How to Improve Your Risk Assessments with Attacker-Centric Threat Modeling

Tony Martin-Vegue

Sr. Manager, Cybercrime & Business Continuity, Gap Inc.

Governance, Risk & Compliance – G33

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

Speaker Bio

Tony Martin-Vegue is Sr. Manager of Cyber-Crime & Business Continuity at Gap, Inc.

His enterprise risk and security analyses are informed by his 20 years of technical expertise in areas such as network operations, cryptography and system administration. He has worked for First Republic Bank, Wells Fargo and Cigna. His current research areas involve improving risk assessments and the risk treatment process, threat modeling and bridging the gap between business needs and information security.

Tony holds a Bachelor of Science in Business Economics from the University of San Francisco and holds many certifications including:

- **CISSP** - Certified Information Systems Security Professional
- **CISM** - Certified Information Security Manager
- **CEH** – Certified Ethical Hacker
- **GCIH** – SANS GIAC Certified Incident Handler
- **GSEC** – SANS GIAC Security Essentials

Tony lives in the San Francisco Bay Area, is a father of two and enjoys swimming and biking in his free time.

Agenda

- Why model threats?
- The three types of threat modeling
- Anatomy of a Risk Assessment
- Diving in: Attacker-Centric modeling
- How to integrate into a risk assessment
- Case study: DDOS attack on a non-profit

What is Threat Modeling?

“All models are wrong, but some are useful.”

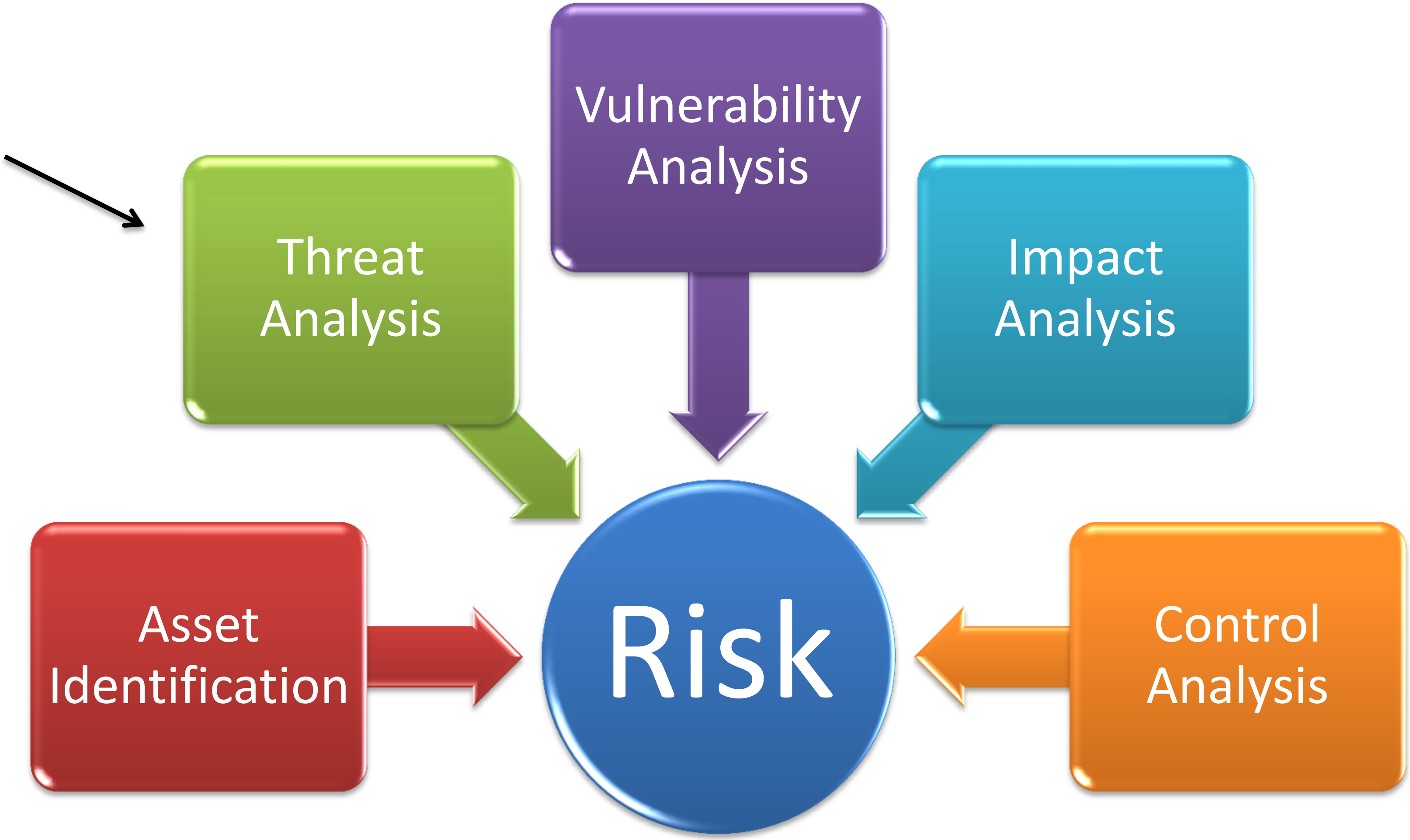
- George Box

Definition

- Looking at an asset and identifying a set of possible attacks and who is capable and willing to carry out the attack

- An essential *component* of risk analysis
  - Not a *replacement* for risk analysis

You're Doing It Already…



Vulnerability Analysis

Threat Analysis

Impact Analysis

Asset Identification

Risk

Control Analysis

In this session

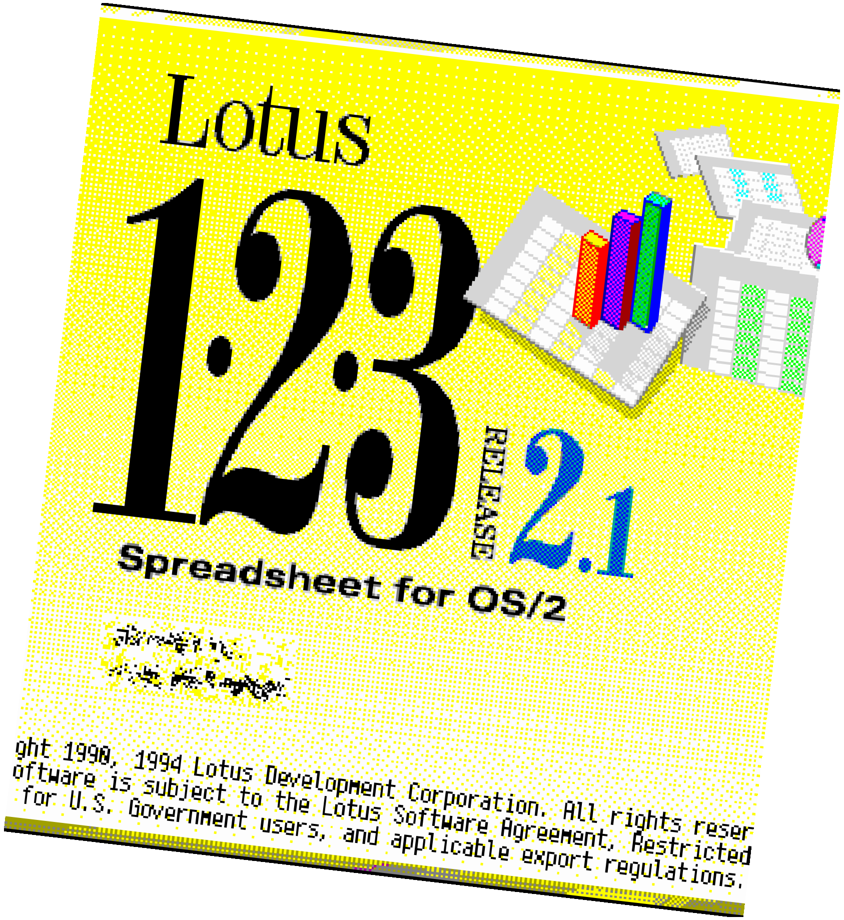
- Build upon what are are already doing
- Speed up the risk assessment process
- Build threat actor profiles and an actor library
- Use the output to feed into risk assessments

3 Types of Modeling

- Software Based
- Asset based
- Attacker based

Software-Centric

- Popularized by Microsoft
- Use during the SDLC to find and remove vulnerabilities at each phase of the development effort
- The goal is to examine software as it is being developed and identify possible attack vectors. This (in theory) results in less vulnerabilities


Lotus
123
RELEASE 2.1
Spreadsheet for OS/2
ght 1990, 1994 Lotus Development Corporation. All rights reser
oftware is subject to the Lotus Software Agreement, Restricted
for U.S. Government users, and applicable export regulations.

Implementations: DREAD, STRIDE, data-flow diagramming

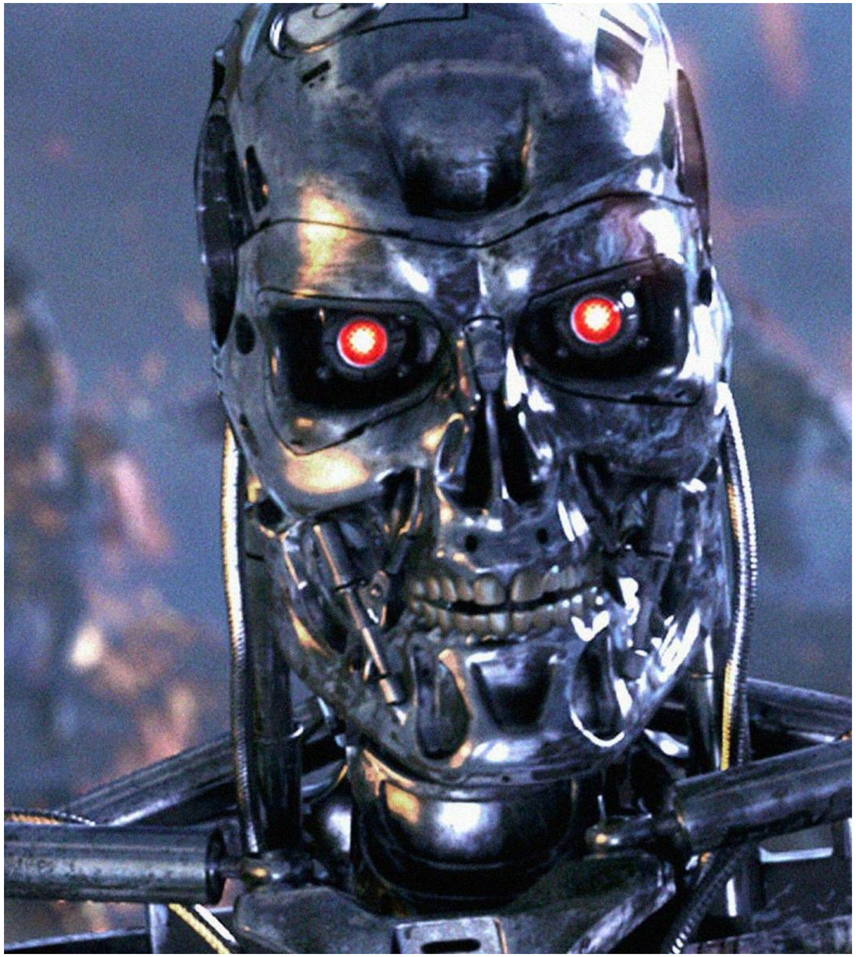
Asset-Centric

- Identifies and defines assets and find the value to an organization
- Focused on finding vulnerabilities and implementing controls commensurate to the value of the asset
- The goal is to produce an assessment that allows for a cost/benefit analysis or ascertaining the cost of controls

Implementations: PASTA, OCTAVE, TRIKE

Attacker-Centric

- Looks at past attacks inside the organization and out
- Looks at methods, objectives, resources, and other data points to build attacker profiles
- The goal is to provide intelligence on how future attacks may progress and communicate present risk.



Implementations: Cyber Kill Chain, Intel's TARA, OODA Loop, Attack Trees

Which One Is Right?

