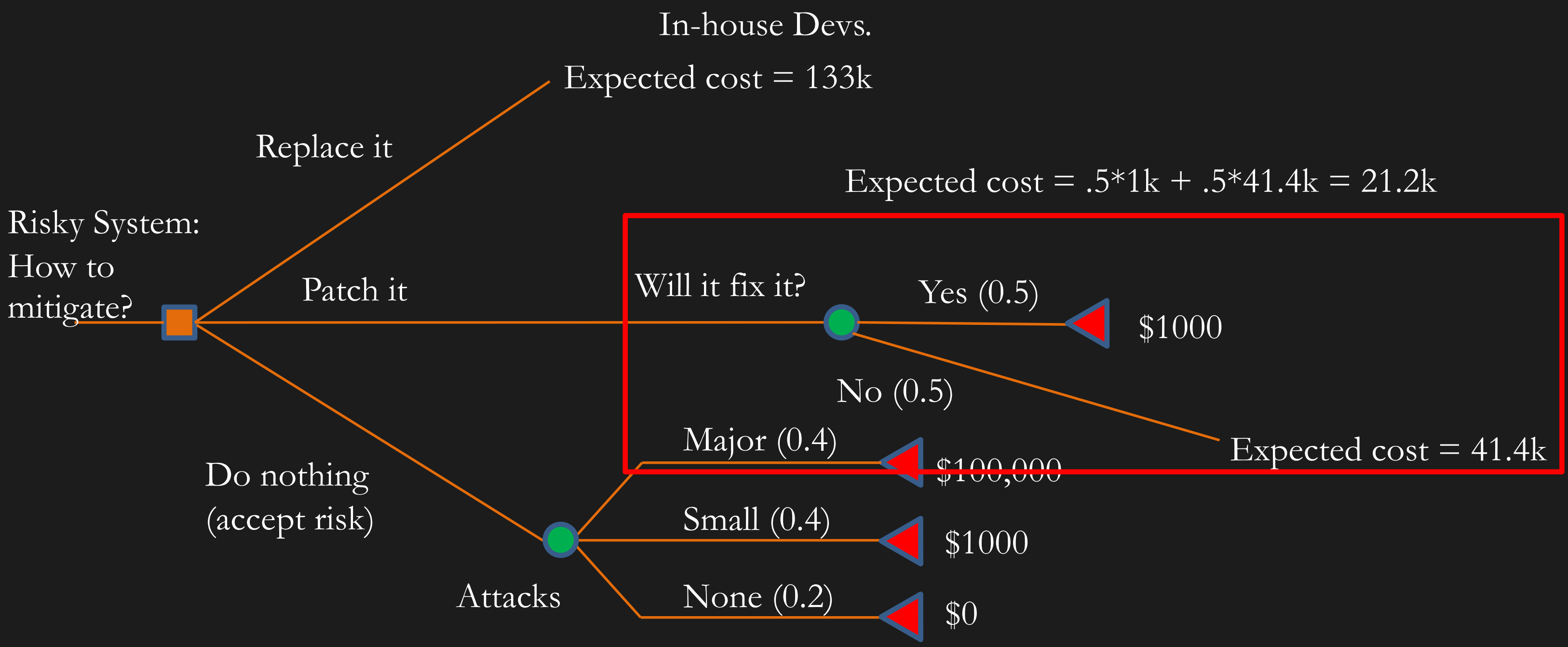
Ex. Security spending vs risk acceptance



