RSAConference2019
San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID:GRC-W12

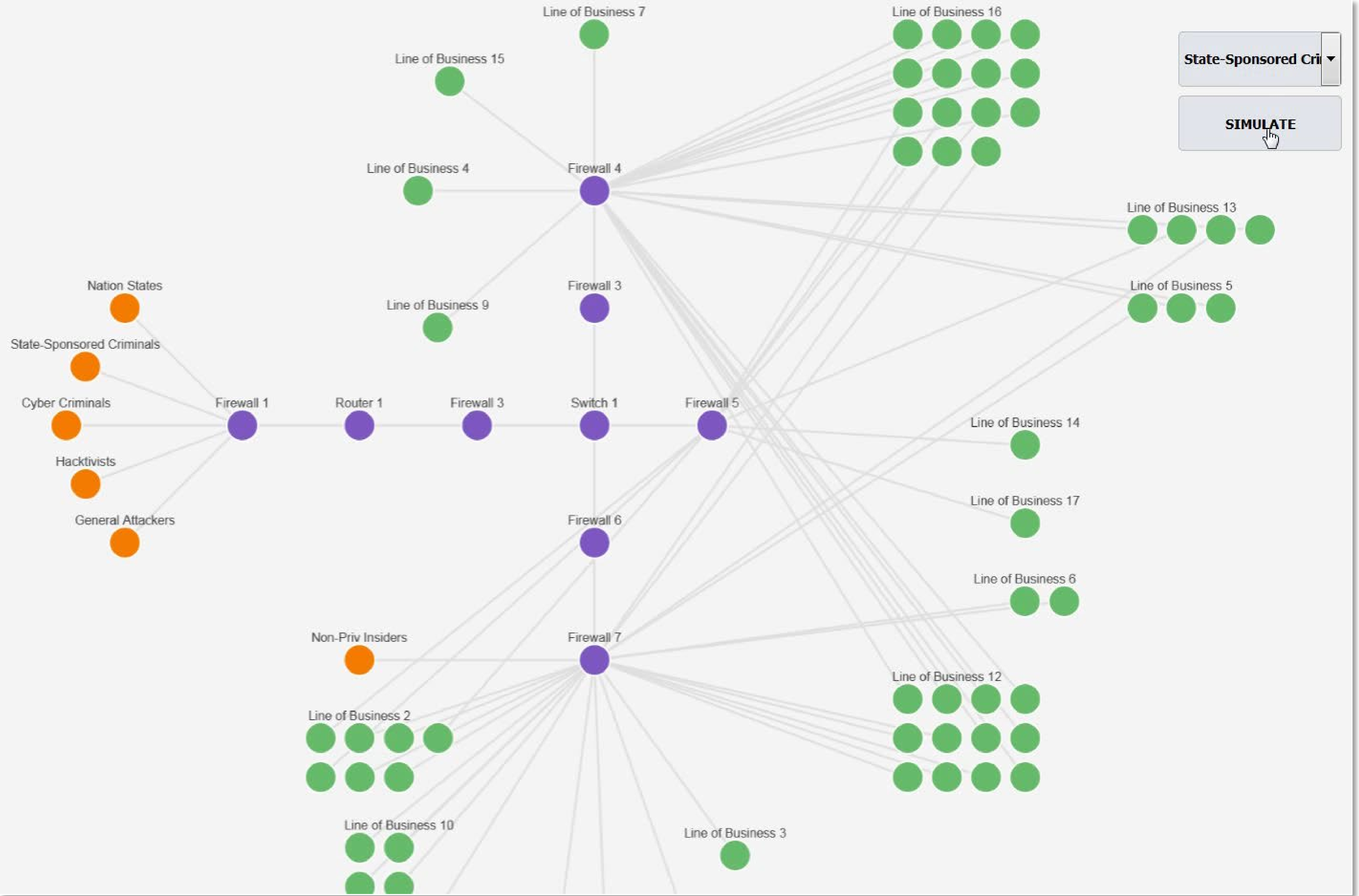
Virtual Pen Testing Using Risk Models

Jack Freund, Ph.D.

Director, Cyber Risk
TIAA
@jackfreund3

Joel Amick

Director, Cyber Analytics & Data Science
TIAA
@JoelAmick

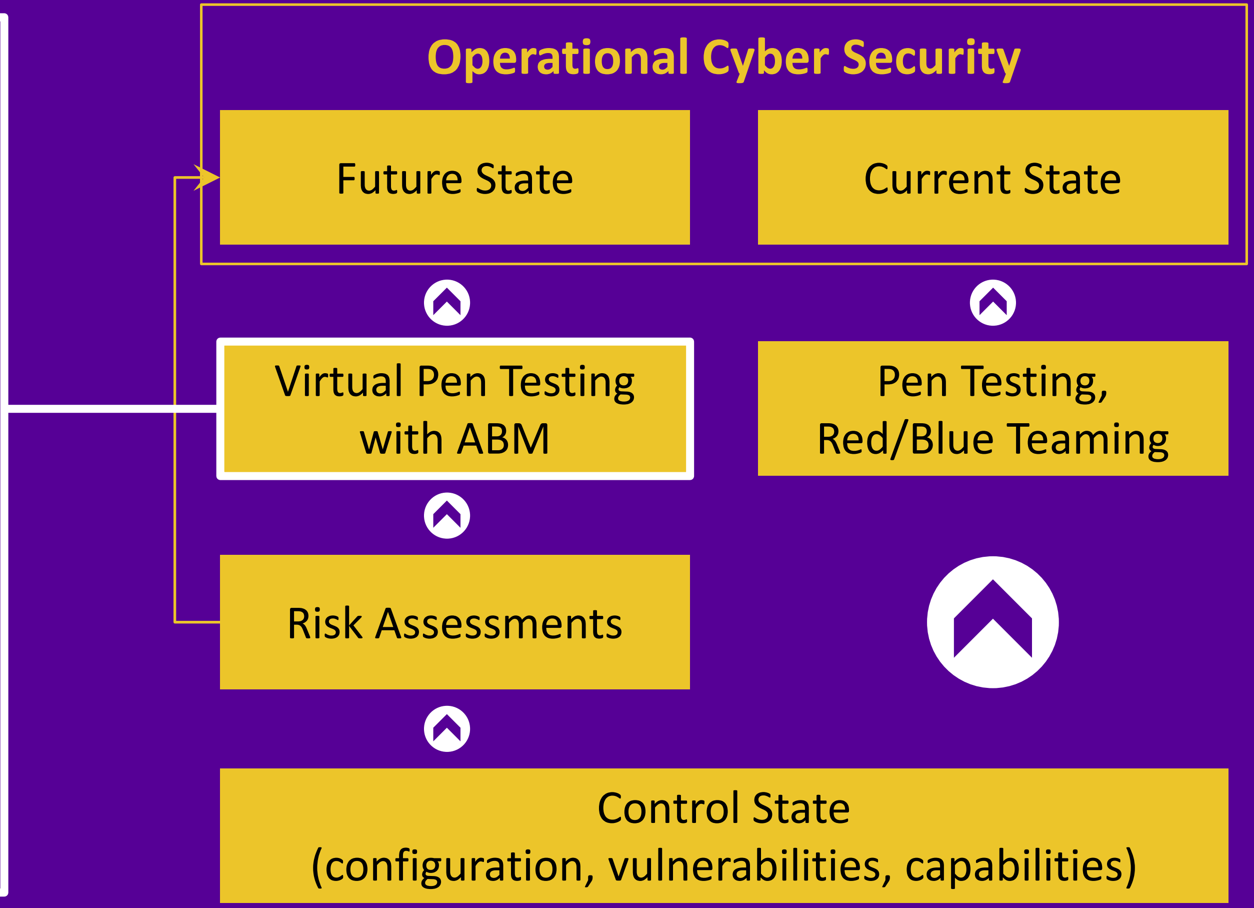


Line of Business 7
Line of Business 16
State-Sponsored Cri
SIMULATE
Line of Business 15
Line of Business 4
Firewall 4
Line of Business 13
Firewall 3
Line of Business 5
Nation States
Line of Business 9
State-Sponsored Criminals
Cyber Criminals
Firewall 1
Router 1
Firewall 3
Switch 1
Firewall 5
Line of Business 14
Hacktivists
Line of Business 17
General Attackers
Firewall 6
Line of Business 6
Non-Priv Insiders
Firewall 7
Line of Business 12
Line of Business 2
Line of Business 10
Line of Business 3

The Missing Link to Integrating Risk Assessments into Cyber Ops

VIRTUAL PEN TESTING

- Based on risk assessment results to provide data about future events
- Simulation is the necessary missing link to provide a view into the future capabilities of the cyber operations (the future is probabilistic)
- Provide risk-based incident forecasting to identify potential breach paths
- Identify vulnerable applications and remediation opportunities
- Visualize network topography from the attacker’s perspective for execs (tell the story)


Operational Cyber Security
Future State
Current State
Virtual Pen Testing with ABM
Pen Testing, Red/Blue Teaming
Risk Assessments
Control State (configuration, vulnerabilities, capabilities)