- All of the above methods are useful and are not mutually exclusive; use Software-centric threat modeling during the SDLC

- Attacker-centric versus Asset-Centric threat modeling both occur in the risk assessment process

- Which one you choose depends on which risk assessment methodology you use – NIST and FAIR uses attacker-based threat scenarios

Benefits

Adds credibility to risk assessments

Repeatable, defensible process

Speeds up assessments over time (reusable components & data)

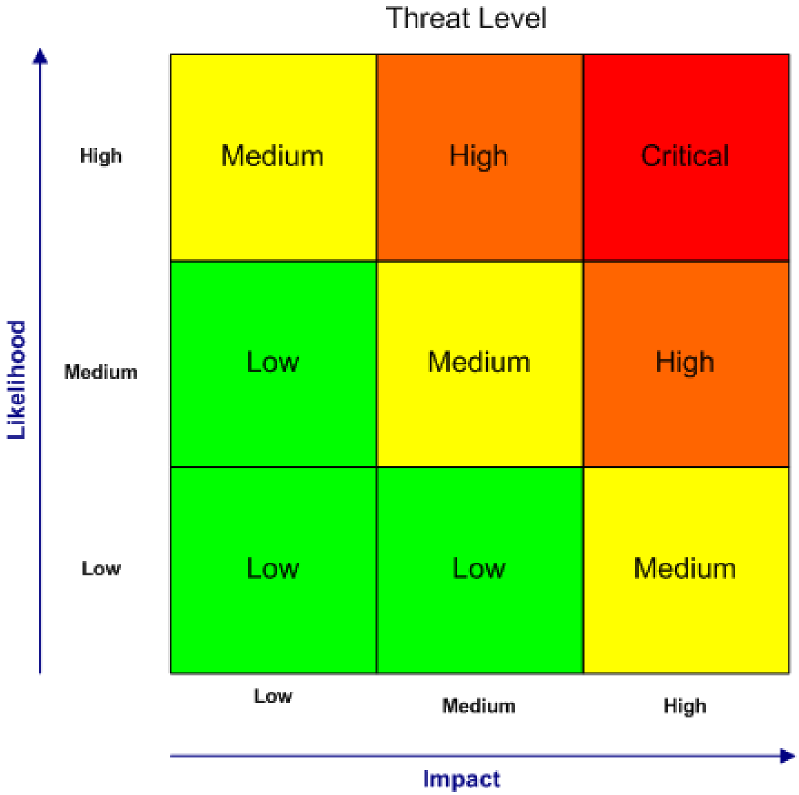
Helps an assessment focus on plausible threats (versus the kitchen sink method)

Anatomy of a Risk Assessment

Anatomy of a Risk Assessment

Basic Risk Calculation

Impact x Likelihood = Risk

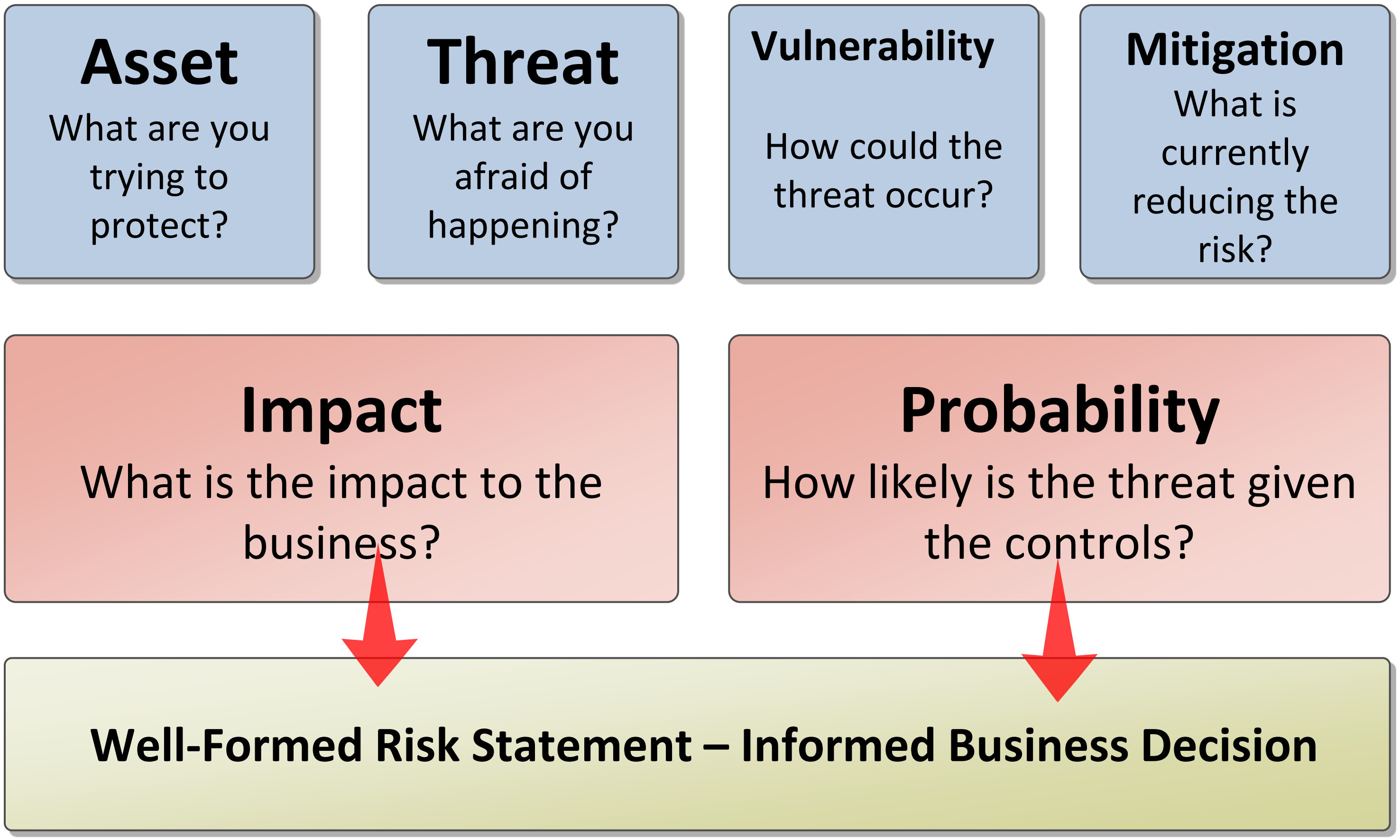


Threat Level

Likelihood \ Impact	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Likelihood
Impact

Individual Components



Asset

What are you trying to protect?

Threat

What are you afraid of happening?

Vulnerability

How could the threat occur?

Mitigation

What is currently reducing the risk?

Impact

What is the impact to the business?

Probability

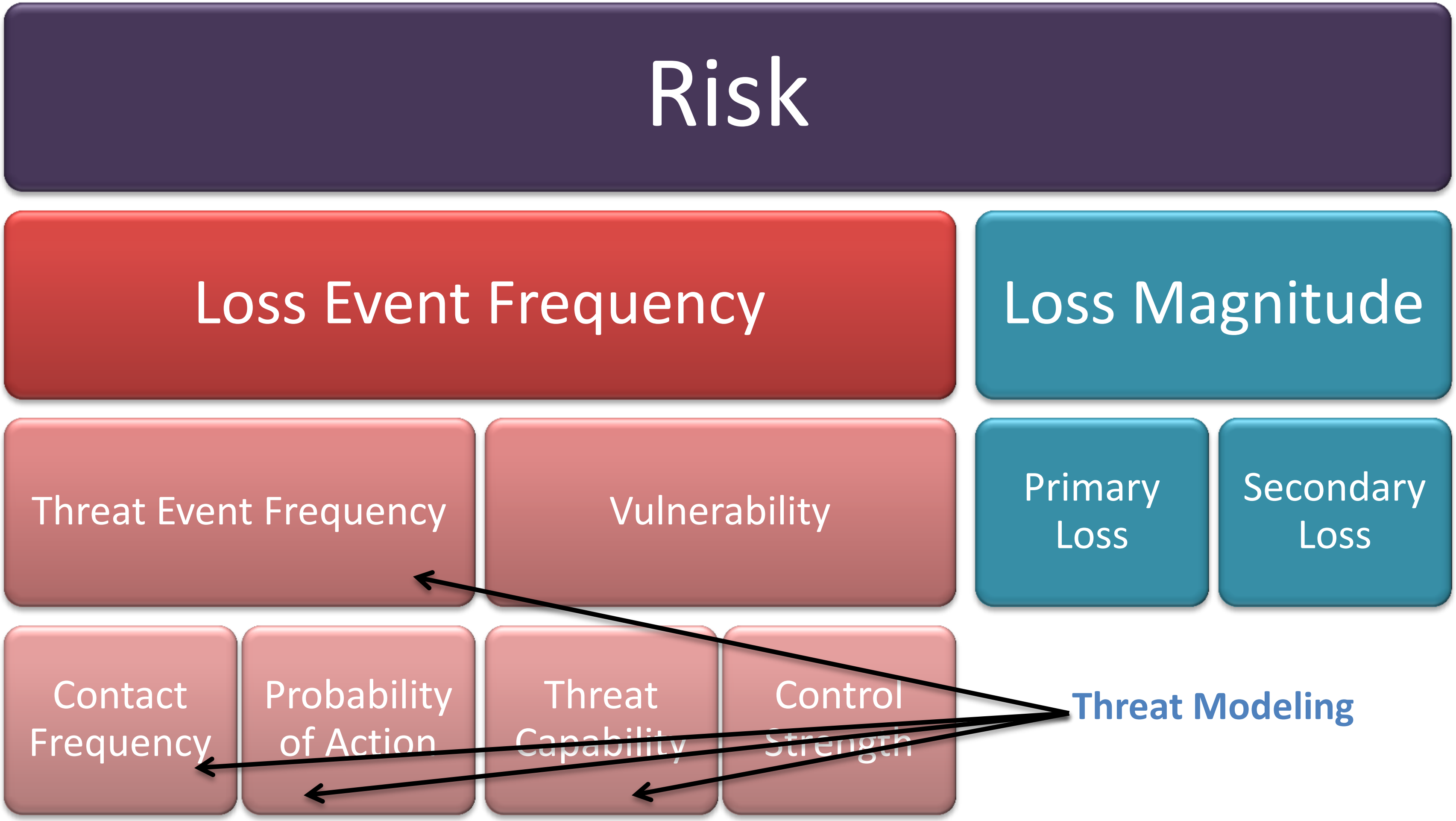
How likely is the threat given the controls?