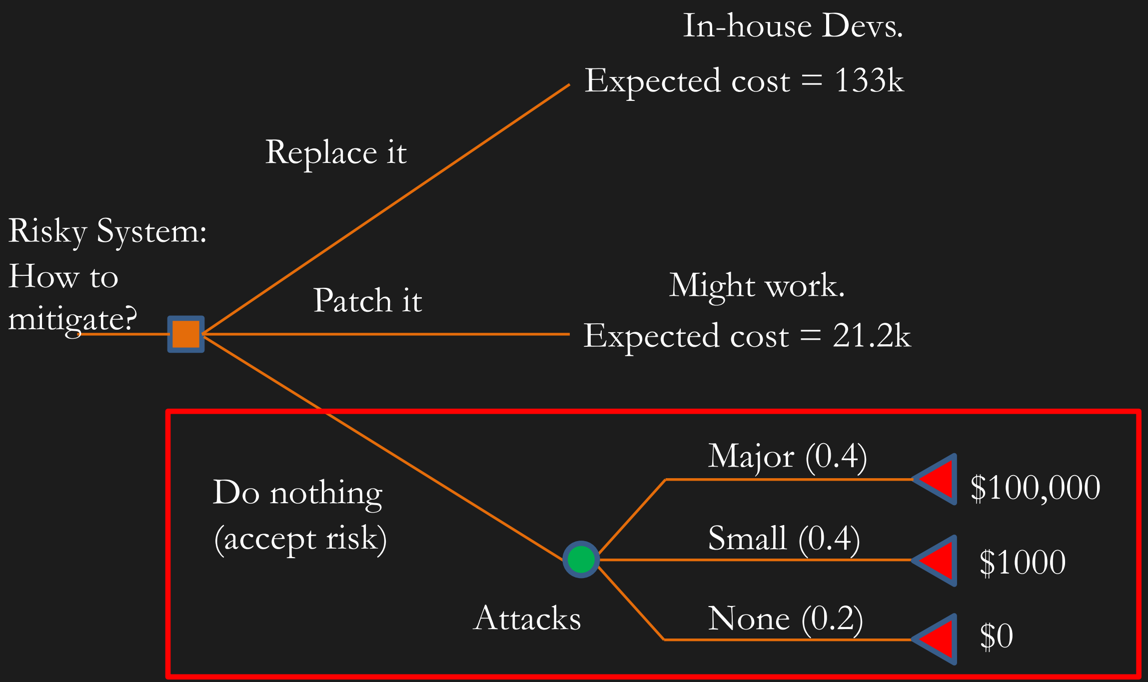
Ex. Security spending vs risk acceptance



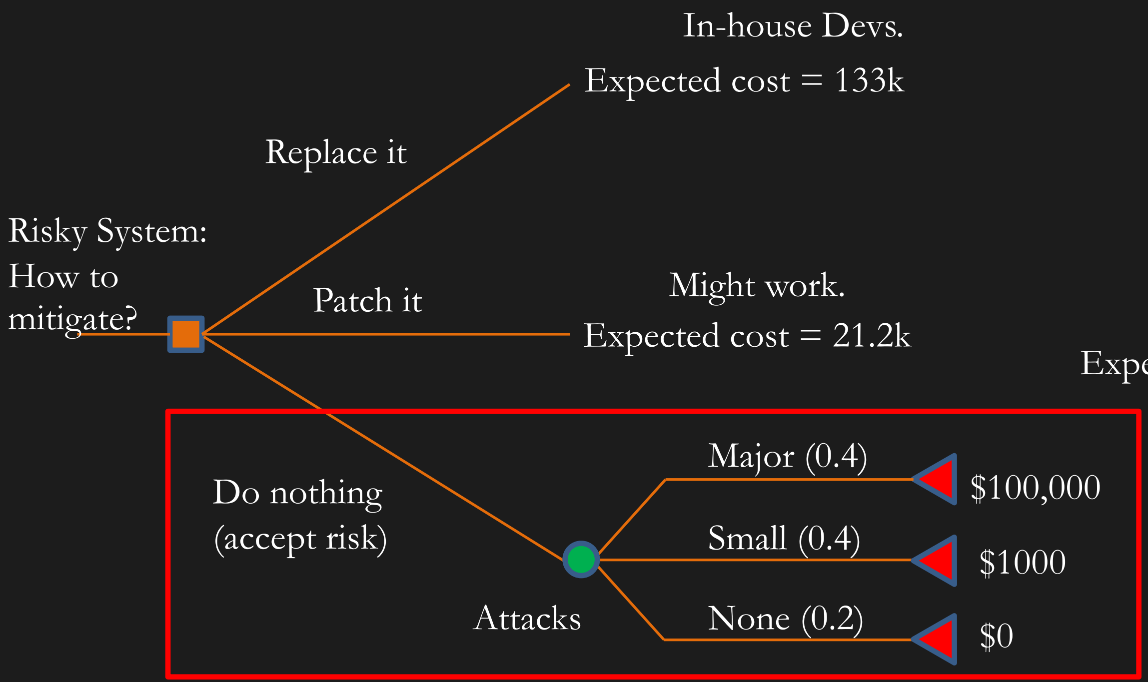
Ex. Security spending vs risk acceptance