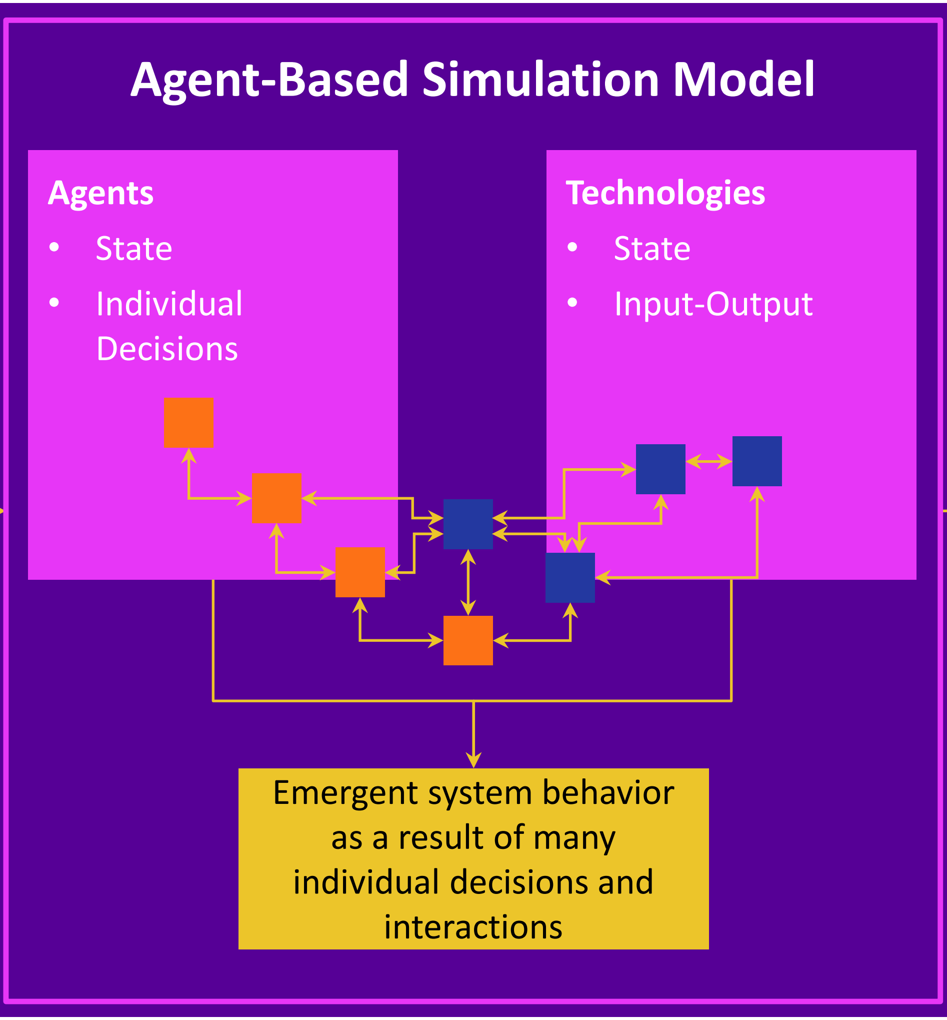
What is an Agent-Based Model?

Inputs
- Scenarios
- Agent Styles
- Technology Properties

Definition

An Agent-Based Model (ABM) consists of a system of agents and the relationships between them and their environment.

- Agents are explicitly represented in a program as a collection of autonomous decision-making entities
- Each agent individually assesses its situation and makes decisions on the basis of a set of rules
- Repetitive competitive interactions between agents are a feature of agent-based modeling
- Agent-based models can exhibit complex behavior patterns and provide valuable information about the dynamics of the real-world system that it emulates.
- Agents may be capable of evolving, allowing unanticipated behaviors to emerge



Agent-Based Simulation Model

Agents
- State
- Individual Decisions

Technologies
- State
- Input-Output

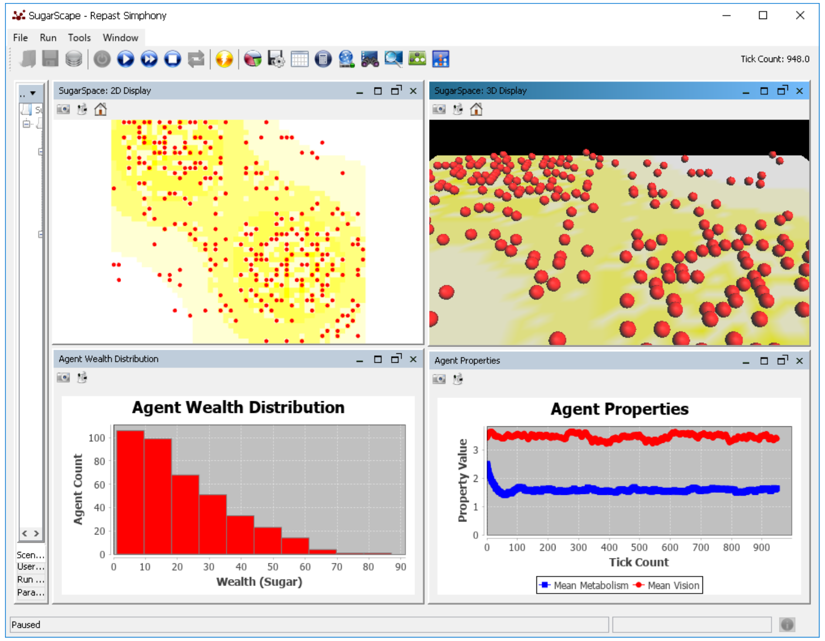
Emergent system behavior as a result of many individual decisions and interactions

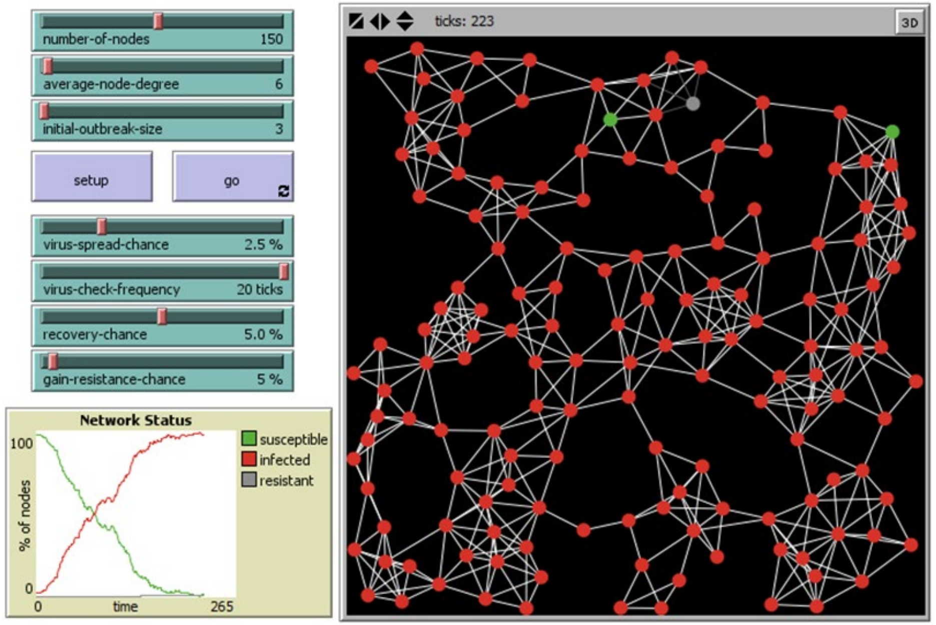
Outputs
- Agent Behavior
- System Behavior

Characteristics

- Distributed artificial intelligence tool
- Uses complexity theory, self-organizing systems, and complex adaptive systems to model reality
- Shows emergent behavior of overall system
- Allows parallel computation (simultaneous attacks)
- Uses rules of interaction for independent agents

Agent-Based Modeling Tools (OSS)




number-of-nodes 150
average-node-degree 6
initial-outbreak-size 3
virus-spread-chance 2.5 %
virus-check-frequency 20 ticks
recovery-chance 5.0 %
gain-resistance-chance 5 %

Custom developing an Agent-Based Model

Drivers for custom development

- Visualization is customizable to fit business needs/expectation
- Programmers can use their tool of choice instead of learning a new tool
- Higher interpretability and exposure into inner-workings of model

Considerations when custom developing

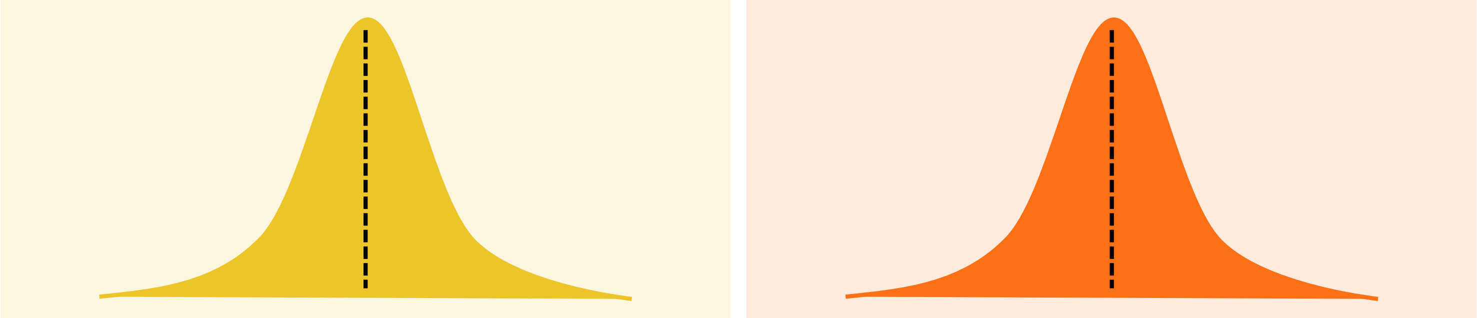
- Ensure output can be easily shared, while also permissioned as needed
- Development tool needs to be common to all developers
- Need to have in-depth understanding of Agent Based Modeling

How Agent-Based Modeling Works

100 Meter Butterfly

Threat Strength (Phelps)

Control Strength (Lochte)