Well-Formed Risk Statement – Informed Business Decision

Let’s look at how two different risk assessment methodologies model threat agents…

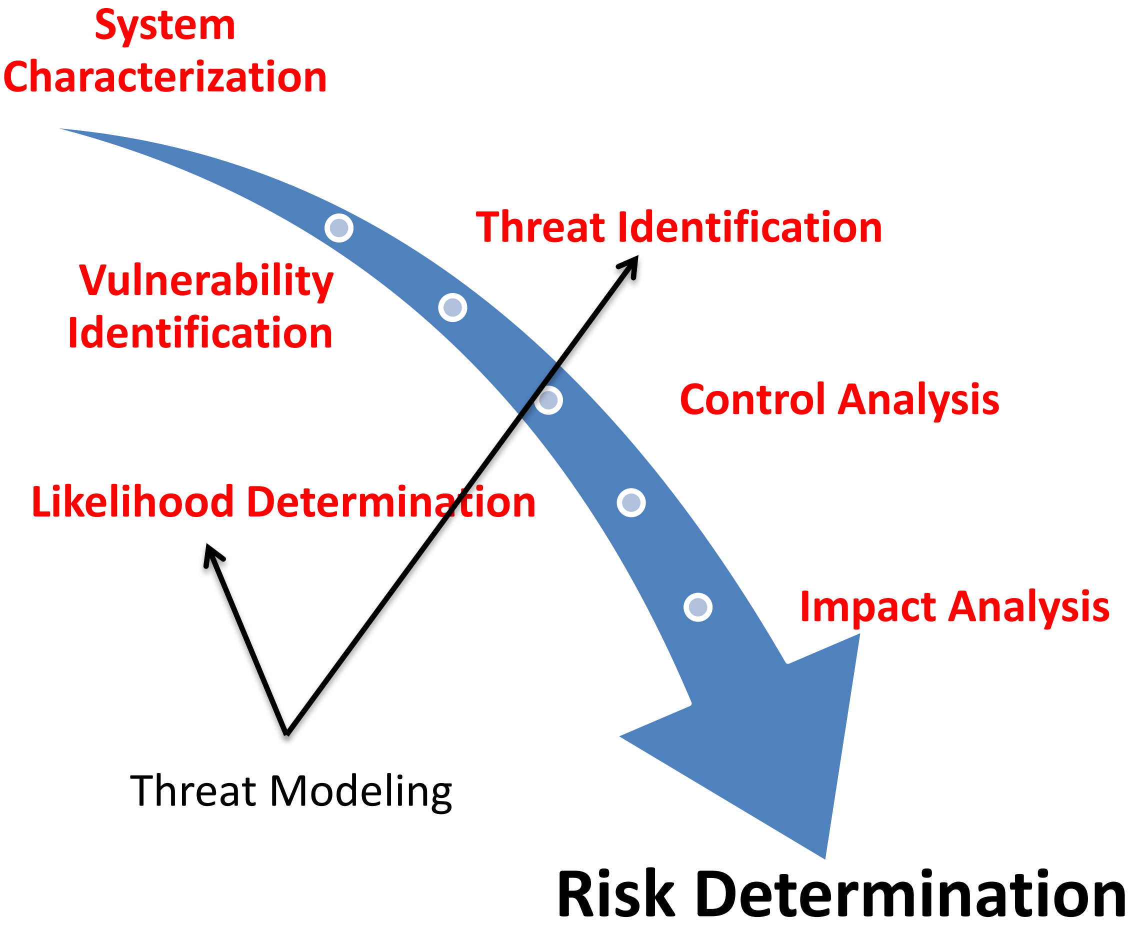
FAIR & NIST

Anatomy of a Risk Assessment - FAIR



Source: *Basic Risk Assessment Guide*; CXOWare; http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf

Anatomy of a Risk Assessment - NIST



System Characterization

Threat Identification

Vulnerability Identification

Control Analysis

Likelihood Determination

Impact Analysis

Threat Modeling

Risk Determination

Source: *Guide For Conducting Risk Assessments*; NIST; http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Anatomy of a Risk Assessment

We’re really good at…

- Finding vulnerabilities (automated tools for this)
- Figuring out the impact (other departments usually have this)
- Knowing what controls to implement (we’re professionals!)

Not so good at

- Understanding the most likely threats to our environment
- Having an idea of a threat’s goal, methods and objectives
- Understanding why the last bullet point is important

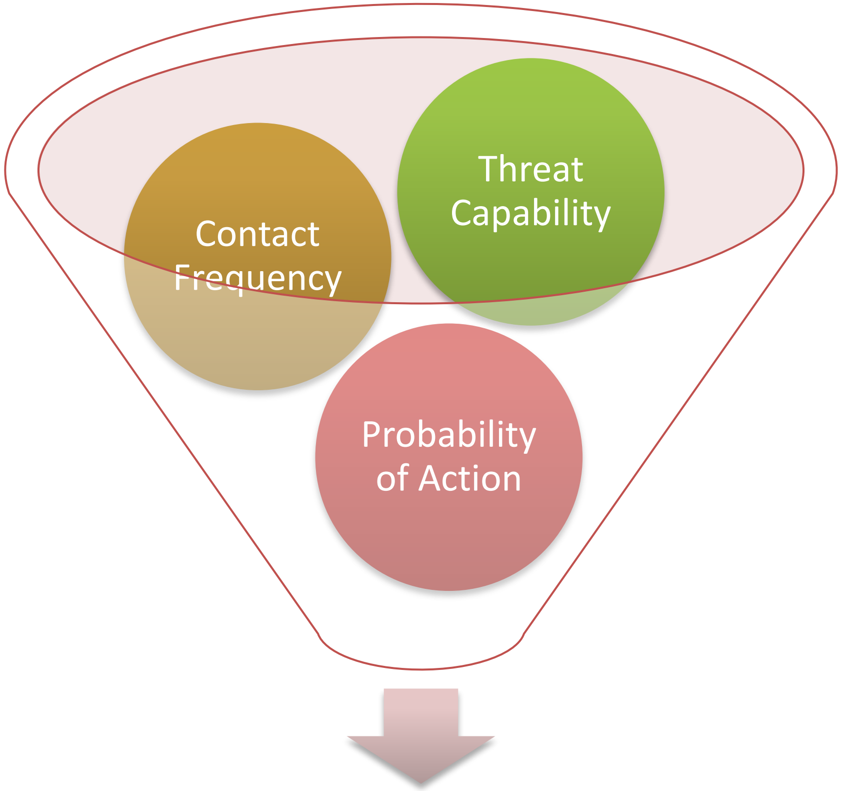
Common Mistakes

- Using a checklist of control objectives
- Using the results of a vulnerability scan
- Not identifying the threat at all

The most common (and most costly mistake) of all…

EVERYTHING'S HIGH RISK

Answers the “probability” question



Contact Frequency

Threat Capability

Probability of Action

Probability of a Loss Event

Diving In

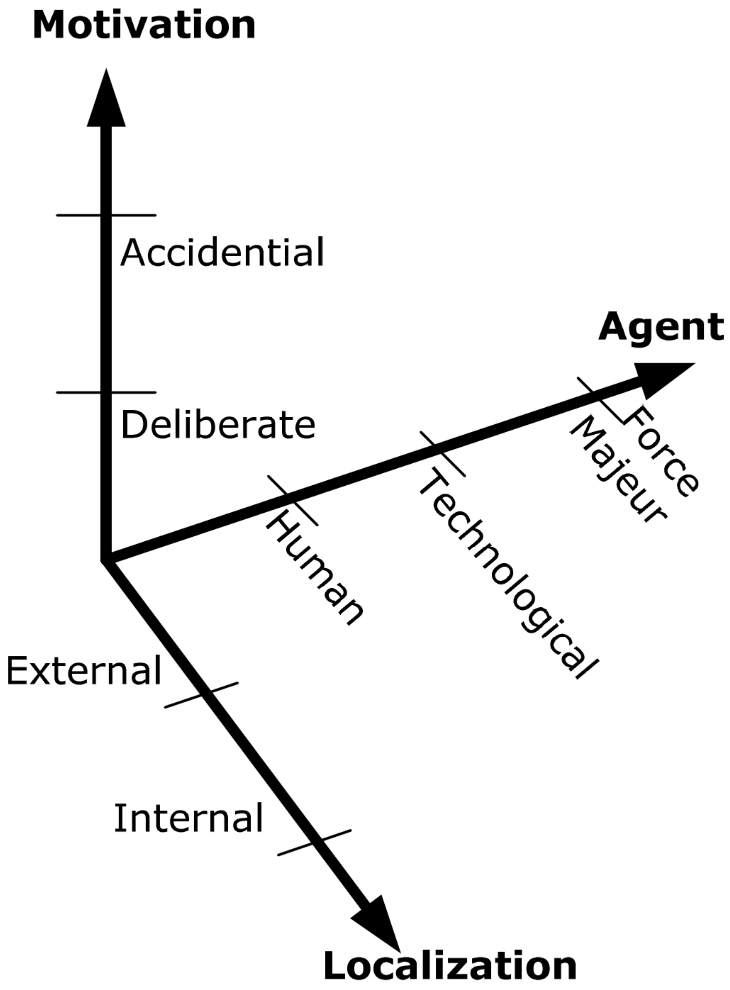
Getting started

- Identify threat agents that are applicable to your company
  - Easiest to use lists that already exist and customize
- Form working committees of SME’s to compile and refine
- Assess threats & create a library
- Focus on issues that other techniques can’t identify
- Sometimes you need to re-invent the wheel to get a better one

Avoid:

- Overdoing it (aim for 20-25 human threat actors max)

Threat Classification Method



- Good starting taxonomy to separate out the major attributes of threat actors
- Pick one attribute from each of the three categories
- We'll pick Human, Deliberate, External

Source: *Threat Modeling in Security Architecture*; ISSS; https://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf

Categories of Threats

Human, Deliberate

- Organized crime
- Hacker
- Competitor
- Disgruntled employee
- etc.

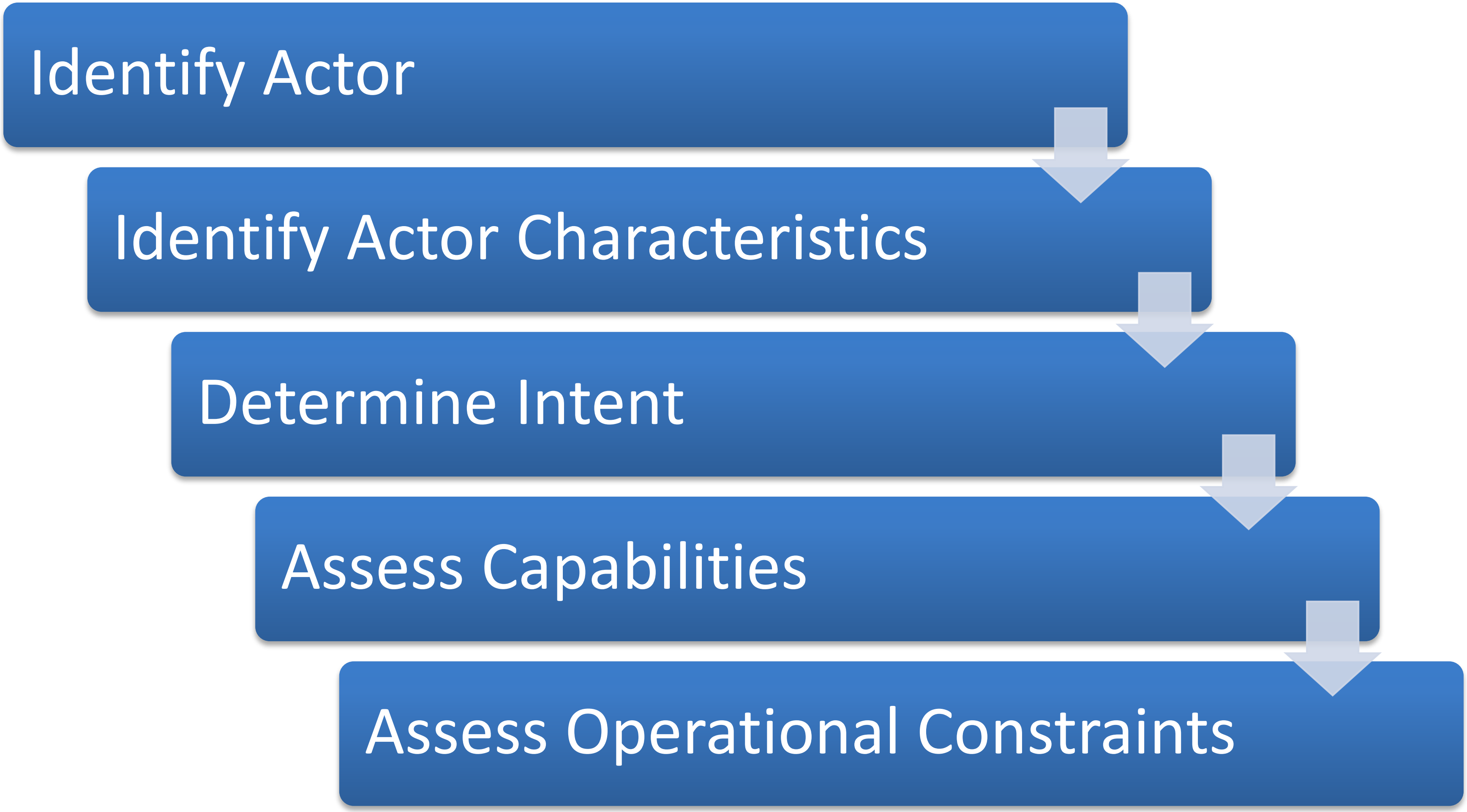
Human, Non-deliberate

- Employee
- Vendor
- Business Partner
- Government Regulator
- etc.