Ex. Security spending vs risk acceptance

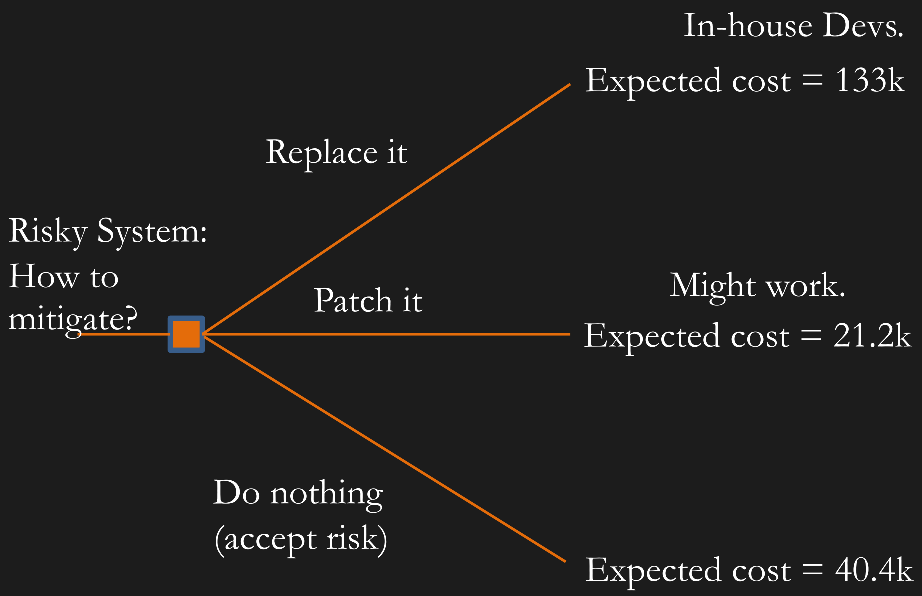


Ex. Security spending vs risk acceptance

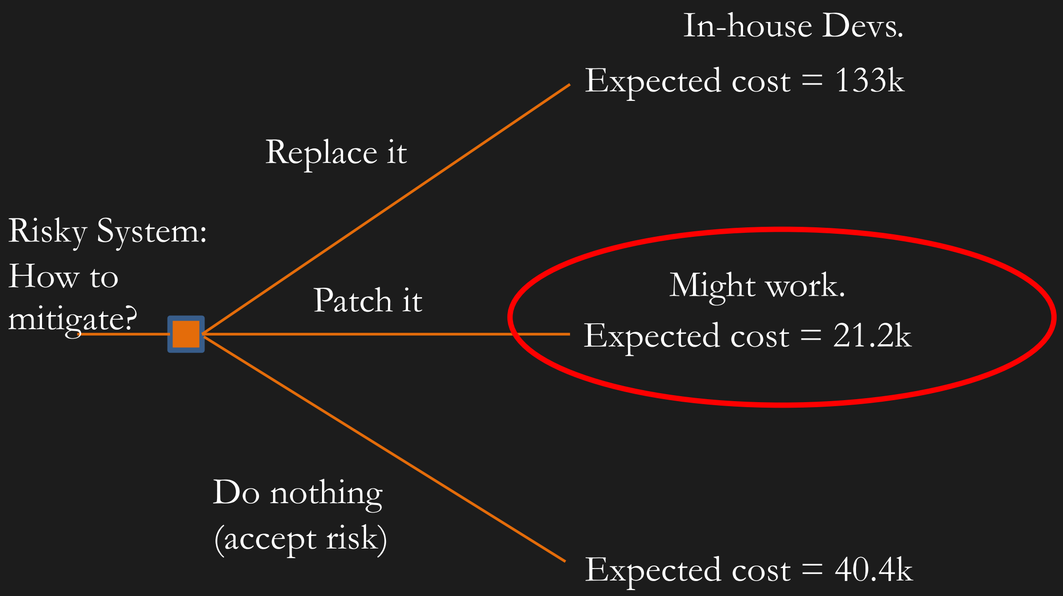


Expected cost = .4*100k + .4*1k + .2*0 = 40.4k

Ex. Security spending vs risk acceptance



Ex. Security spending vs risk acceptance



Despite using the same garbage legacy system and annoying its users, the organization opts to just add another patch.