52 seconds

54 seconds

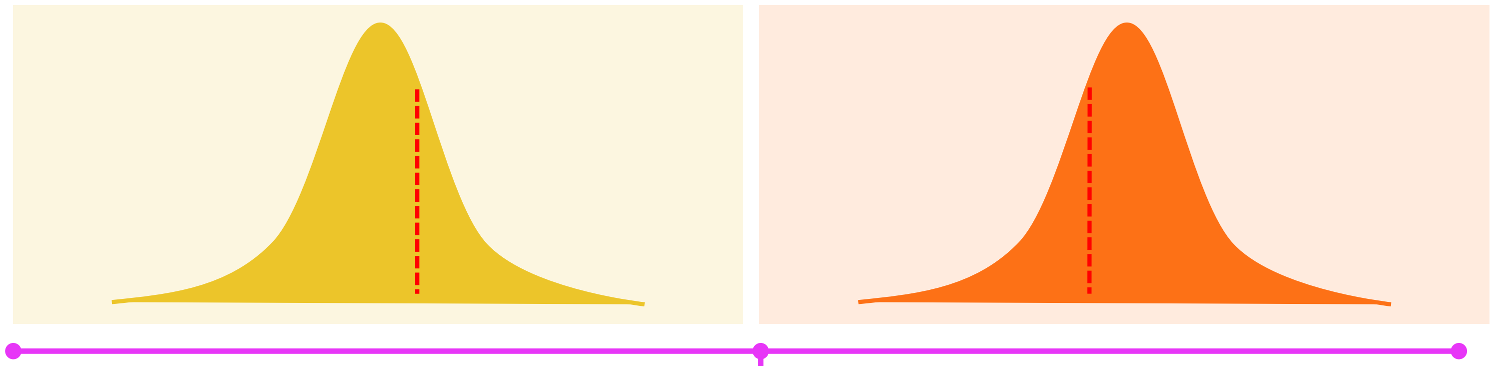
Phelps has a slight advantage

How Agent-Based Modeling Works

100 Meter Butterfly

Threat Strength (Phelps)

Control Strength (Lochte)



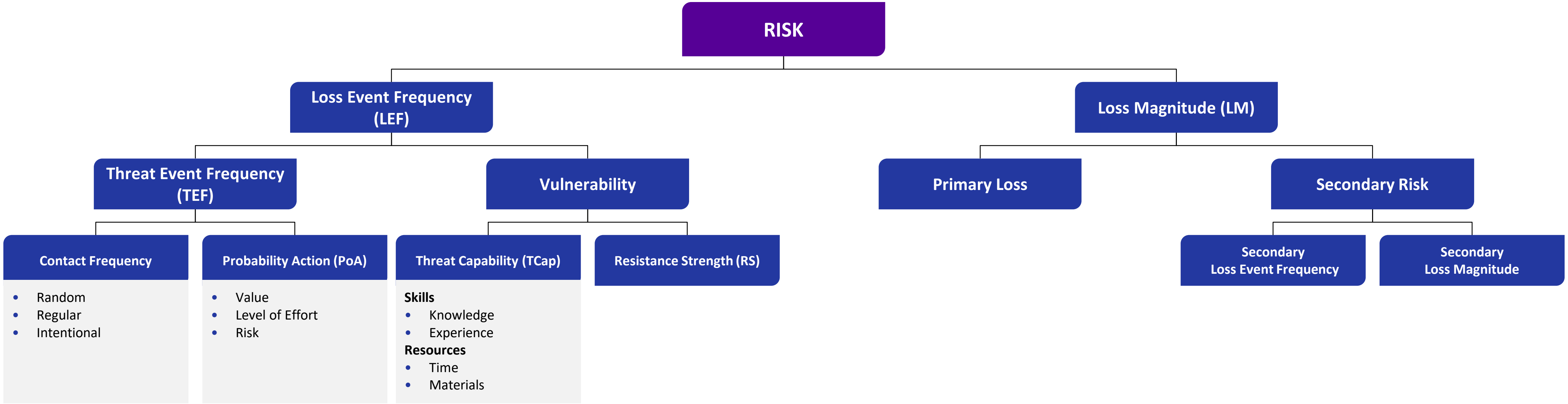
54 seconds

53 seconds

Lochte wins in an upset!

Simulation runs 125k total times

Factor Analysis of Information Risk (FAIR) Model Overview



RISK

Loss Event Frequency (LEF)

Loss Magnitude (LM)

Threat Event Frequency (TEF)

Vulnerability

Primary Loss

Secondary Risk

Contact Frequency
- Random
- Regular
- Intentional

Probability Action (PoA)
- Value
- Level of Effort
- Risk

Threat Capability (TCap)

Skills
- Knowledge
- Experience

Resources
- Time
- Materials

Resistance Strength (RS)

Secondary Loss Event Frequency

Secondary Loss Magnitude

RISK

The probable frequency and probable magnitude of future loss

LOSS EVENT FREQUENCY

The Frequency, within a given timeframe, that loss is expected to occur

THREAT EVENT FREQUENCY

The Frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss

VULNERABILITY

The probability that a threat event will become a loss event

THREAT CAPACITY

The level of force a threat agent is able to apply

RESISTANCE STRENGTH

A measure of how difficult it is for a threat actor to inflict harm (a.k.a. – Difficulty)

SECONDARY LOSS EVENT FREQUENCY

The percentage of time that secondary stakeholders are likely to react negatively to an event

PRODUCTIVITY LOSS

Loss that results from an operational inability to deliver products or services

RESPONSE COSTS

Loss associated with the costs of managing an event

REPLACEMENT COSTS

Loss that results from an organization having to replace capital assets

COMPETITIVE ADVANTAGE LOSS

Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

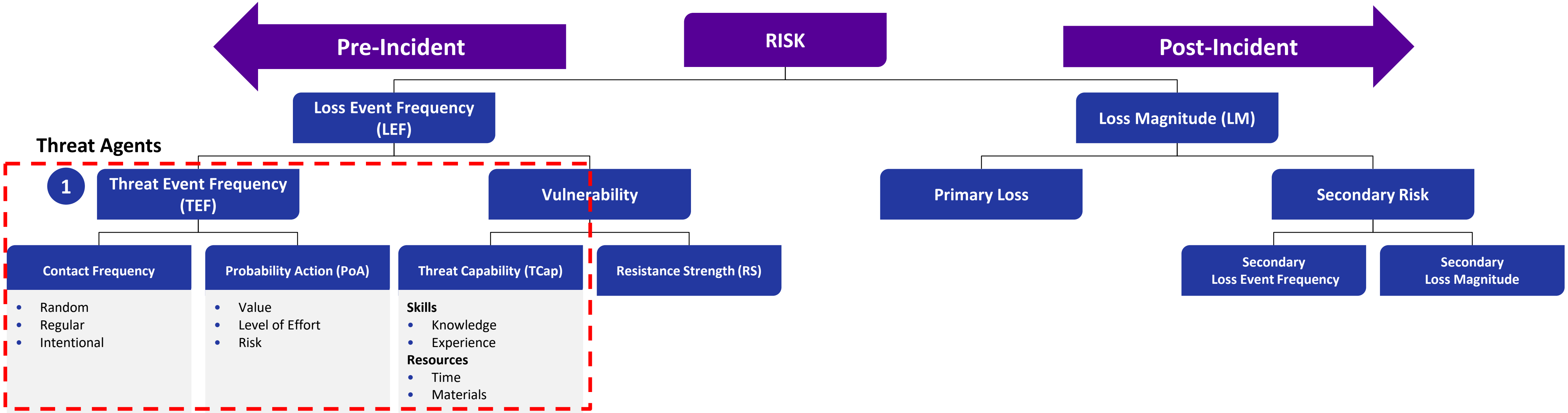
FINES AND JUDGMENTS

Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE

Loss resulting from an external stakeholder perspective that an organization’s value has decreased and/or that its liability has increased

FAIR Variables in ABM Model: Threat Agents



Contact Frequency

- Random
- Regular
- Intentional

Probability Action (PoA)

- Value
- Level of Effort
- Risk

Threat Capability (TCap)

Skills

- Knowledge
- Experience

Resources

- Time
- Materials

RISK

The probable frequency and probable magnitude of future loss

LOSS EVENT FREQUENCY

The Frequency, within a given timeframe, that loss is expected to occur

THREAT EVENT FREQUENCY

The Frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss

VULNERABILITY

The probability that a threat event will become a loss event

THREAT CAPACITY

The level of force a threat agent is able to apply

RESISTANCE STRENGTH

A measure of how difficult it is for a threat actor to inflict harm (a.k.a. – Difficulty)

SECONDARY LOSS EVENT FREQUENCY

The percentage of time that secondary stakeholders are likely to react negatively to an event

PRODUCTIVITY LOSS

Loss that results from an operational inability to deliver products or services

RESPONSE COSTS

Loss associated with the costs of managing an event

REPLACEMENT COSTS

Loss that results from an organization having to replace capital assets

COMPETITIVE ADVANTAGE LOSS

Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

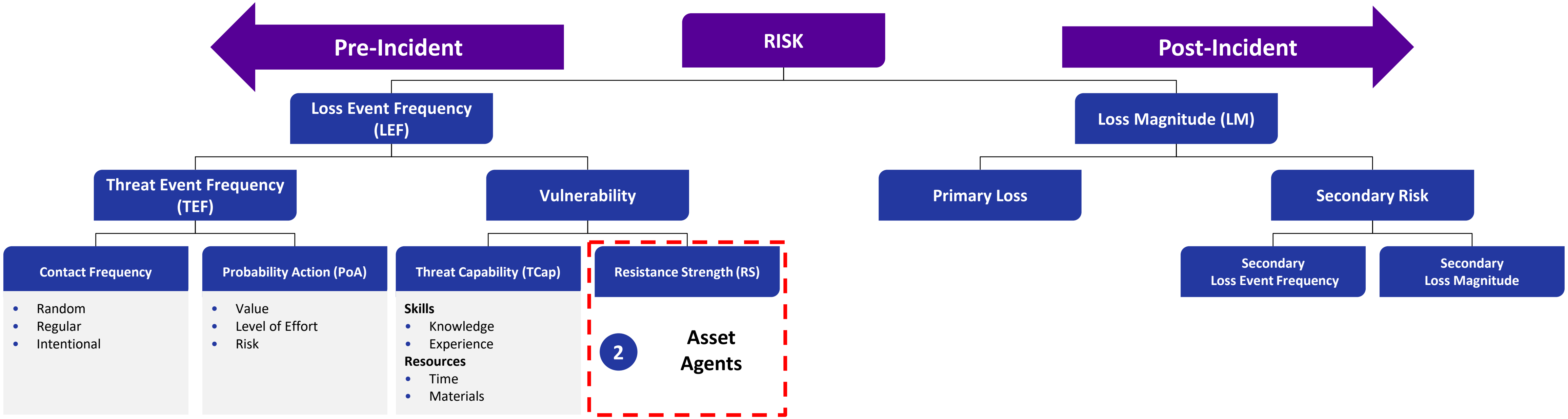
FINES AND JUDGMENTS

Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE

Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

FAIR Variables in ABM Model: Asset Agents



Pre-Incident

RISK

Post-Incident

Loss Event Frequency (LEF)