Force Majeure

- Earthquake
- Tornado
- Tsunami
- Hurricane
- etc.

Profile “Human, Deliberate, External”



Identify Actor

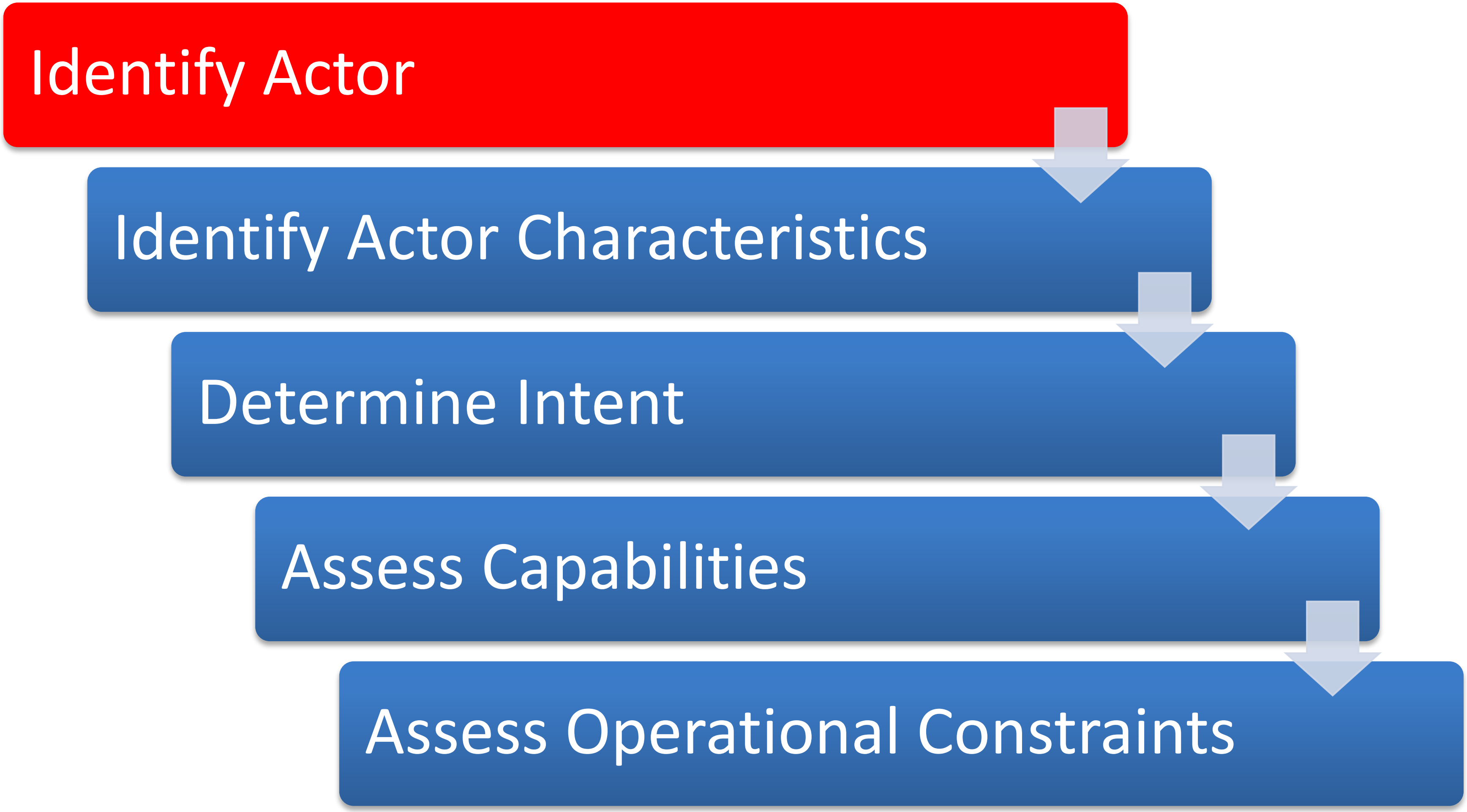
Identify Actor Characteristics

Determine Intent

Assess Capabilities

Assess Operational Constraints

Profile “Human, Deliberate, External”



Identify Actor

Identify Actor Characteristics

Determine Intent

Assess Capabilities

Assess Operational Constraints

Profile “Human, Deliberate, External”

Develop list of agents

Research past activities

Ascertain capabilities

Ascertain intentions

Do I have to develop my own list?

It’s up to you, but I wouldn’t

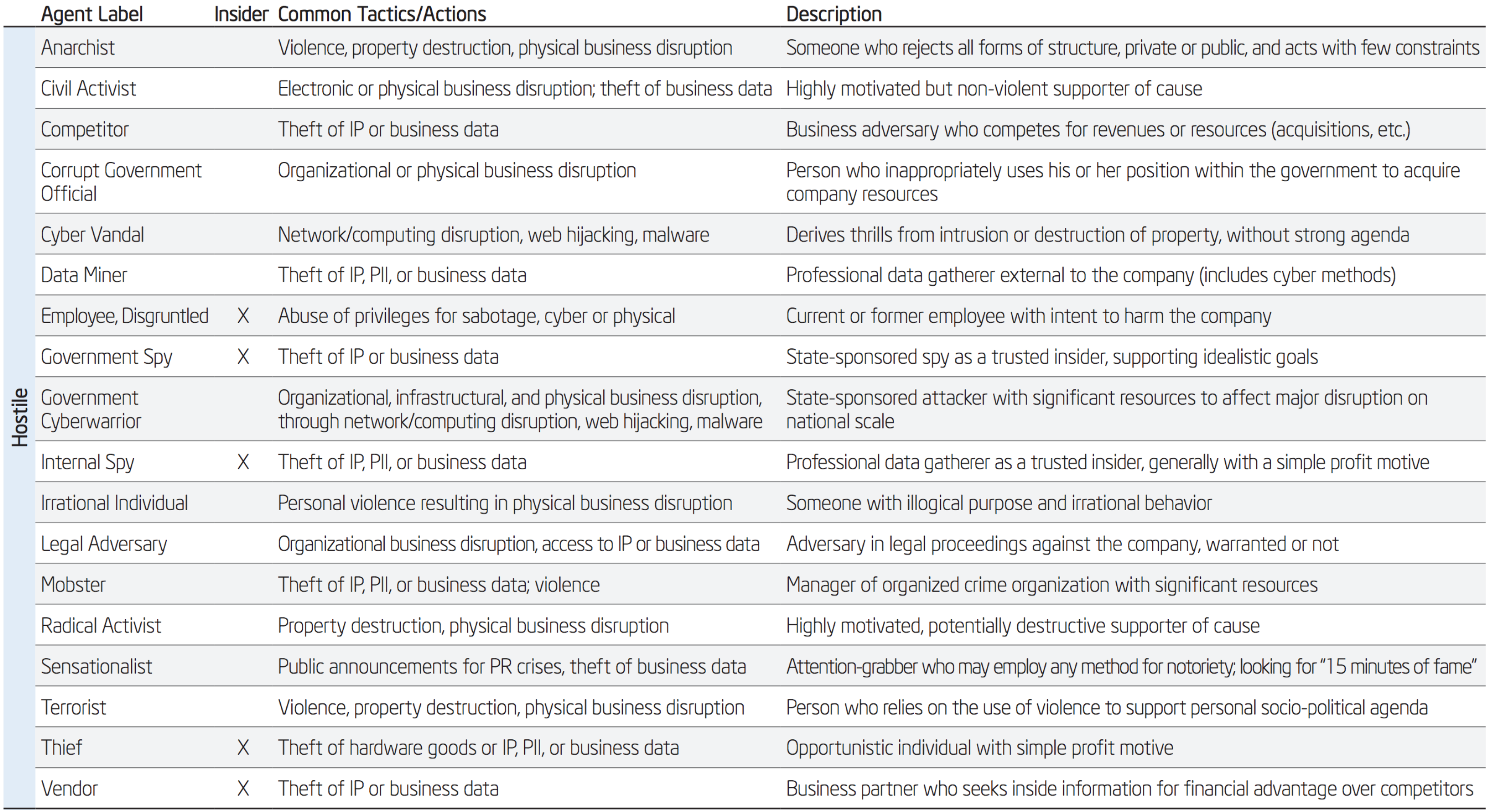
Develop a list

- Internal metrics
- Threat intelligence
- Business partners
- Attack trees

Use a list

- OWASP
- Intel
- Homeland Security

Intel’s TARA



	Agent Label	Insider	Common Tactics/Actions	Description
Hostile	Anarchist		Violence, property destruction, physical business disruption	Someone who rejects all forms of structure, private or public, and acts with few constraints
	Civil Activist		Electronic or physical business disruption; theft of business data	Highly motivated but non-violent supporter of cause
	Competitor		Theft of IP or business data	Business adversary who competes for revenues or resources (acquisitions, etc.)
	Corrupt Government Official		Organizational or physical business disruption	Person who inappropriately uses his or her position within the government to acquire company resources
	Cyber Vandal		Network/computing disruption, web hijacking, malware	Derives thrills from intrusion or destruction of property, without strong agenda
	Data Miner		Theft of IP, PII, or business data	Professional data gatherer external to the company (includes cyber methods)
	Employee, Disgruntled	X	Abuse of privileges for sabotage, cyber or physical	Current or former employee with intent to harm the company
	Government Spy	X	Theft of IP or business data	State-sponsored spy as a trusted insider, supporting idealistic goals
	Government Cyberwarrior		Organizational, infrastructural, and physical business disruption, through network/computing disruption, web hijacking, malware	State-sponsored attacker with significant resources to affect major disruption on national scale
	Internal Spy	X	Theft of IP, PII, or business data	Professional data gatherer as a trusted insider, generally with a simple profit motive
	Irrational Individual		Personal violence resulting in physical business disruption	Someone with illogical purpose and irrational behavior
	Legal Adversary		Organizational business disruption, access to IP or business data	Adversary in legal proceedings against the company, warranted or not
	Mobster		Theft of IP, PII, or business data; violence	Manager of organized crime organization with significant resources
	Radical Activist		Property destruction, physical business disruption	Highly motivated, potentially destructive supporter of cause
	Sensationalist		Public announcements for PR crises, theft of business data	Attention-grabber who may employ any method for notoriety; looking for "15 minutes of fame"
	Terrorist		Violence, property destruction, physical business disruption	Person who relies on the use of violence to support personal socio-political agenda
	Thief	X	Theft of hardware goods or IP, PII, or business data	Opportunistic individual with simple profit motive
	Vendor	X	Theft of IP or business data	Business partner who seeks inside information for financial advantage over competitors