Example (discussion)

The decision might be different if a second attribute factor (like how old the system is) was added to the consideration or if the organization's risk preference was different. This would encourage the organization to consider a new system over patching the old one.

Example (discussion)

This is a good demonstration of why established organizations rarely replace old systems with new. It doesn't consider any of the other benefits of updating to a new system. If you find yourself in a leadership position you *should* consider other factors in your analysis.

Summary: Decision Making Philosophy

- Dollars spent for security measures should be less than the expected losses they seek to prevent
- Rational strategic thinking minimizes loss and maximizes value to an organization
- Risk preferences affect decision making and can influence valuation functions
- Important to consider all relevant attributes and not simply those related to preventing loss (security)

Rule of Thumb: Decision Making Philosophy

When making a decision, ensure your choices maximize your value and minimize your loss.

Homework

Hw2: Decision Trees and Risk

https://mlhale.github.io/CYBR3600/homework/iasc3600-homework2.pdf

(Due by class time Tuesday Sept. 5th)

R
E
A
D
I
N
G

None

Next Time

Forming High Level Policy

Next Time

Quiz Next Thursday (Sept. 6th) on Decision Trees

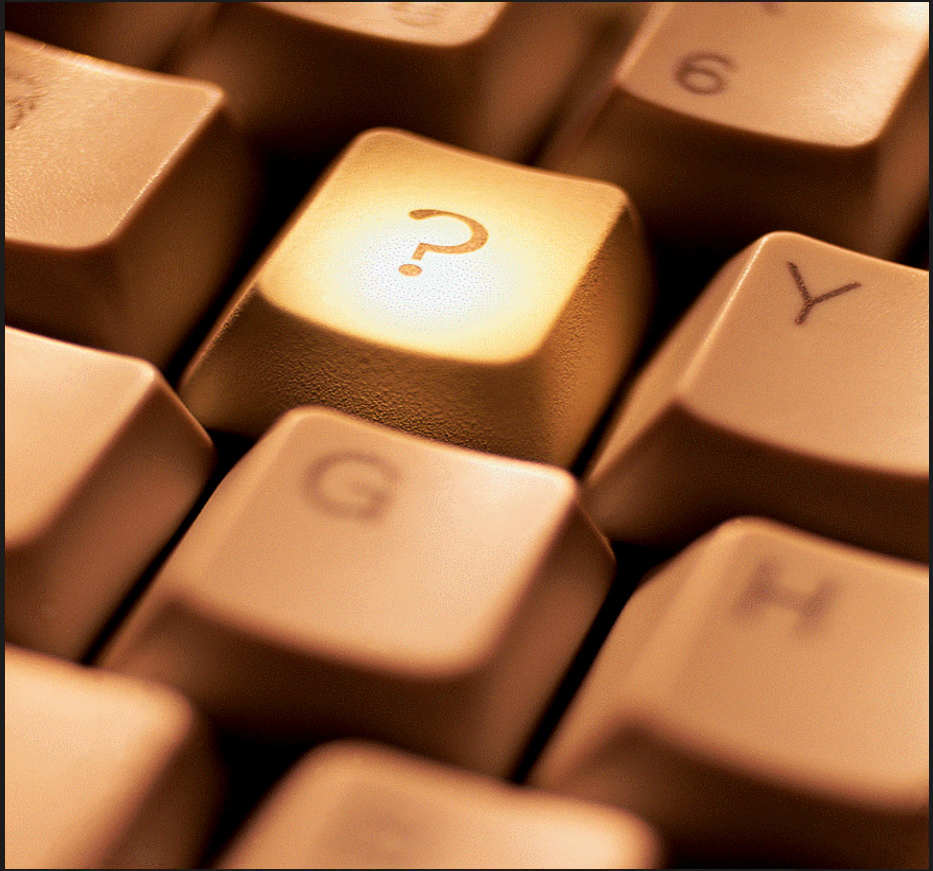
Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics
mlhale@unomaha.edu

Twitter: @mlhale_



© 2014-2018 Matthew L. Hale