Loss Magnitude (LM)

Threat Event Frequency (TEF)

Vulnerability

Primary Loss

Secondary Risk

Contact Frequency
- Random
- Regular
- Intentional

Probability Action (PoA)
- Value
- Level of Effort
- Risk

Threat Capability (TCap)

Skills
- Knowledge
- Experience

Resources
- Time
- Materials

Resistance Strength (RS)

2 Asset Agents

Secondary Loss Event Frequency

Secondary Loss Magnitude

RISK

The probable frequency and probable magnitude of future loss

LOSS EVENT FREQUENCY

The Frequency, within a given timeframe, that loss is expected to occur

THREAT EVENT FREQUENCY

The Frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss

VULNERABILITY

The probability that a threat event will become a loss event

THREAT CAPACITY

The level of force a threat agent is able to apply

RESISTANCE STRENGTH

A measure of how difficult it is for a threat actor to inflict harm (a.k.a. – Difficulty)

SECONDARY LOSS EVENT FREQUENCY

The percentage of time that secondary stakeholders are likely to react negatively to an event

PRODUCTIVITY LOSS

Loss that results from an operational inability to deliver products or services

RESPONSE COSTS

Loss associated with the costs of managing an event

REPLACEMENT COSTS

Loss that results from an organization having to replace capital assets

COMPETITIVE ADVANTAGE LOSS

Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

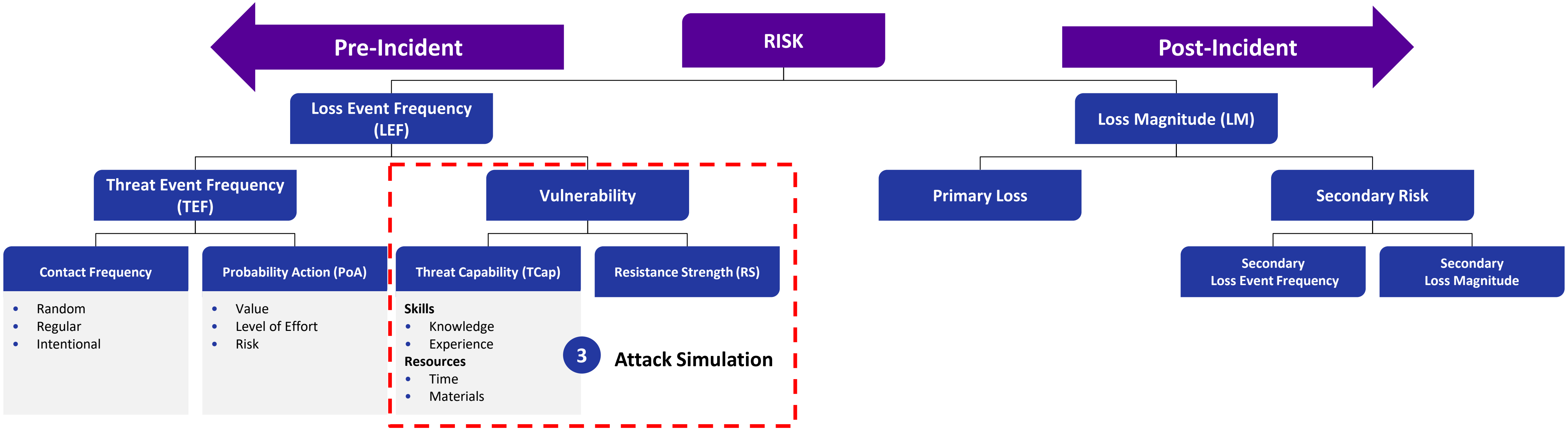
FINES AND JUDGMENTS

Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE

Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

FAIR Variables in ABM Model: Attack Simulation



RISK

The probable frequency and probable magnitude of future loss

LOSS EVENT FREQUENCY

The Frequency, within a given timeframe, that loss is expected to occur

THREAT EVENT FREQUENCY

The Frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss

VULNERABILITY

The probability that a threat event will become a loss event

THREAT CAPACITY

The level of force a threat agent is able to apply

RESISTANCE STRENGTH

A measure of how difficult it is for a threat actor to inflict harm (a.k.a. – Difficulty)

SECONDARY LOSS EVENT FREQUENCY

The percentage of time that secondary stakeholders are likely to react negatively to an event

PRODUCTIVITY LOSS

Loss that results from an operational inability to deliver products or services

RESPONSE COSTS

Loss associated with the costs of managing an event

REPLACEMENT COSTS

Loss that results from an organization having to replace capital assets

COMPETITIVE ADVANTAGE LOSS

Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

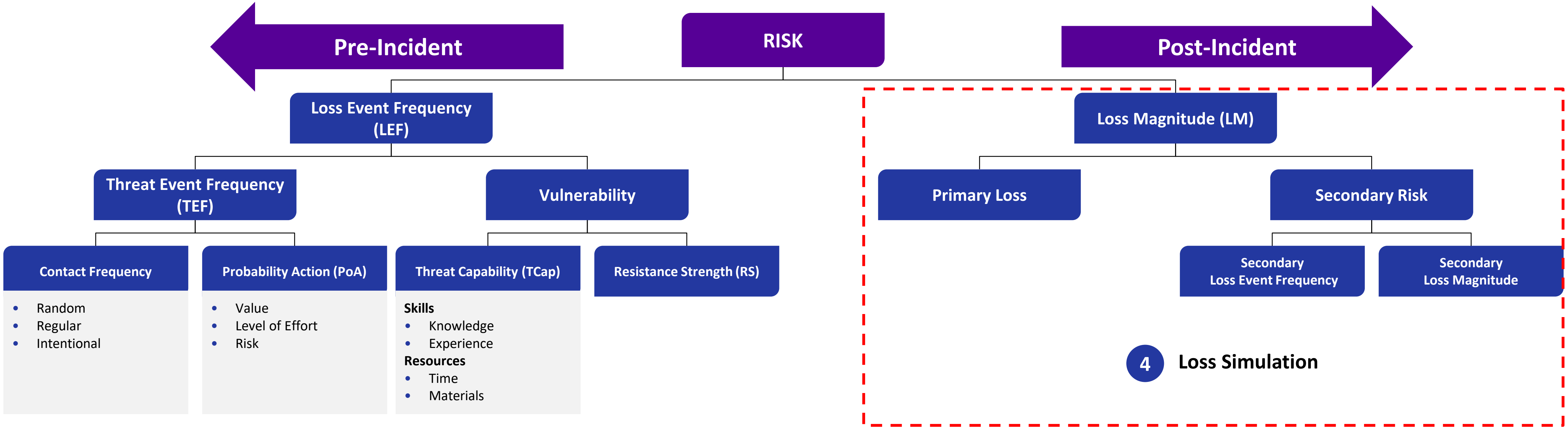
FINES AND JUDGMENTS

Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE

Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

FAIR Variables in ABM Model: Loss Simulation



Pre-Incident

RISK

Post-Incident

Loss Event Frequency (LEF)

Loss Magnitude (LM)

Threat Event Frequency (TEF)

Vulnerability

Primary Loss

Secondary Risk

Contact Frequency
- Random
- Regular
- Intentional

Probability Action (PoA)
- Value
- Level of Effort
- Risk

Threat Capability (TCap)

Skills
- Knowledge
- Experience

Resources
- Time
- Materials

Resistance Strength (RS)

Secondary Loss Event Frequency

Secondary Loss Magnitude

4 Loss Simulation

RISK

The probable frequency and probable magnitude of future loss

LOSS EVENT FREQUENCY

The Frequency, within a given timeframe, that loss is expected to occur

THREAT EVENT FREQUENCY

The Frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss

VULNERABILITY

The probability that a threat event will become a loss event

THREAT CAPACITY

The level of force a threat agent is able to apply

RESISTANCE STRENGTH

A measure of how difficult it is for a threat actor to inflict harm (a.k.a. – Difficulty)

SECONDARY LOSS EVENT FREQUENCY

The percentage of time that secondary stakeholders are likely to react negatively to an event

