Dare You Risk IT?

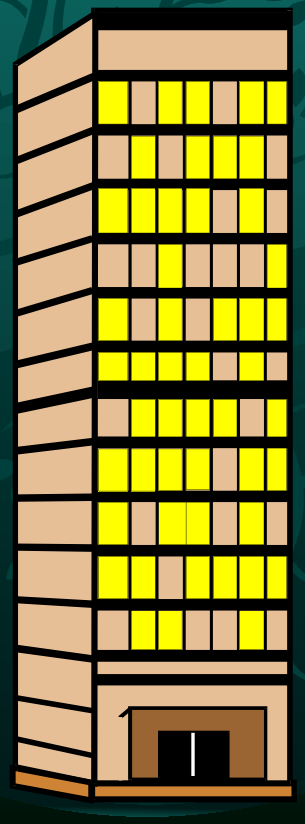
Optimizing Risk in the Corporate IT Environment

Military Intelligence

Risk Minimization

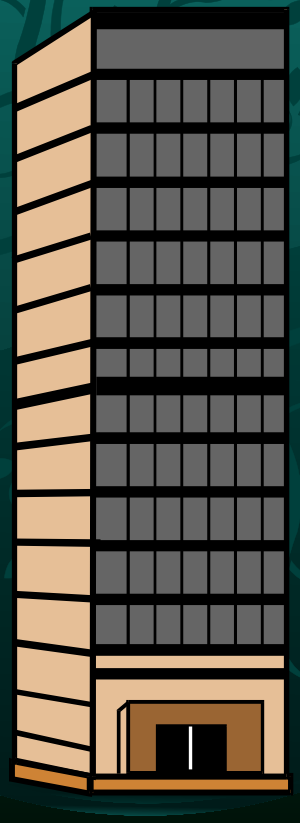
Risk Free Business

Risk Minimization



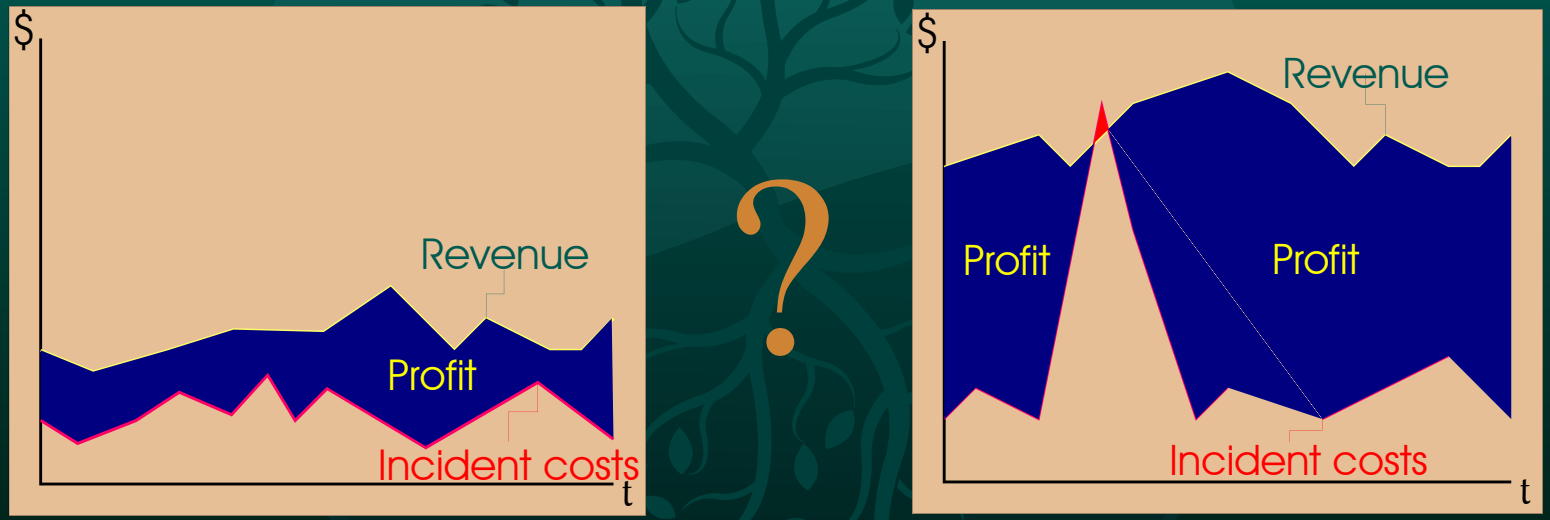
Risk Free Business

Profit Minimization



Optimal Risk

Maximize Profit Over the Long Haul



Charge!