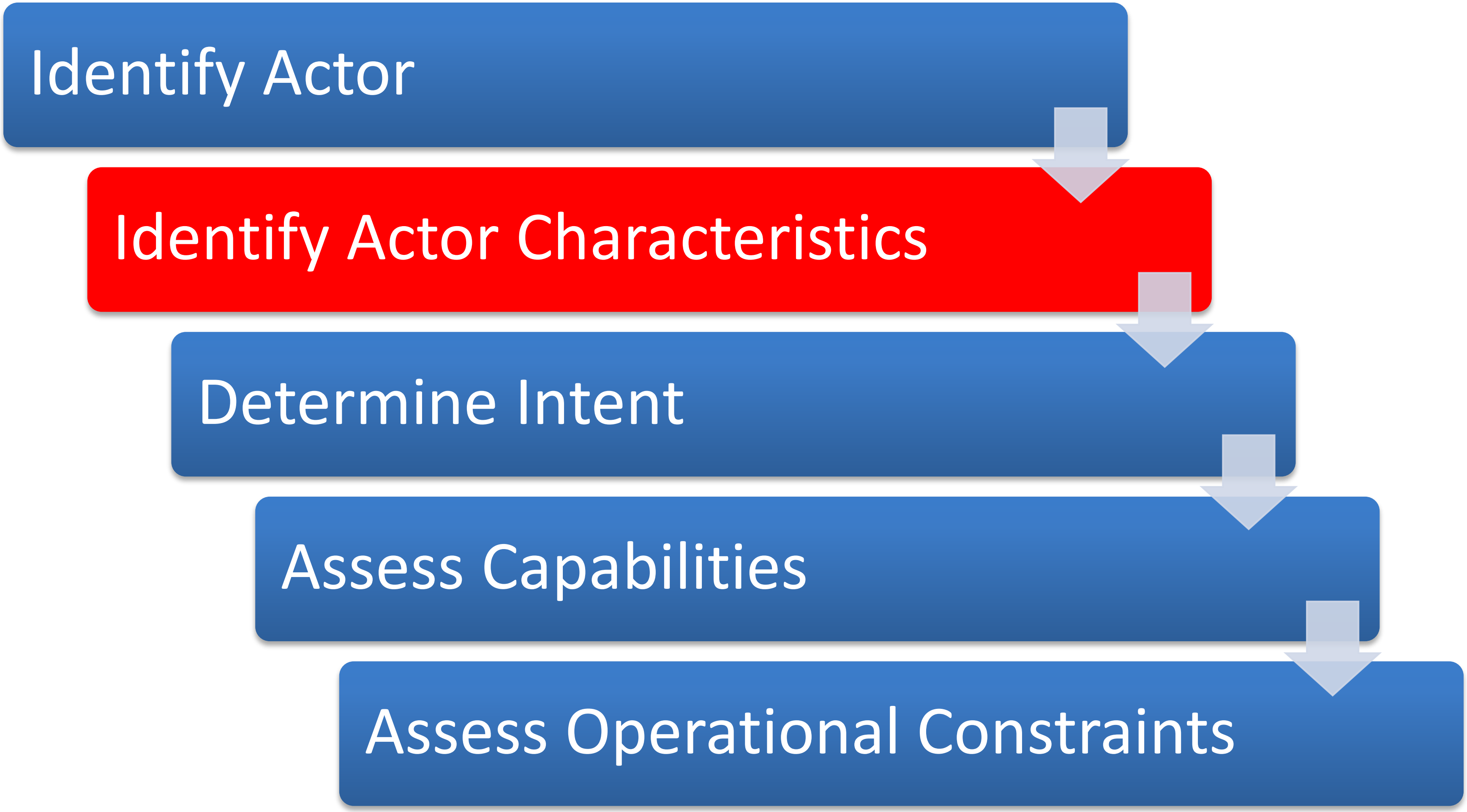
Source: *Prioritizing Information Security Risks With Threat Agent Risk Assessment*; Intel; https://communities.intel.com/community/itpeernetwork/blog/2010/01/05/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment

Let’s Pick “Cyber Vandal”

“Derives thrills from intrusion or destruction of property, without strong agenda.”

Source: *Prioritizing Information Security Risks With Threat Agent Risk Assessment*; Intel; https://communities.intel.com/community/itpeernetwork/blog/2010/01/05/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment

Profile “Human, Deliberate, External”



Identify Actor

Identify Actor Characteristics

Determine Intent

Assess Capabilities

Assess Operational Constraints

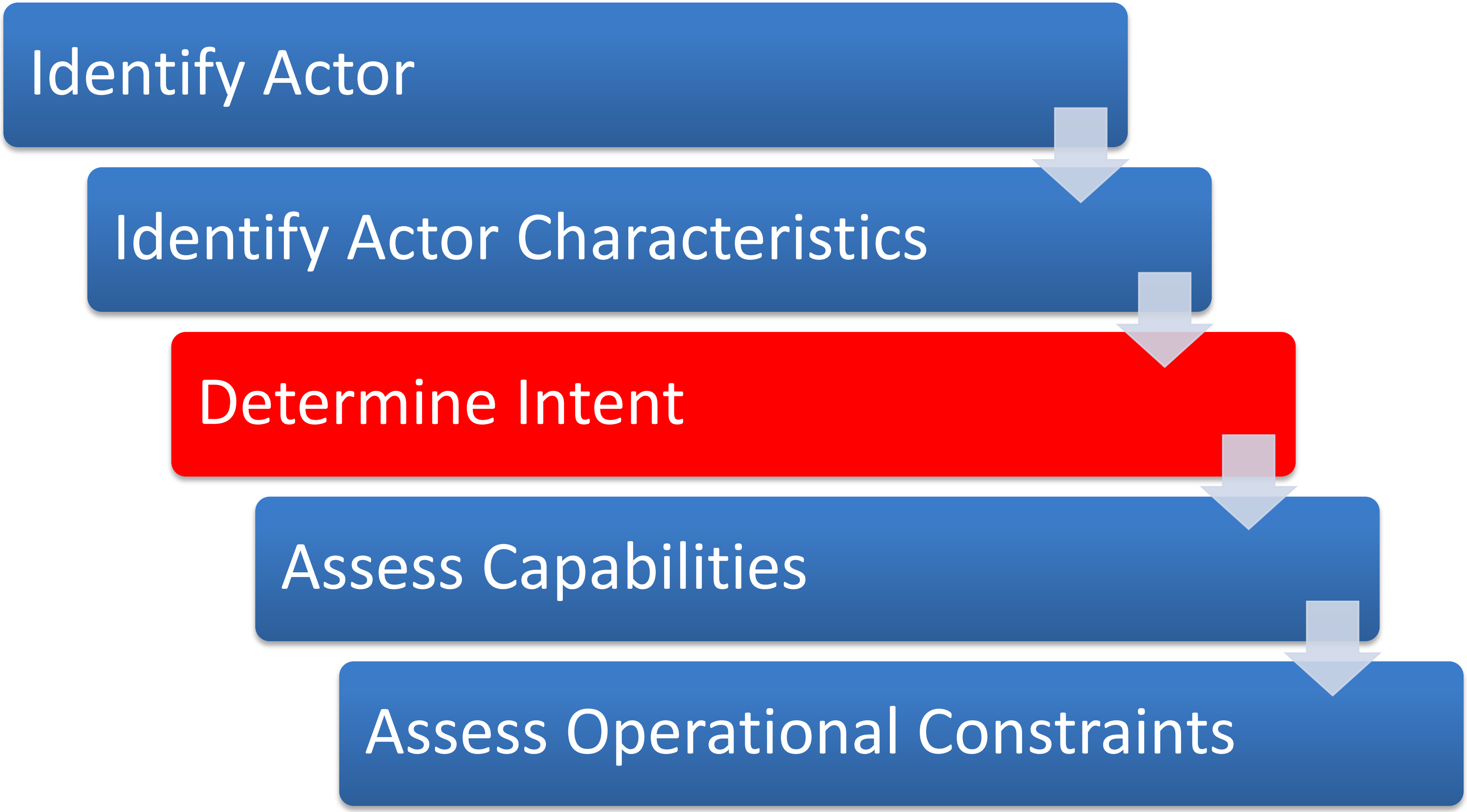
Actor Characteristics

- External (versus insider)
- Not a strong agenda or motivation
- Uses network/computing disruption, malware and web hijacking

Gather Intelligence

- We know (from TARA) a basic description, common tactics & actions and that they are external
- Meet with internal SME’s
- Examine external data (ISAC’s, VZ DBIR, etc.)

Profile “Human, Deliberate, External”



Identify Actor

Identify Actor Characteristics

Determine Intent

Assess Capabilities

Assess Operational Constraints

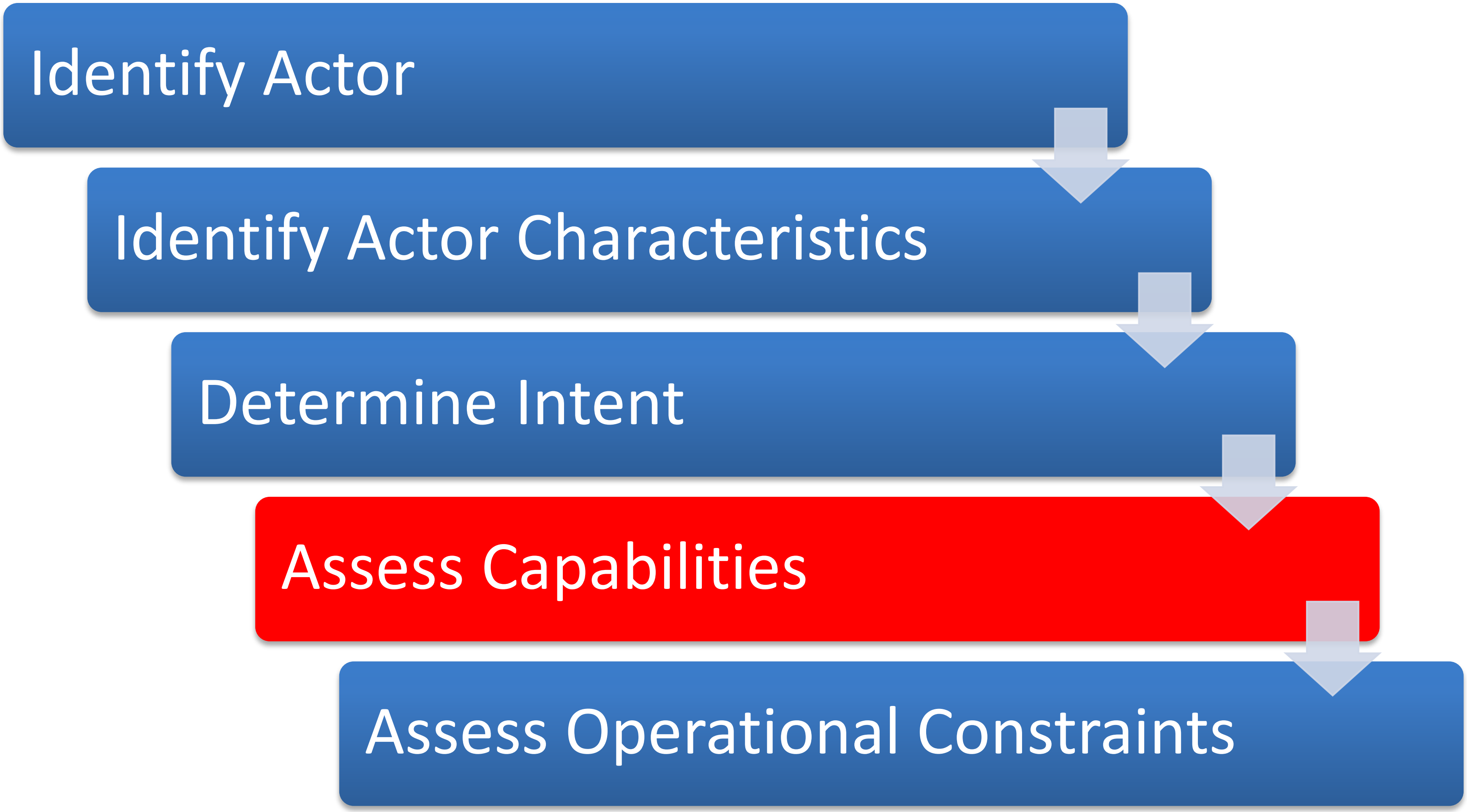
Objective

- Power Projection
- Political Pressure
- Obstruction
- Deception
- Intelligence Gathering
- Counterintelligence
- Financial Gain
- Amusement
- Gratuitous Defacement or Damage
- Advocacy

Intended Outcome

- Acquisition/Theft
- Damage
- Embarrassment
- Gratuitous Defacement

Profile “Human, Deliberate, External”