PRODUCTIVITY LOSS

Loss that results from an operational inability to deliver products or services

RESPONSE COSTS

Loss associated with the costs of managing an event

REPLACEMENT COSTS

Loss that results from an organization having to replace capital assets

COMPETITIVE ADVANTAGE LOSS

Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

FINES AND JUDGMENTS

Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE

Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

Threat Community Actors Overview

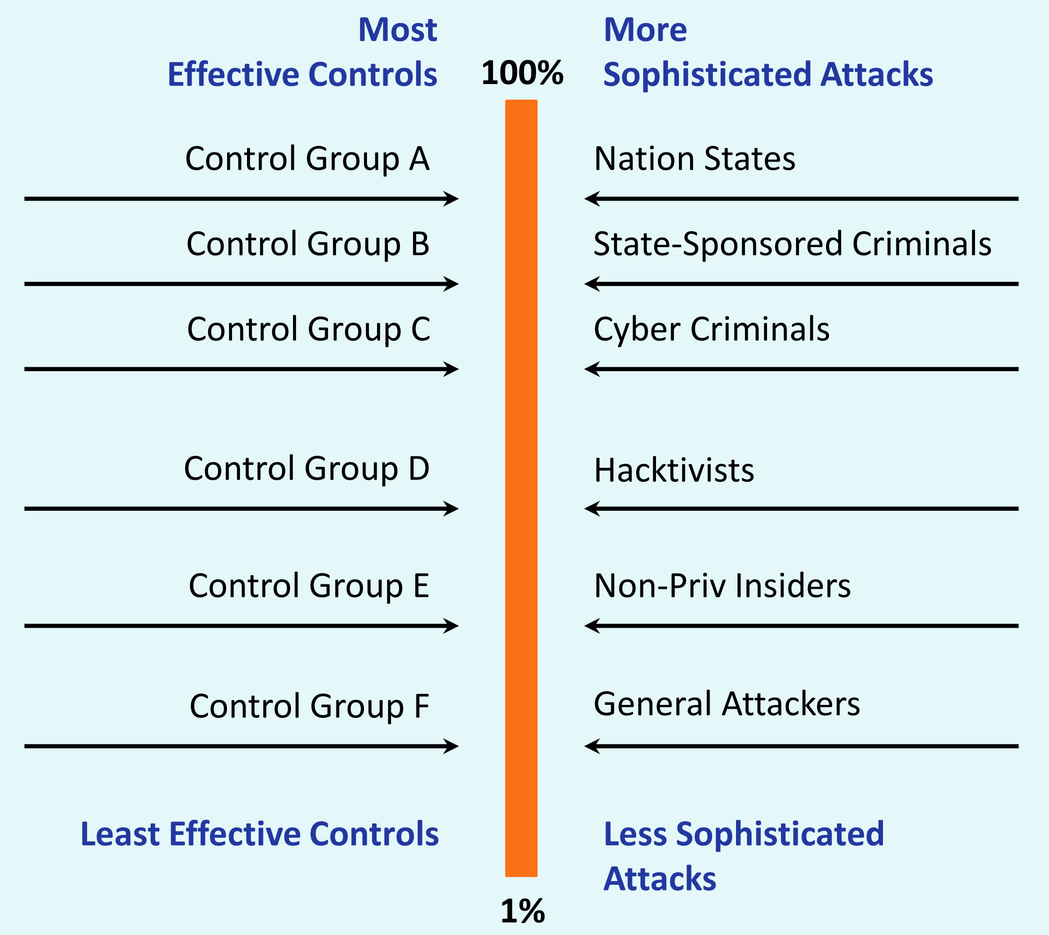
Threat Community (TCom)	Definition	Metrics	
		Threat Event Frequency (TEF)	Threat Capability (TCap)
Nation States	State sponsored professional groups that are engaged in espionage and either clandestine or overt action.	The probable frequency, within a given timeframe, that the threat will act in a manner that may result in loss. • Measured in number of times per year that an active attempt is made by this group **Contributing factors** • Contact Frequency (random, regular, Intentional/Targeted) • Probability of Action (likelihood over time that this group may act against asset). Must consider risk to the attacker (aka controls)	The probable level of force that the threat is capable of applying against an asset. • Measured using a ratio scale (percentage). **Contributing Factors** • Skills, access, resources, time, funding available to the threat • Conceptually similar to administering a "hacker" test and reporting performance as a percentile (i.e., 90th percentile hacker)
Cyber Criminals	A generic term for any group of criminal enterprises or loosely organized criminals. They are reasonably well-funded but not as well as a nation state.		
Privileged Insiders (Malicious)	People inside your organization with specific access levels, knowledge, or some other privilege for which they do not need to overcome any controls to cause harm. Also people in which the organization has placed trust such that if they wanted to do some harm, they could. • **Malicious** – Those whom intend their actions to cause harm • **Error** – Those who make mistakes that affect security		
Privileged Insiders (Errors)			
Non-Privileged Insiders (Malicious)	Everyone inside the organization who isn't privileged. These are the people who have to overcome some form of resistive control in order to affect harm.		
Hacktivists/Eco-Terrorists	Generic term for those that are interested in embarrassing and making moral, disciplined, or some other conscientious argument expressed through some cyber means.		

Cyber Risk Control Strength Overview

Control Strength

A measure of how difficult it is for a threat actor to inflict harm

- We measure control strength against the same scale as attacker capability
- Higher level controls deflect lower level attackers



Most Effective Controls

100%

More Sophisticated Attacks

Control Group A → ← Nation States

Control Group B → ← State-Sponsored Criminals

Control Group C → ← Cyber Criminals

Control Group D → ← Hacktivists

Control Group E → ← Non-Priv Insiders

Control Group F → ← General Attackers

Least Effective Controls

1%

Less Sophisticated Attacks

Threat Capability Continuum

Threat Capability

The probable level of force that the threat is capable of applying against a resource

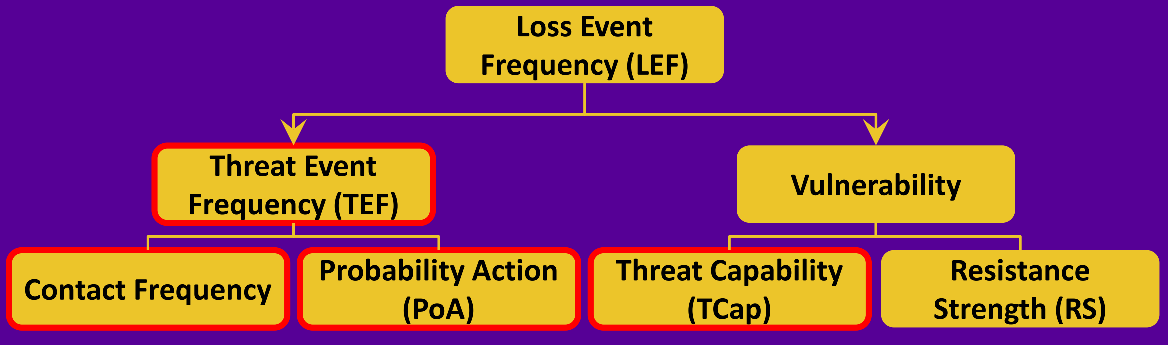
Contributing Factors

- Skills, access, resources, time, funding
- Conceptually similar to administering a “hacker” test and reporting performance as a percentile (i.e., 90th percentile hacker)

ABM Example: Threat Agents

Threat Community	Description
Nation States	State sponsored professional groups that are engaged in espionage and either clandestine or overt action
State-Sponsored Cyber Criminals	Cyber Criminals funded by a nation state
Cyber Criminals	Criminal enterprises or loosely organized criminal groups. They are reasonably well-funded
Hacktivists	Those interested in embarrassing and making moral, disciplined, or some other conscientious argument expressed through some cyber means
Non-Privileged Insiders	Employee attack.
General Attackers	Grandma on a Chromebook

Variables Modeled by Rules



Loss Event Frequency (LEF)

Threat Event Frequency (TEF)

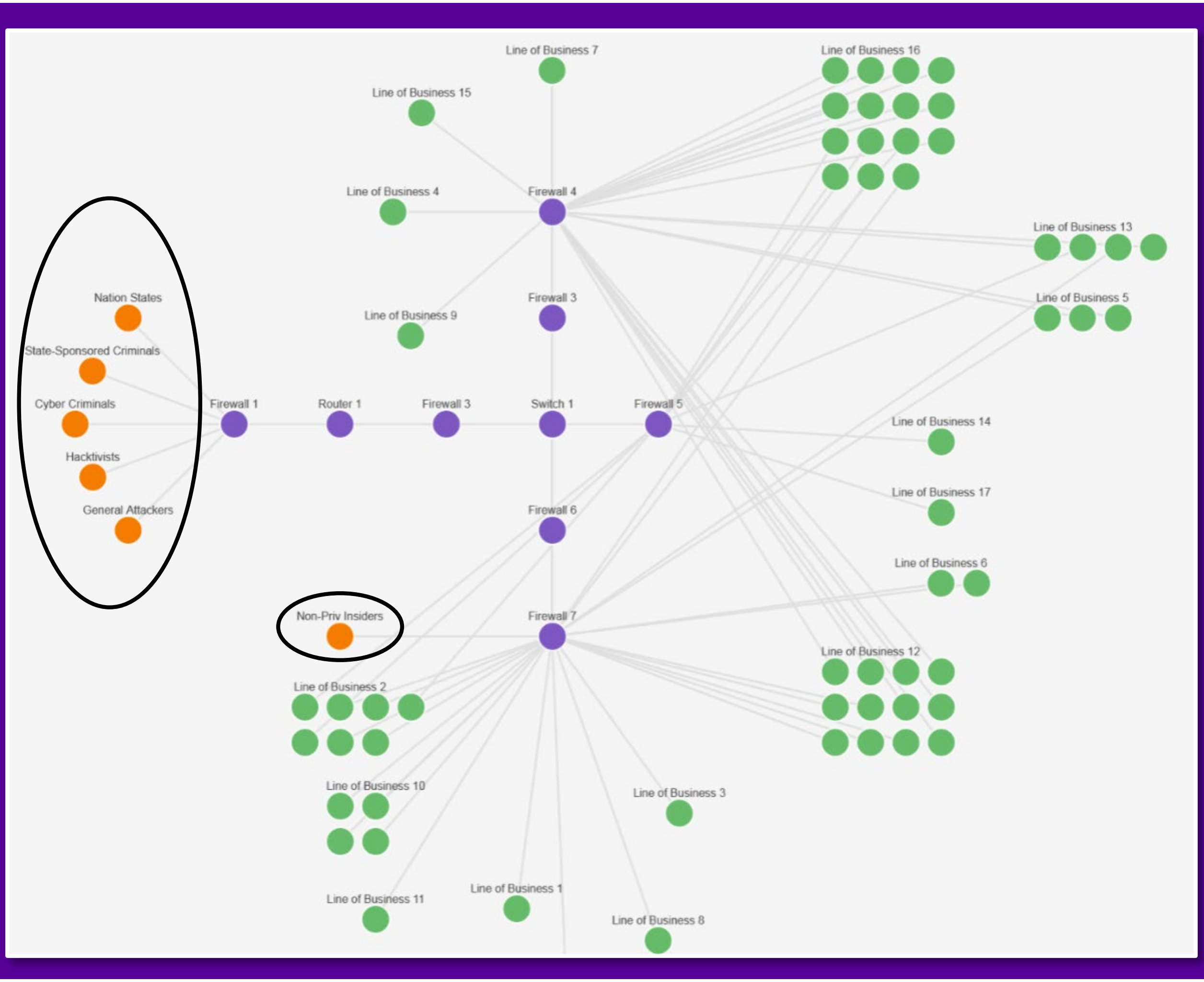
Vulnerability

Contact Frequency

Probability Action (PoA)