Couldn't they do better than this?

- 44 million cards in Canada
- $142M in fraud losses!
  - Stats from the Canadian Banker's Association

Charge!

Couldn't they do better than this?

- 44 million cards in Canada
- $142M in fraud losses!
- $121B volume
  - Suppose 3% transaction fee = $3.6B revenue

Charge!

Maybe they did it right after all.

What if cutting fraud losses to $^{1}/_{10}$ cut sales in ½?
Suppose 10% of revenue is profit.

10% × $3.6B = $360M
$360M - $142M = $218

?

10% × $1.8B = $180M
$180M - $14M = $166

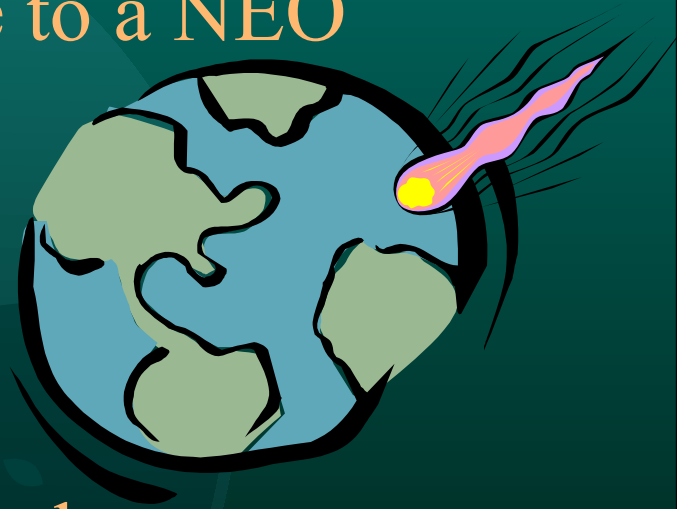
Definition of Risk

Risk ≡ Probability × Damage

- Can't determine probability of infrequent events
- IT stuff never lasts long enough to gather stats!
- Are incidents with High Probability/Low Impact equivalent to Low Probability/High Impact events?
- Hostile, intelligent adversaries are adaptable
- Probabilities don't deal well with irrational people

Was Velikovsky Right?

By middle age, risk of dying due to a NEO collision is 1 in 10,000.



One 100m object/10,000 years; ~100 Megaton explosion.

1 Km objects hit every 100,000 years. Will kill about 25% of the human race.

I.e., 150 deaths per year in the UK (acceptable?)

(Note: compared with ~85 UK bathtub deaths/year)

BUT – single event death toll of 15 million Brits

Risk ≡ Probability x Damage

Classic definition of risk. Yields a cost/year figure.

- Can't find the probability of infrequent events.
- Rarely have to worry about frequent events
  - Why?
- Considers an infrequent, high cost incident to be equivalent to a frequent, low cost event
- Ignores knowledge about capabilities of enemy
- An intelligent enemy adapts