Identify Actor

Identify Actor Characteristics

Determine Intent

Assess Capabilities

Assess Operational Constraints

Resources

- Government
- Organization

Vast resources, highly organized and motivated

- Team
- Contest

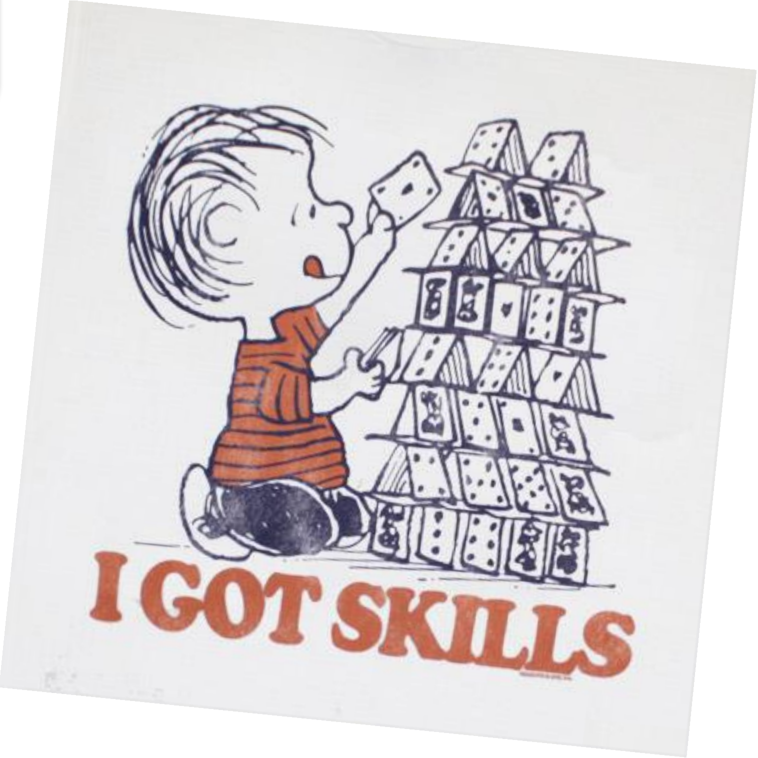
Semi-formal organization with a leader; persists long term; may be organized around an objective

- Club
- Individual

Average individual or small group acting independently

Skills

- Adept
- Operational
- Minimal
- None

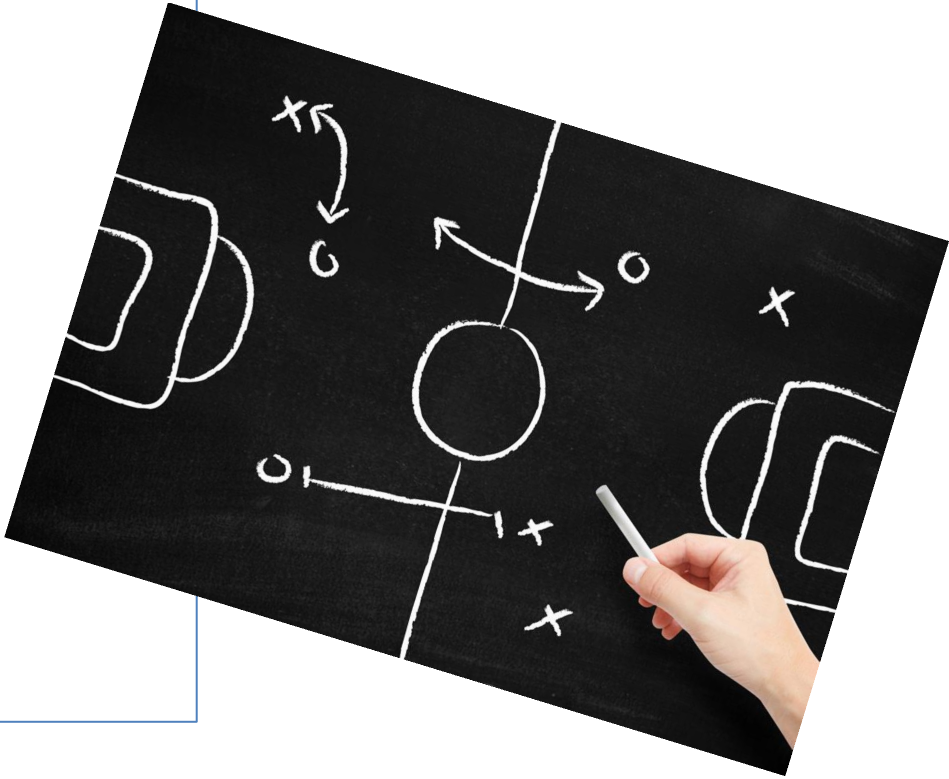


Funding

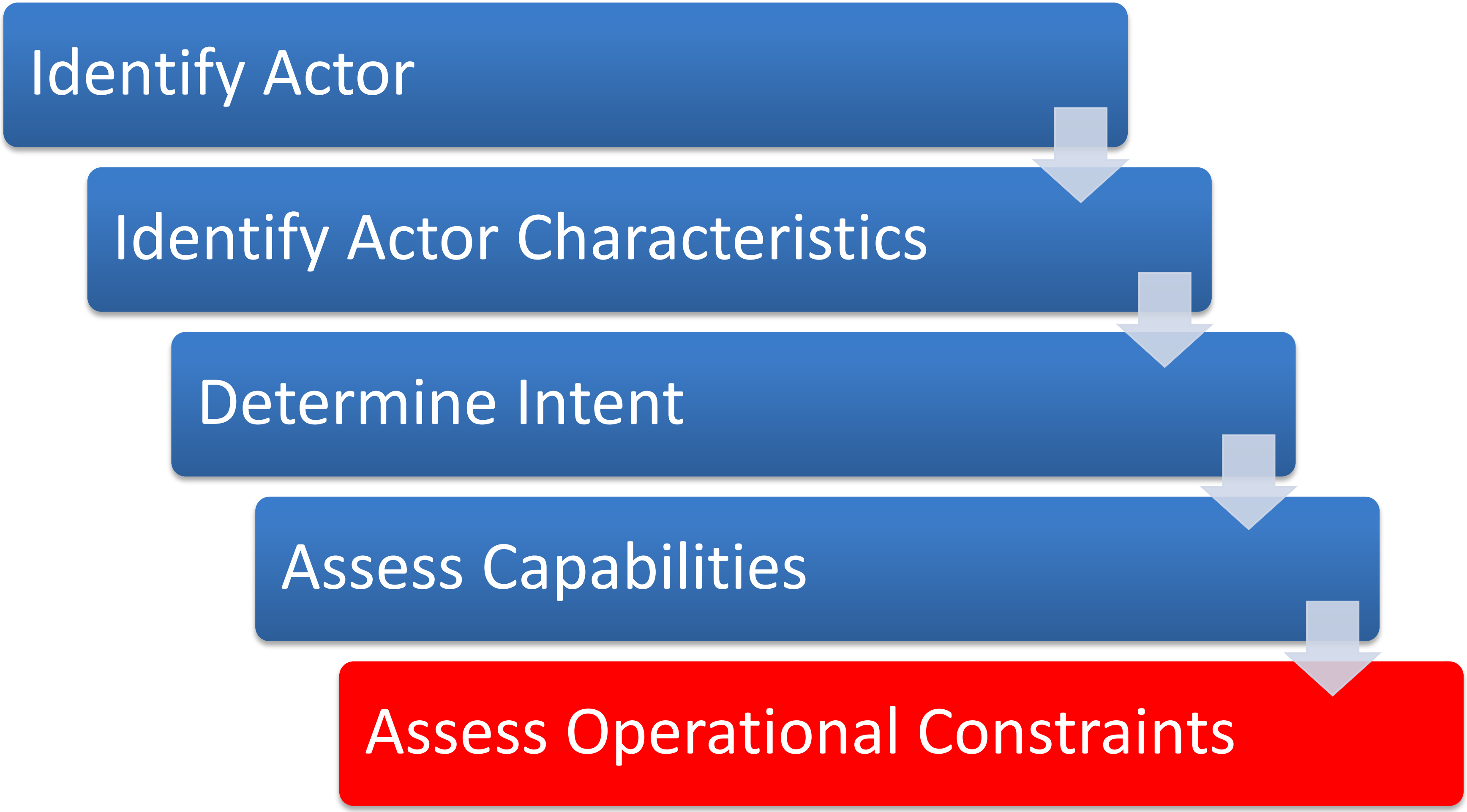
- Unlimited (> $5 million)
- Significant ($500k - $5 mil)
- Limited ($5,000 - $500k)
- No Funding (< $5,000)

Tactical Means

- Copy
- Deny
- Destroy (includes death)
- Degrade/injure
- Take
- Exploit
- Does not care



Profile “Human, Deliberate, External”



Identify Actor

Identify Actor Characteristics

Determine Intent

Assess Capabilities

Assess Operational Constraints

Visibility

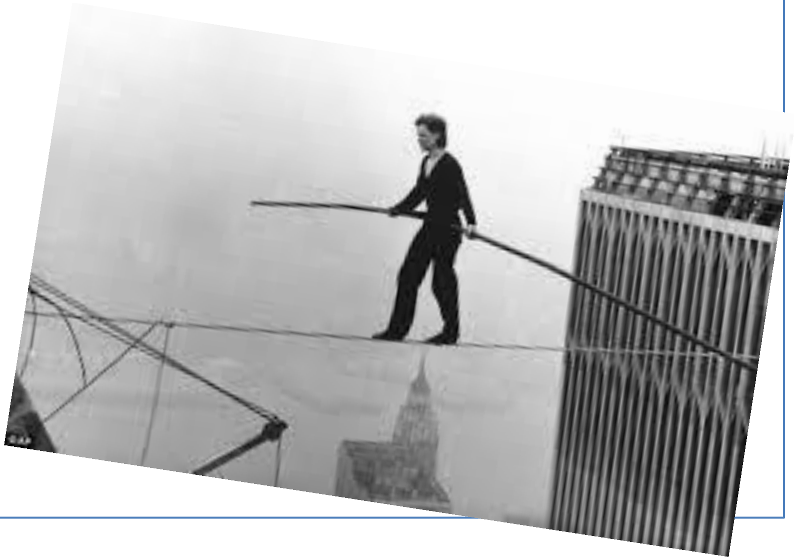
- Covert
- Overt
- Clandestine
- Unknown
- Does not care

Moral Limits

- None
- Unknown
- Illegal, major
- Illegal, minor
- Legal
- Code of Conduct

Personal Risk Tolerance

- High / Does not care
- Medium
- Low (Not a risk taker)