Threat Capability (TCap)

Resistance Strength (RS)

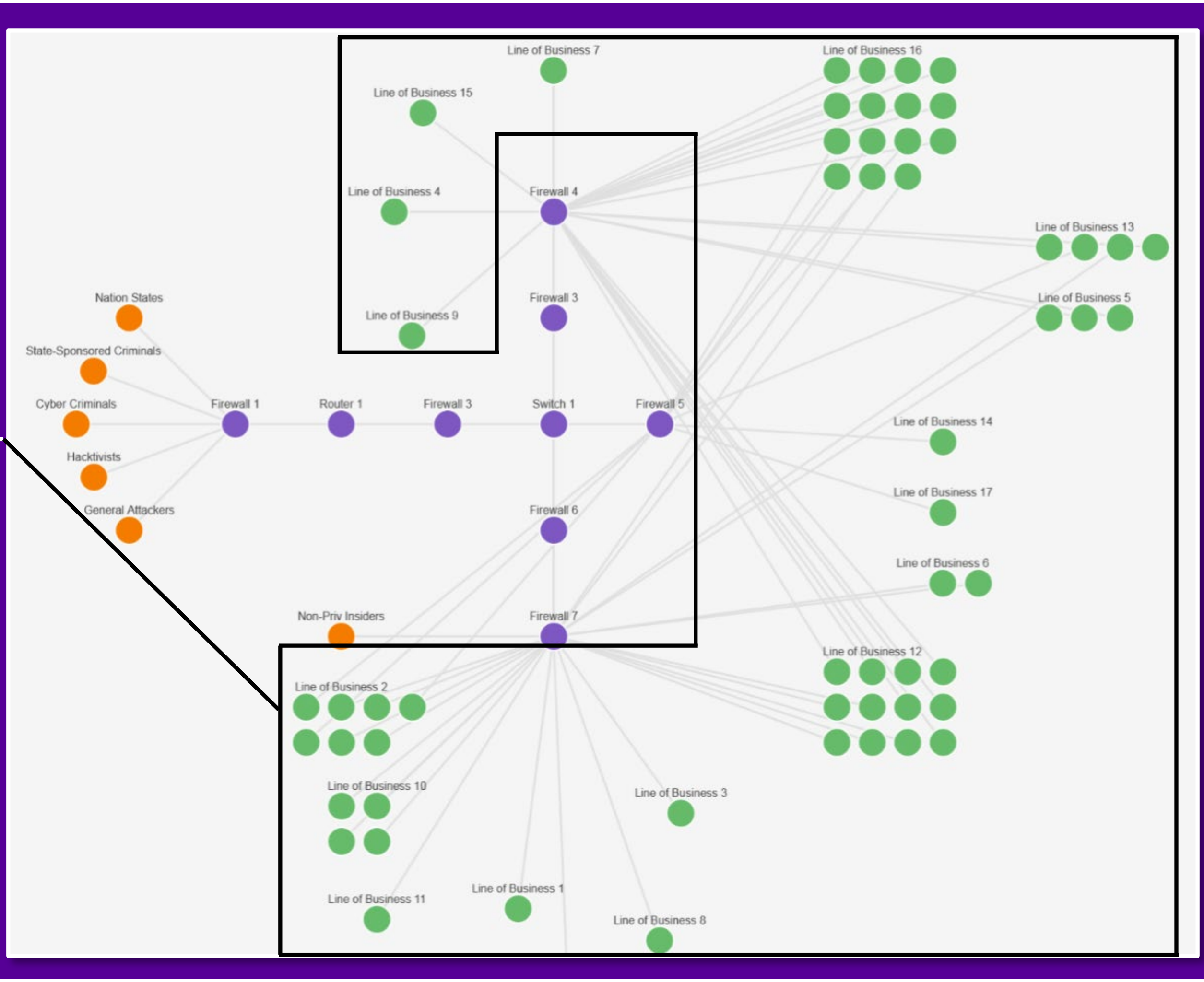


ABM Example: Applications

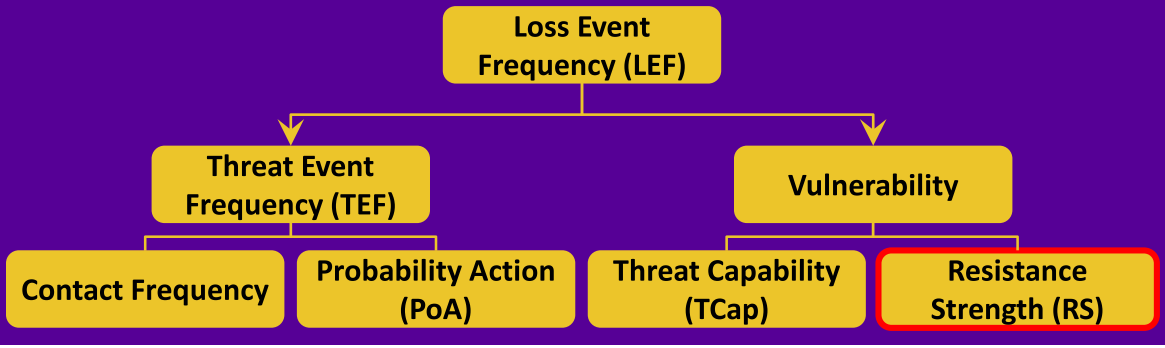
Applications Agents

1. Digital Channel
2. Marketing
3. Human Resources

Applications



Variables Modeled by Rules



Loss Event Frequency (LEF)

Threat Event Frequency (TEF)

Vulnerability

Contact Frequency

Probability Action (PoA)

Threat Capability (TCap)

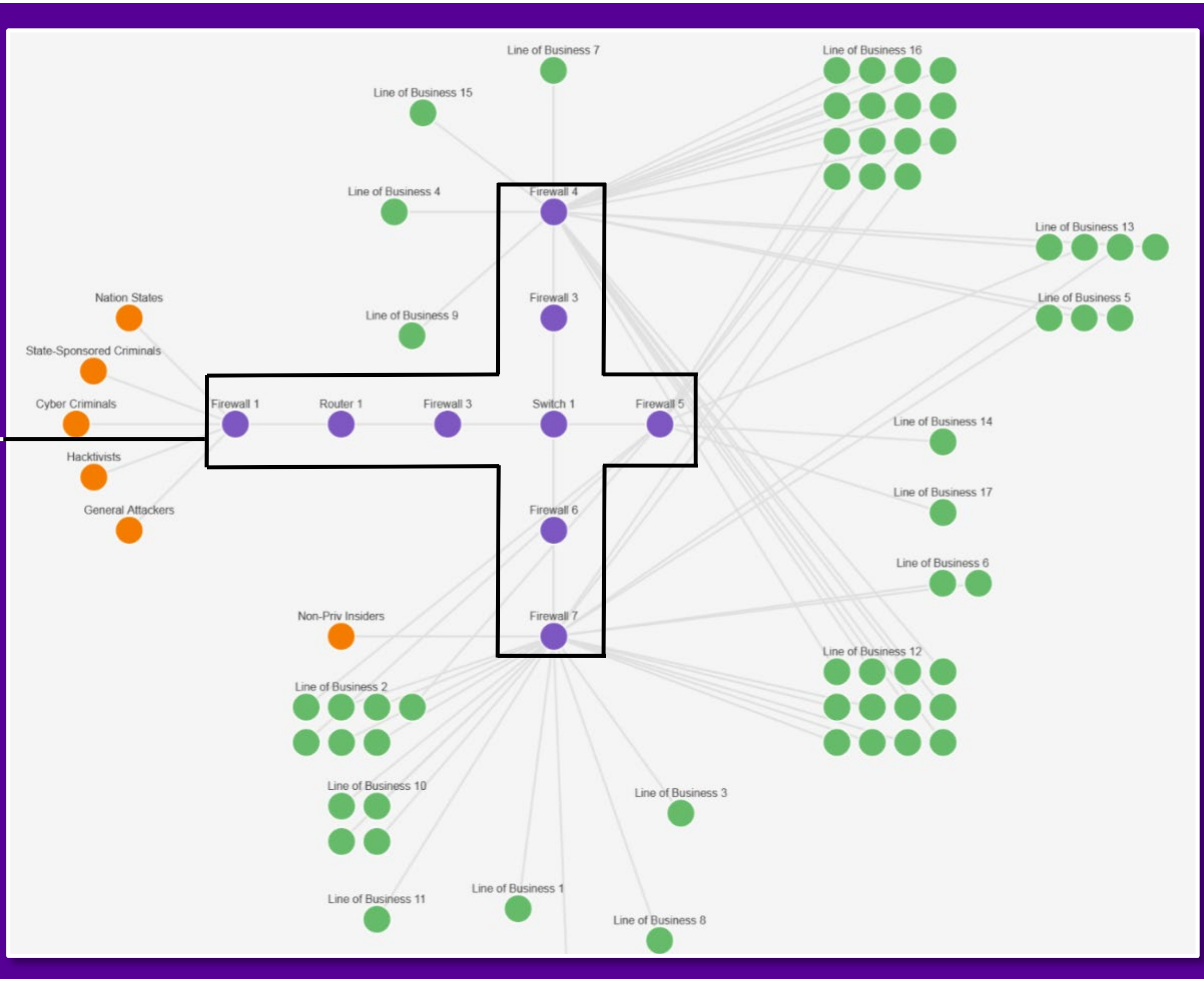
Resistance Strength (RS)