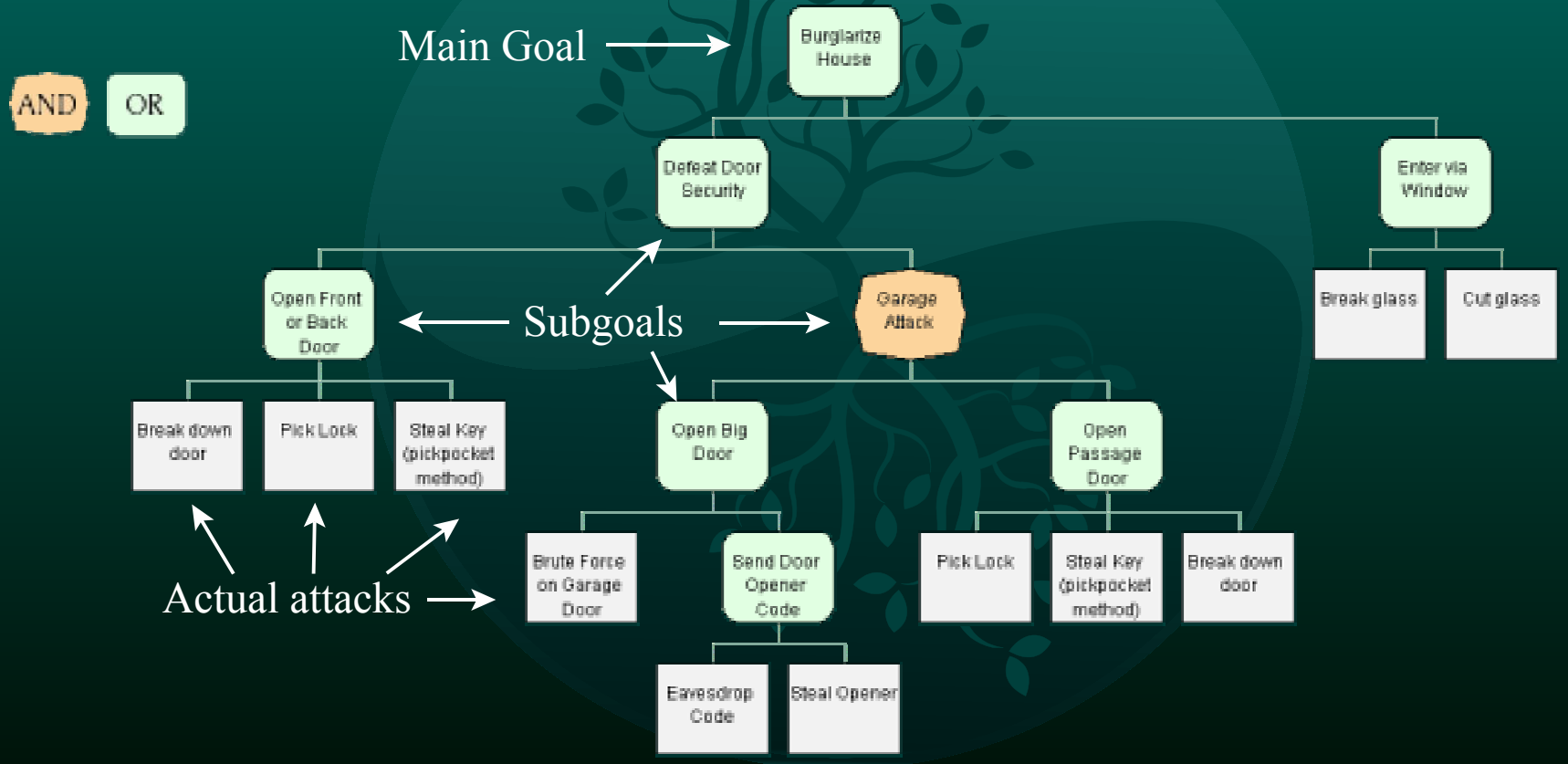
Don’t Reinvent the Wheel

Listen carefully, grasshopper . . .