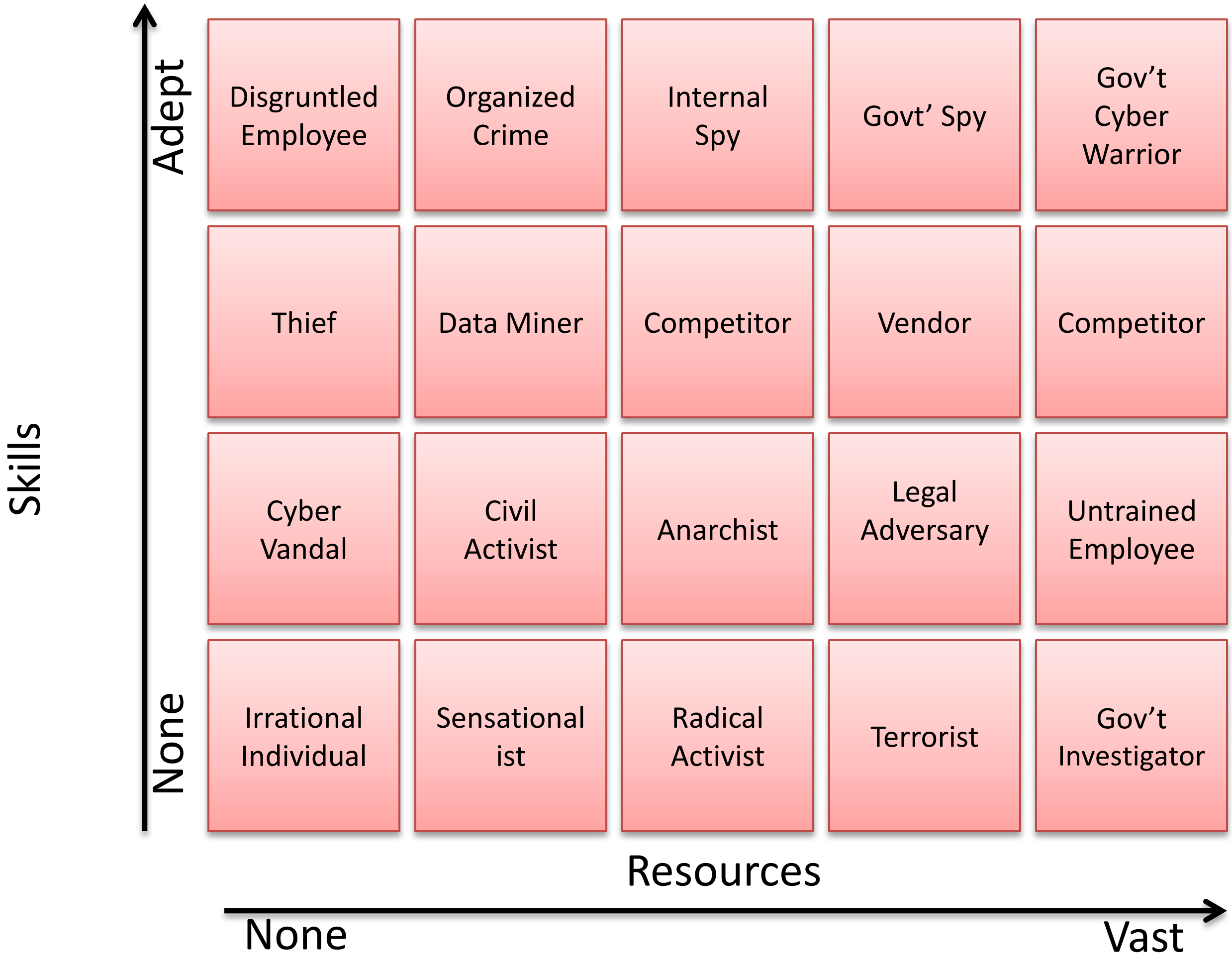


Cyber Vandal

Derives thrills from intrusion or destruction of property, without strong agenda

Characteristics	• **Human**, **external actor** • Uses network/computing disruption, malware and web hijacking
Objective	• **Amusement** – Perform for enjoyment • **Gratuitous Defacement or Damage** - Disfigure or impair the usefulness
Resources	• **Club** - Members interact on a social and volunteer basis and often have little personal interest towards a specific target • **Individual** - Average person who acts independently • **Contest** - Short-lived and perhaps anonymous interaction that concludes when single objective is complete
Skills	• **Minimal** - Can copy and use existing techniques
Funding	• **None** – Less than $5,000
Tactical Means	• **Degrade/Injure** – People or functions are damaged, but still in the company's possession providing only limited functionality or value • **Deny** – Affect the company's ability to use people, processes or technology • **None** - The actor does not have a rational plan, or, may make a choice to opportunistically cause an incident
Visibility	• **Overt** – The actor's identity and attack intentionally become obvious before or at the time of execution • **Does Not Care** - The actor does not have a rational plan, may make a choice opportunistically at the time of attack, or may not place importance on secrecy
Moral limits	• **Illegal**, minor
Personal Risk Tolerance	• **Medium** – Willing to take some personal risk

A Picture Starts to Emerge…



Skills

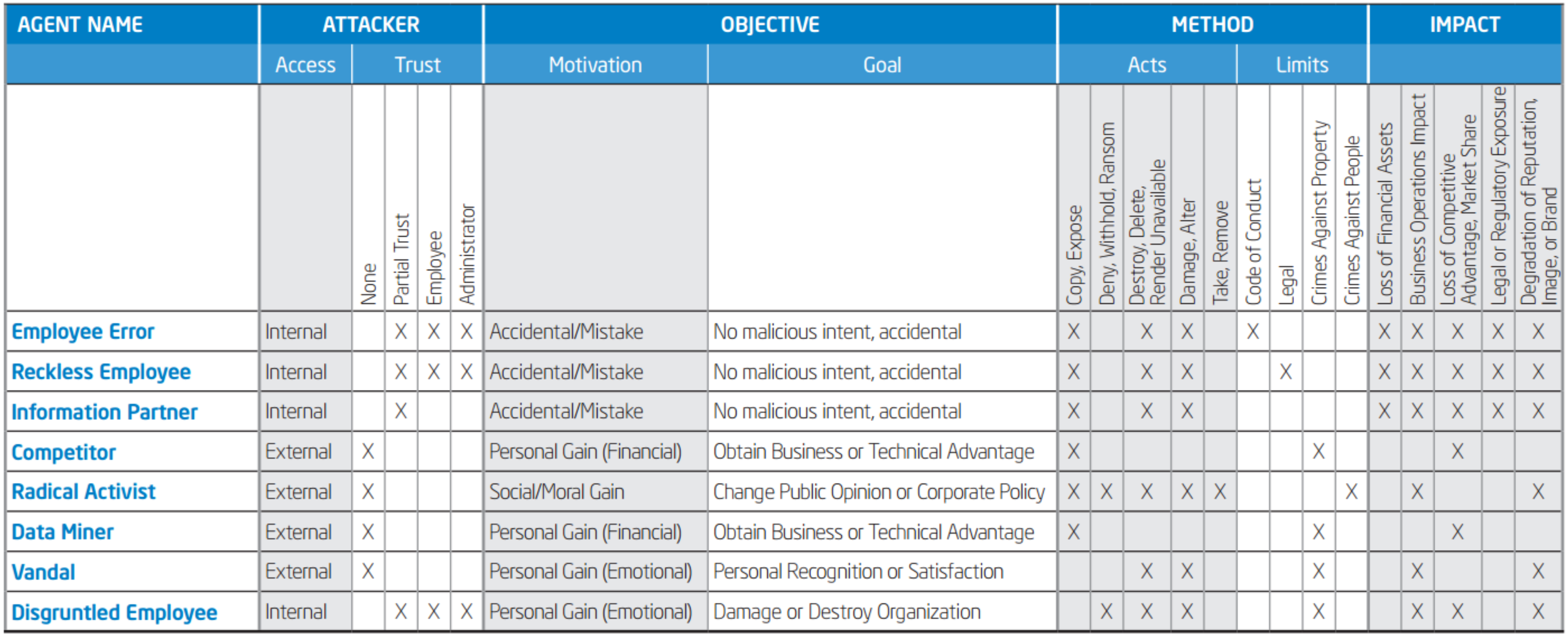
Adept	Disgruntled Employee	Organized Crime	Internal Spy	Govt’ Spy	Gov’t Cyber Warrior
	Thief	Data Miner	Competitor	Vendor	Competitor
	Cyber Vandal	Civil Activist	Anarchist	Legal Adversary	Untrained Employee
None	Irrational Individual	Sensational ist	Radical Activist	Terrorist	Gov’t Investigator

Resources

None

Vast

Or, Compile by Methods and Objectives

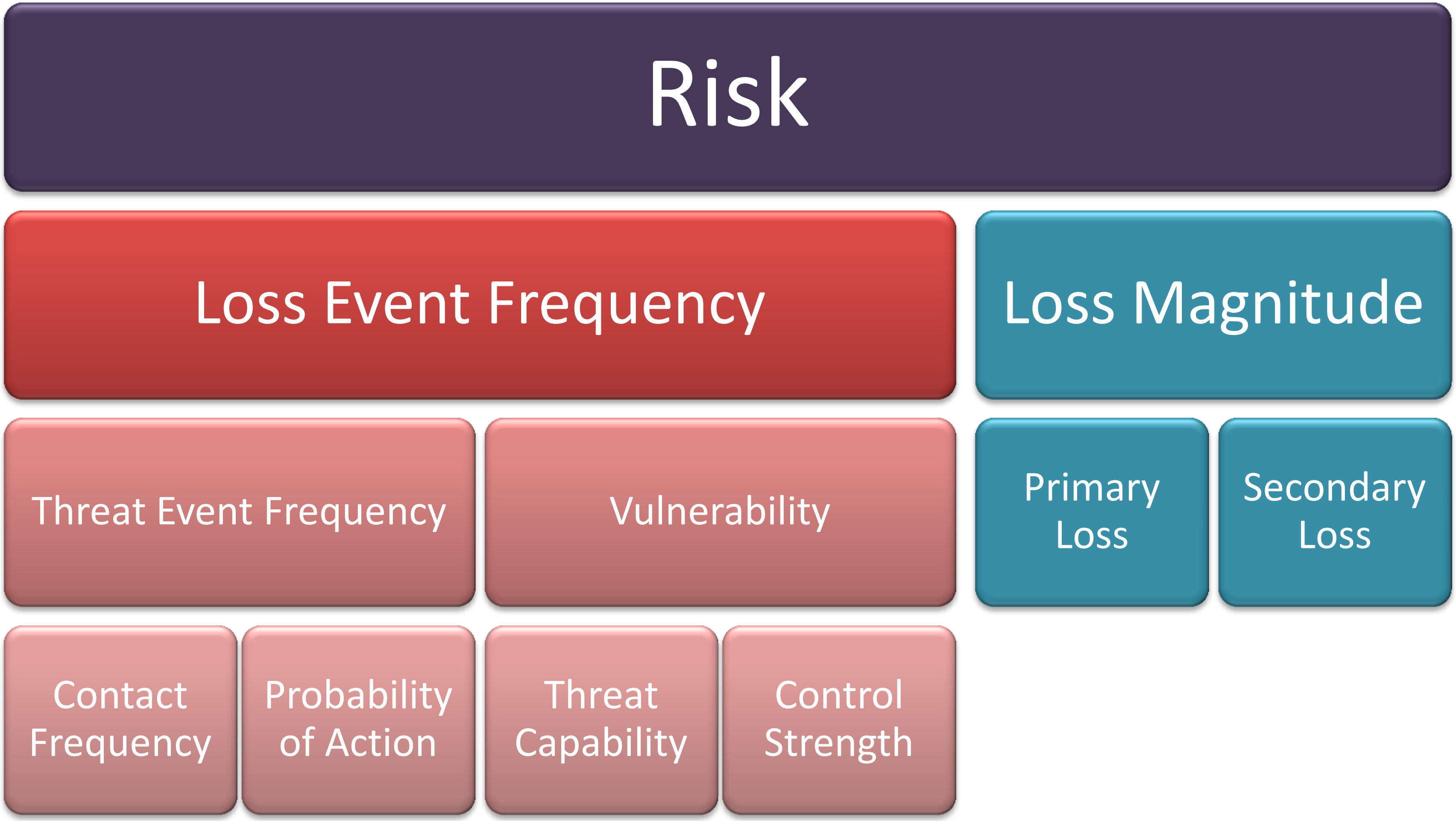


AGENT NAME	ATTACKER					OBJECTIVE		METHOD									IMPACT				
	Access	Trust				Motivation	Goal	Acts					Limits								
		None	Partial Trust	Employee	Administrator			Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Code of Conduct	Legal	Crimes Against Property	Crimes Against People	Loss of Financial Assets	Business Operations Impact	Loss of Competitive Advantage, Market Share	Legal or Regulatory Exposure	Degradation of Reputation, Image, or Brand
Employee Error	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X		X				X	X	X	X	X
Reckless Employee	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X			X			X	X	X	X	X
Information Partner	Internal		X			Accidental/Mistake	No malicious intent, accidental	X		X	X						X	X	X	X	X
Competitor	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Radical Activist	External	X				Social/Moral Gain	Change Public Opinion or Corporate Policy	X	X	X	X	X				X		X			X
Data Miner	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Vandal	External	X				Personal Gain (Emotional)	Personal Recognition or Satisfaction			X	X				X			X			X
Disgruntled Employee	Internal		X	X	X	Personal Gain (Emotional)	Damage or Destroy Organization		X	X	X				X			X	X		X