ABM Example: Network Devices

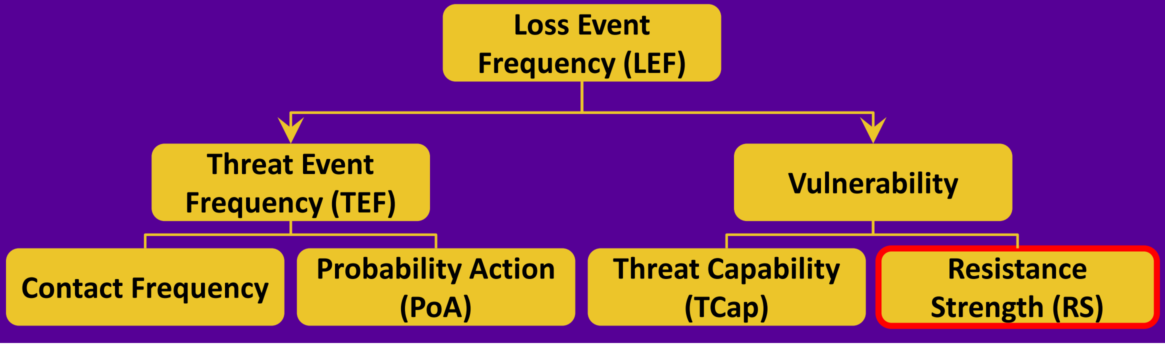
Network Agents

1. Network Tier 1
2. Network Tier 2
3. Network Tier 3

Network Infrastructure



Variables Modeled by Rules



Loss Event Frequency (LEF)

Threat Event Frequency (TEF)

Vulnerability

Contact Frequency

Probability Action (PoA)

Threat Capability (TCap)

Resistance Strength (RS)

ABM Example: Interaction Rules

Attacker

Asset

Threat Capability (TCap)

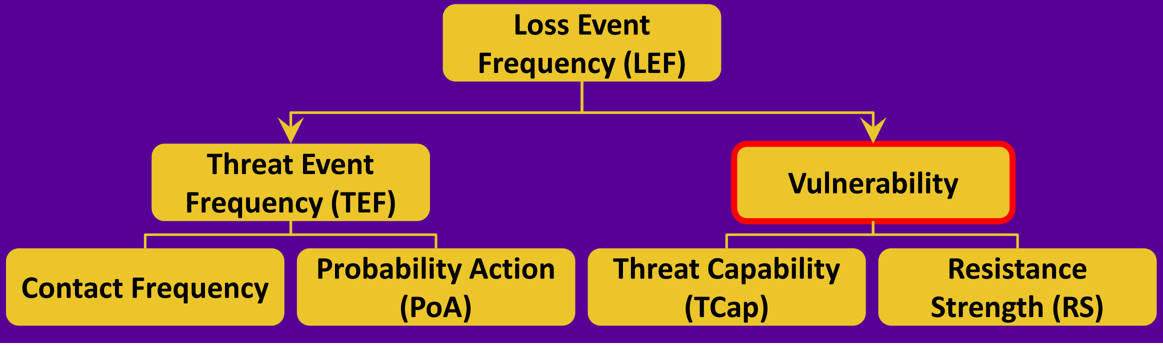
Losses/Totals Sims = Vulnerability

Resistance Strength (RS)

Attacker Interaction Rules

1. Attaches to resource over network
2. Attacks next best asset based on prioritization (if > 1 choice)

Variables Modeled by Rules



Loss Event Frequency (LEF)

Threat Event Frequency (TEF)

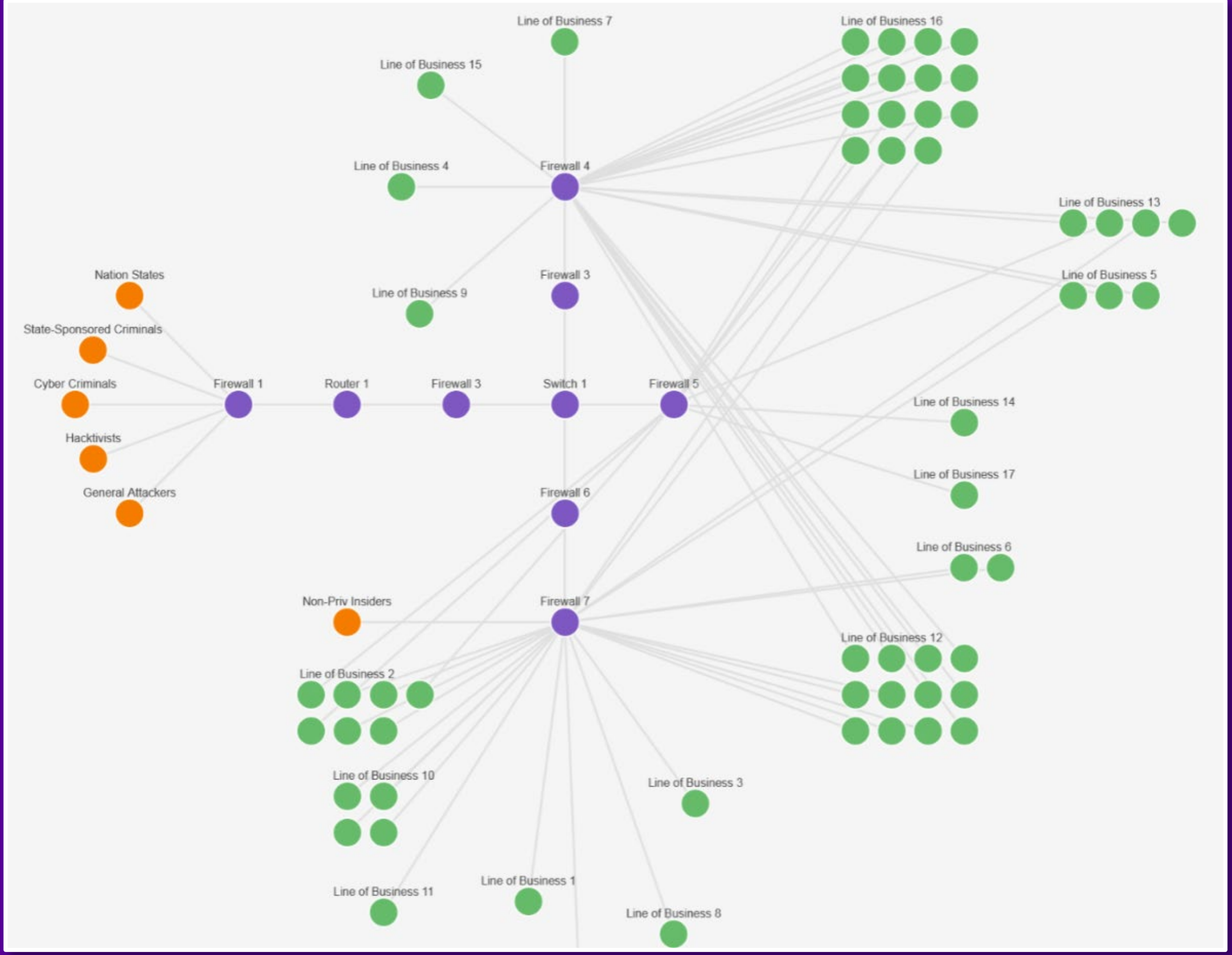
Vulnerability

Contact Frequency

Probability Action (PoA)