- IT isn’t the first industry to deal with risk
- Gas pipelines, chemical plants, industrial applications use fault trees and hazard trees
- Bruce Schneier suggested using *Attack Trees* for IT risk in a conference in 1997
- Tree describes **how** attacks could occur

Vulnerability Analysis

Attack Trees - Capability-Based Approach

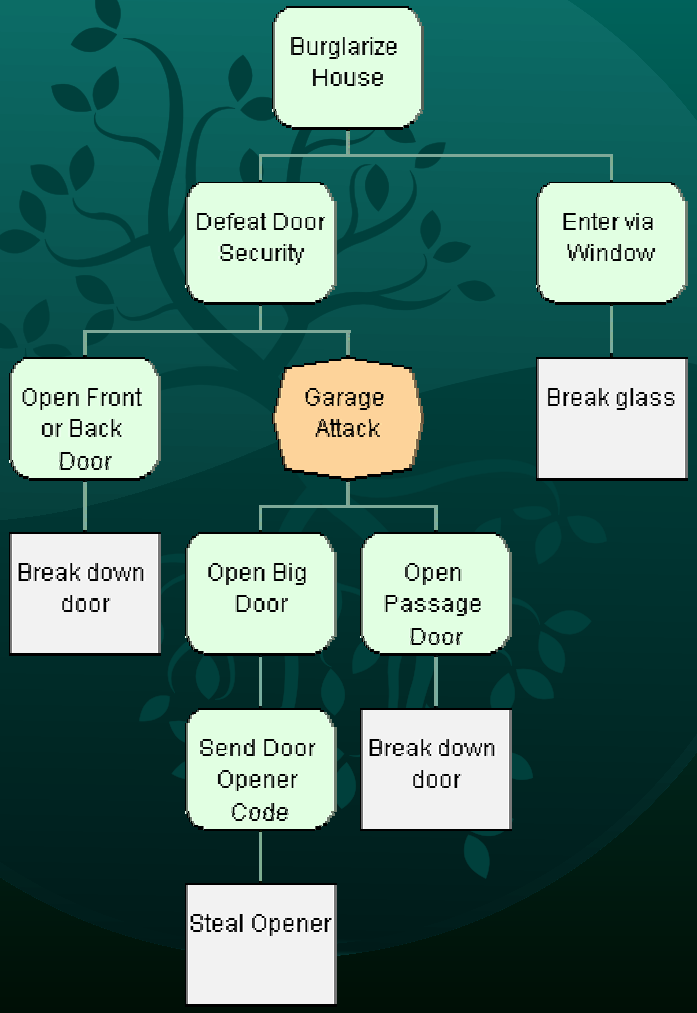


Possibility vs Probability

Can it happen?

- Even lunatics & fanatics are resource constrained
- Choose resources that influence human behavior
  - Cost, Technical ability, Materials, Escapability
- Compare resources required for each (leaf) attack with capabilities of attackers
- Remove infeasible attacks from model
  - Remaining attacks are areas of concern
  - It helps to have a tool – Secur*IT*ree

Attack Prediction



Juvenile Delinquent

Cost of Attack <= 50
Prob. of Apprehension <= 0.5
Technical Ability <= 15

Assumptions

- If they Can, They Will
  - ≈ true for sufficiently large groups of people
- The analyst is as smart as the enemy
  - Mustn't forget any attacks
- Must know what resources constrain the enemy
- Reasonably accurate attack resource estimates

Conventional vs Capabilities

Conventional Risk Assessment gives you . . .

1. Avoid - you get to do something about it
2. Assign - somebody else gets to do something about it
3. Accept - nobody does anything about it

Capabilities-based Attack Tree

Easy to understand graphical output

- If isolated vulnerabilities then try a point sol'n
  - Raise attacker's resource requirements
- Vulnerabilities on one subtree may suggest an architectural solution
  - Create an AND node with a secure system
- Unfixable vulnerabilities?
  - Reduce attacker's resources (Bush & Iraq)
  - Create unbearable attack cost (Cold War and MAD)

Leverage Expert Skills

Knowledge reuse

- Tree structure suited to subdivision of tasks
  - Independent work can be combined later if care used
- Trees built by experts can be reused
  - Experts are scarce
  - Less knowledgeable people can tweak a template
- Combine expertise from diverse fields in trees

Live Demo

Murphy has to leave the room

- Example is a Corporate Intranet
- Web portal application

We model the unthinkable.

Amenaza Technologies Limited
Suite 550 1000 8th Ave SW
Calgary, AB Canada T2P 3M7

www.amenaza.com
1-888-949-9797 toll free
403-630-5931