Source: *Prioritizing Information Security Risks With Threat Agent Risk Assessment*; Intel; https://communities.intel.com/community/itpeernetwork/blog/2010/01/05/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment

Integrating Into Risk Assessments

Anatomy of a Risk Assessment - FAIR



Risk

Loss Event Frequency

Loss Magnitude

Threat Event Frequency

Vulnerability

Primary Loss

Secondary Loss

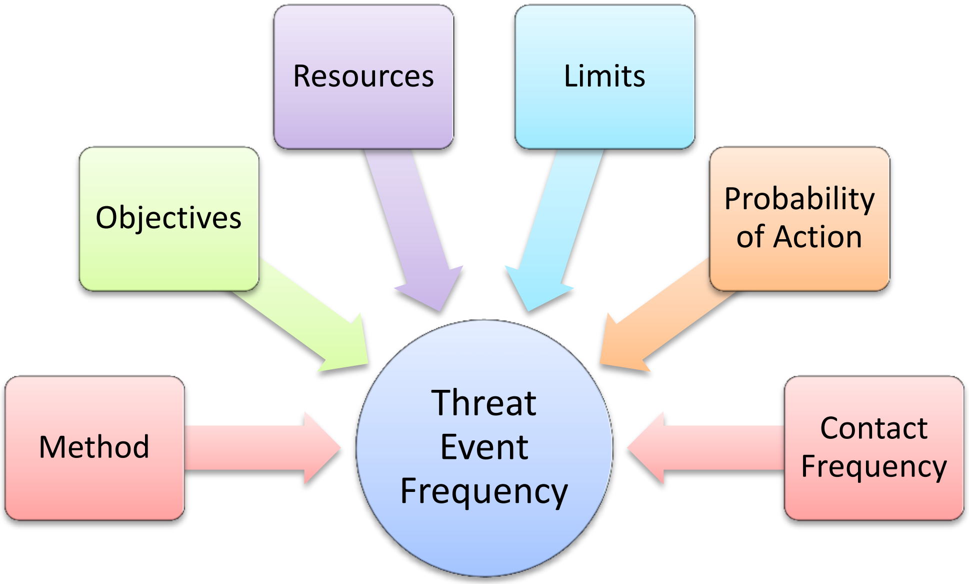
Contact Frequency

Probability of Action

Threat Capability

Control Strength

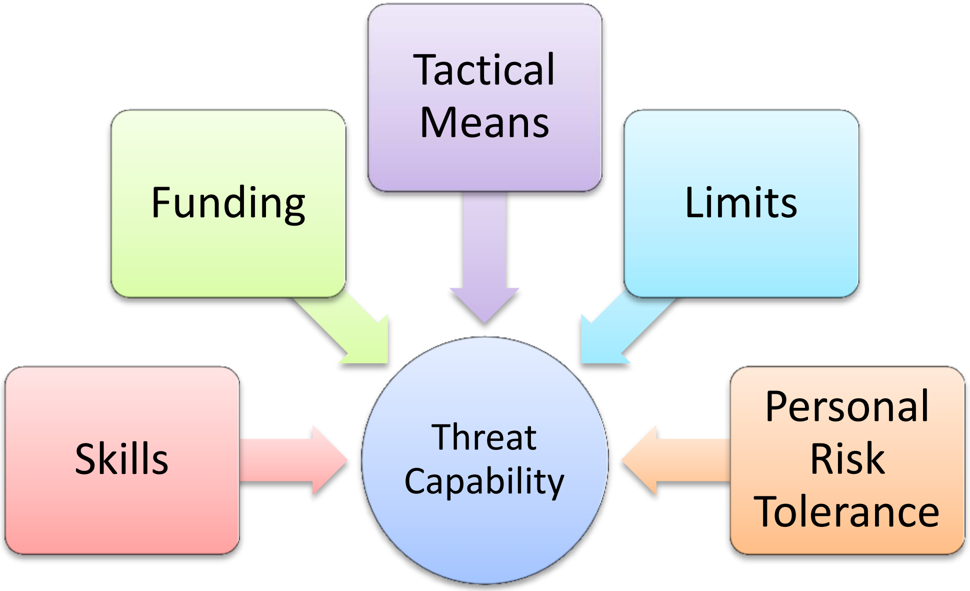
Inputs – Threat Event Frequency



Threat Event Frequency

> 100x/year
10-100x/year
1-10x/year
.1-1x/year
<.1x/year

Inputs – Threat Capability



Threat Capability

Top 2%
Top 16%
Average skill and resources
Bottom 16%
Bottom 2%

Case Study

Case Study

- San Francisco-based, medium sized non-profit
- Does not sell anything, but accepts online donations
- Primary content on the website is opinion pieces, fact pages and several blogs

Scenario

- Management is concerned about Distributed Denial of Service attacks from cyber protest groups and activists
- Several successful attempts in the past

Project:

- Determine the level of risk associated with a denial of service attack against the non-profit's public facing website

Scope

Step 1: Identify assets at risk, relevant threat agents and the effect

Asset	Threat Agent	Effect
Client transactions (donations)	Cyber Vandal	Availability
Client transactions (donations)	Radical Activist	Availability

Reference Threat Agent Library

Step 2: Pull threat agents out of the pre-built library

Review and update, if necessary

Cyber Vandal

Derives thrills from intrusion or destruction of property, without strong agenda

Characteristics	• **Human**, **external actor** • Uses network/computing disruption, malware and web hijacking
Objective	• **Amusement** – Perform for enjoyment • **Gratuitous Defacement or Damage** - Disfigure or impair the usefulness
Resources	• **Club** - Members interact on a social and volunteer basis and often have little personal interest towards a specific target • **Individual** - Average person who acts independently • **Contest** - Short-lived and perhaps anonymous interaction that concludes when single objective is complete
Skills	• **Minimal** - Can copy and use existing techniques
Funding	• **None** – Less than $5,000
Tactical Means	• **Degrade/Injure** – People or functions are damaged, but still in the company's possession providing only limited functionality or value • **Deny** – Affect the company's ability to use people, processes or technology • **None** - The actor does not have a rational plan, or, may make a choice to opportunistically cause an incident
Visibility	• **Overt** – The actor's identity and attack intentionally become obvious before or at the time of execution • **Does Not Care** - The actor does not have a rational plan, may make a choice opportunistically at the time of attack, or may not place importance on secrecy
Moral limits	• **Illegal**, minor – Relatively minor, non-violent transgressions can occur, such as vandalism or trespass
Personal Risk Tolerance	• **Medium** – Willing to take some personal risk

Radical Activist

Highly motivated, potentially destructive supporter of a cause

Characteristics	• **Human**, **external actor** • Property destruction, business disruption (physical & electronic)
Objective	• **Advocacy** – Plead or argue in favor of a cause, idea or policy • **Obstruction** - Cause a delay in the conduct of business • **Gratuitous Defacement or Damage** - Disfigure or impair the usefulness
Resources	• **Organization** – Private, larger and better resourced than a Club; similar structure as a Company (strong leadership and defined objectives). Usually with multiple geographies and persists long-term. • **Club** - Members interact on a social and volunteer basis and often have little personal interest towards a specific target
Skills	• **Operational** – Understands the underlying technology, tools and methods and can create new attacks within a narrow domain.
Funding	• **Limited Funding** - $5,000 - $500,000
Tactical Means	• **Destroy (includes death)** – People, processes or technology are destroyed and of no utility or value to the Company or to the actor. • **Degrade/Injure** – People or functions are damaged, but still in the company’s possession providing only limited functionality or value • **Deny** – Affect the company’s ability to use people, processes or technology
Visibility	• **Overt** – The actor’s identity and attack intentionally become obvious before or at the time of execution • **Does Not Care** - The actor does not have a rational plan, may make a choice opportunistically at the time of attack, or may not place importance on secrecy
Moral limits	• **Illegal**, major – No account is taken of the law; felonious behavior up to and including significant financial impact and extreme violence
Personal Risk Tolerance	• **Medium** – Willing to take some personal risk

Start the Risk Assessment

- We’ve scoped the project, identified assets and have enough information on the threat agents to get started.

- We’ll use FAIR for the assessment, but you can use any other framework you want. All risk frameworks use threat scenarios to help determine likelihood.

Step 3: Threat Event Frequency

The probable frequency, within a given timeframe, that a threat agent will act against an asset

Contact Frequency

- Random
- Regular
- Intentional

Probability of Action

- Value of the asset to them
- How vulnerable the asset appears to be
- Limits
  - Motives and objectives
  - Legal limits
  - Consequences of getting caught

Determine Threat Event Frequency

Cyber Vandal

- **Contact Frequency**: Regular; regularly looks for victims, but does not necessarily target our company
- **Probability of Action:** Low; no credible threats, asset is of low value
- No previous incidents.
- No credible threats.
- Similar non-profits have been victimized.

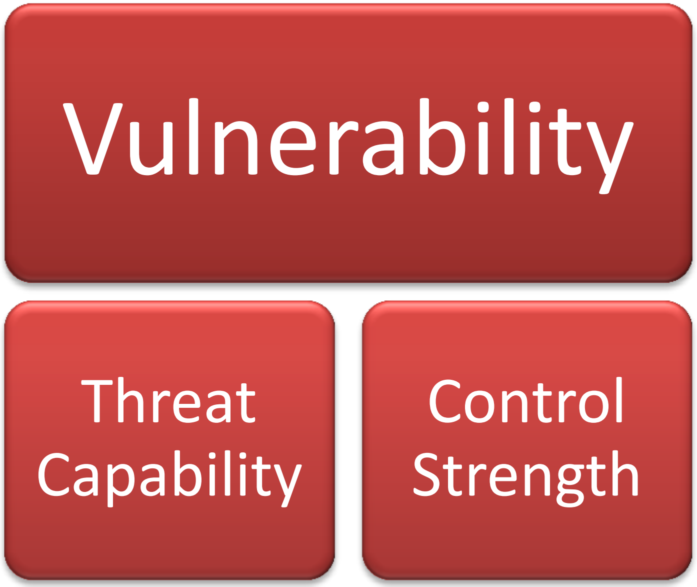
TEF: < .1x / year

Radical Activist

- **Contact Frequency**: Intentional; seeks to damage our company
- **Probability of Action:** High; group is opposed to our ideology
- Website was DDOSed last year; radical group took responsibility.
- No recent threats.
- Similar non-profits have received threats.

TEF: 1x / year to .1x / year

Step 4: Threat Capability



Vulnerability

Threat Capability

Control Strength

The probability that an asset will be unable to resist the actions of a threat agent.

Top 2%
Top 16%
Average skill and resources
Bottom 16%
Bottom 2%

Step 5: Derive Risk

Loss Event Frequency
1x / year to .1x / year

Vulnerability
Threat Capability
Medium/Average
Control Strength
Low – Only protects against the bottom 16%

Evaluate Probable Loss
Response: $16,000
Productivity: $25,000 per day

Radical Activist

Risk
Moderate
Loss: $36,000 1x - .1x year

Step 5: Derive Risk

Loss Event Frequency
<.1x / year

Vulnerability
Threat Capability
Low- Bottom 16%
Control Strength
Low – Only protects against the bottom 16%

Evaluate Probable Loss
Response: $16,000
Productivity: $25,000 per day

Cyber Vandal

Risk
Moderate
Loss: $36,000 1x - .1x year

Conclusion

“You have more data than you think, and you need less data than you think.”

- Douglas Hubbard, “How To Measure Anything”

Further Reading

Books

The Failure of Risk Management; Douglas Hubbard

How to Measure Anything; Douglas Hubbard

Measuring and Managing Information Risk: A FAIR Approach by Jack Jones and Jack Freund

Online Resources

Intel's Threat Agent Risk Assessment: https://communities.intel.com/docs/DOC-1151

Information Technology Sector Baseline Risk Assessment (DHS): http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf

OWASP: Threat Risk Modeling: https://www.owasp.org/index.php/Threat_Risk_Modeling