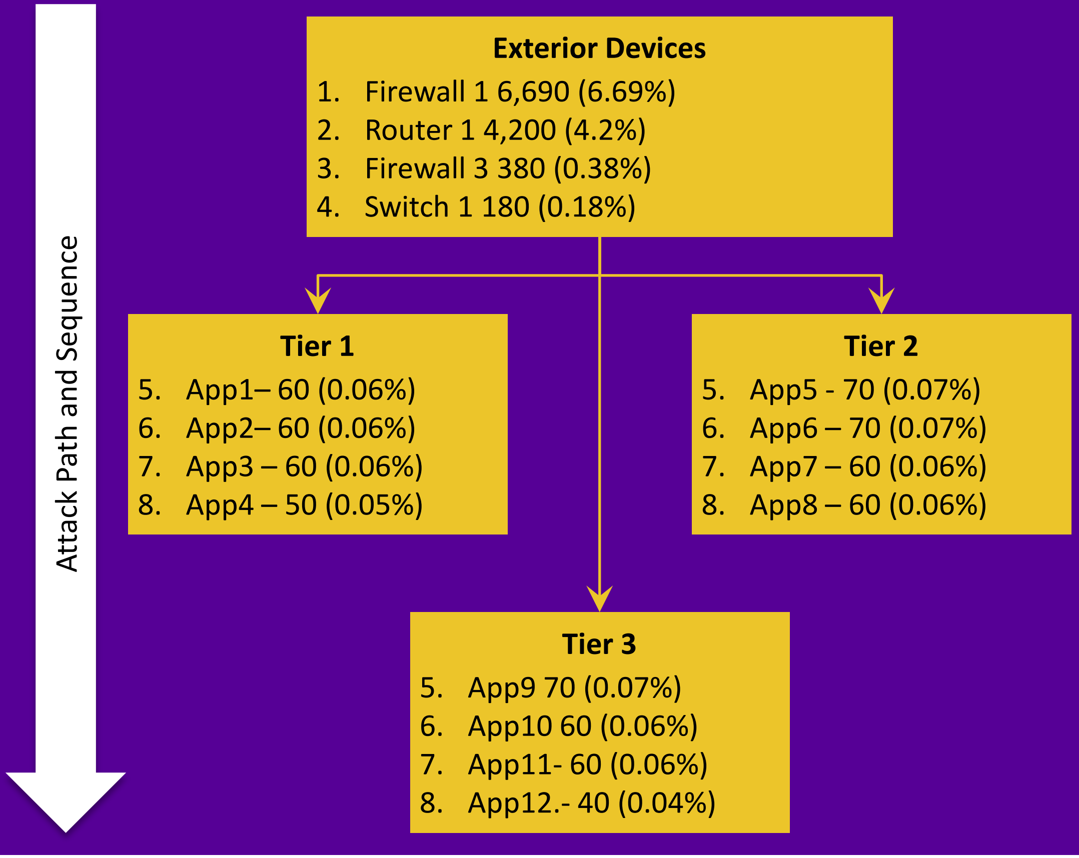
Threat Capability (TCap)

Resistance Strength (RS)



Basic Agent-Based Modeling Demo: State-Sponsored Network-Based Attack Scenario

Out of 100,000 simulated attacks, how often was each Network Device and Application compromised, and where did the attackers go?



Attack Path and Sequence

Exterior Devices

1. Firewall 1 6,690 (6.69%)
2. Router 1 4,200 (4.2%)
3. Firewall 3 380 (0.38%)
4. Switch 1 180 (0.18%)

Tier 1

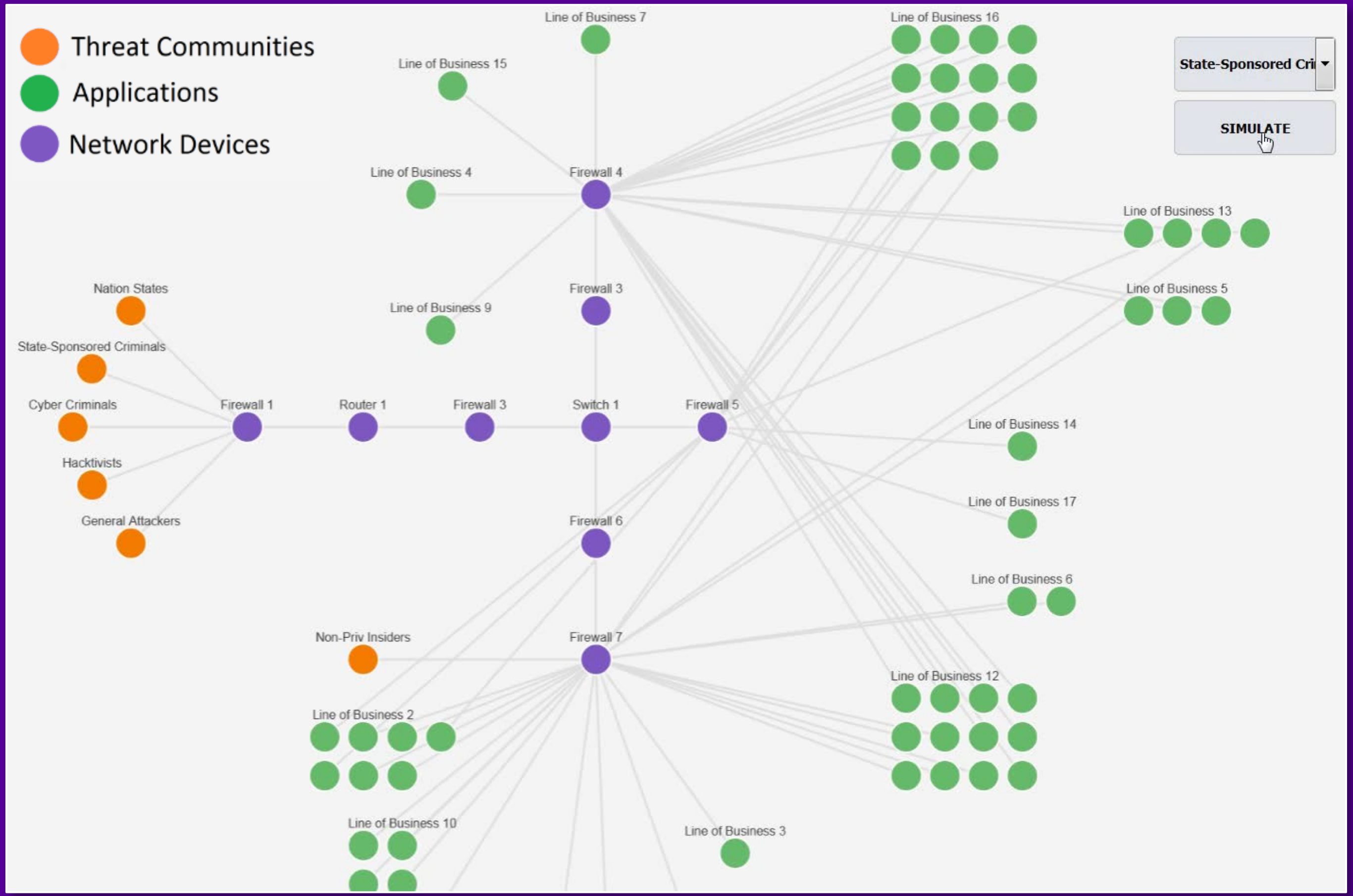
5. App1– 60 (0.06%)
6. App2– 60 (0.06%)
7. App3 – 60 (0.06%)
8. App4 – 50 (0.05%)

Tier 2

5. App5 - 70 (0.07%)
6. App6 – 70 (0.07%)
7. App7 – 60 (0.06%)
8. App8 – 60 (0.06%)

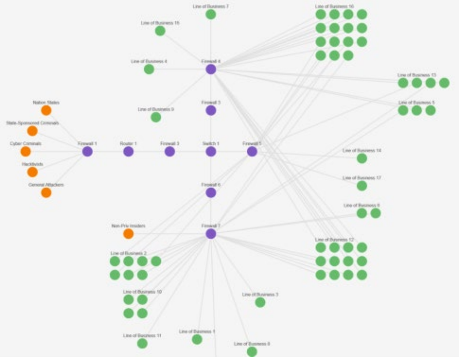
Tier 3

5. App9 70 (0.07%)
6. App10 60 (0.06%)
7. App11- 60 (0.06%)
8. App12.- 40 (0.04%)

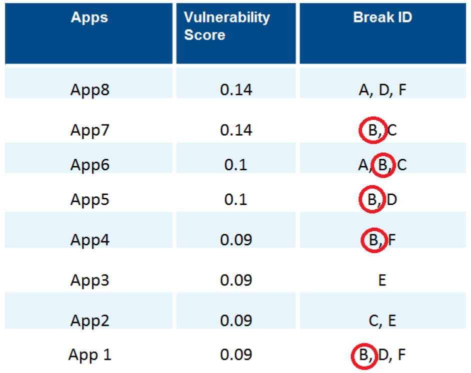


Key Benefits of using ABM for Virtual Pen Testing

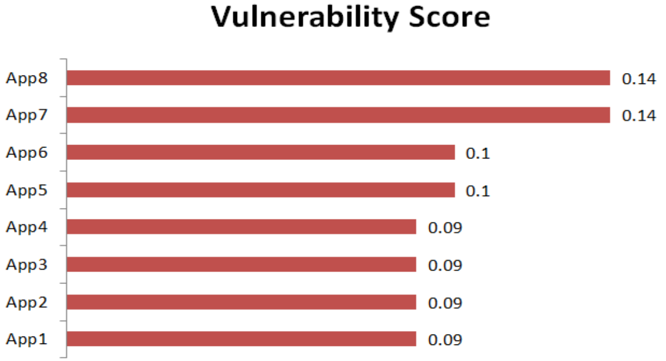
Communicate visually the full Threat-Control-Risk story to stakeholders 1



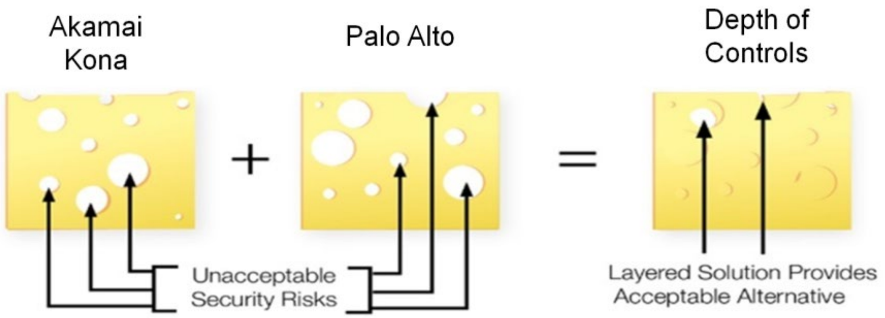
2 Prioritize control deficiency fix based on probability of attack



Apps	Vulnerability Score	Break ID
App8	0.14	A, D, F
App7	0.14	B, C
App6	0.1	A, B, C
App5	0.1	B, D
App4	0.09	B, F
App3	0.09	E
App2	0.09	C, E
App 1	0.09	B, D, F



Quantify application vulnerability rates 3


Akamai Kona
+
Palo Alto
=
Depth of Controls
Unacceptable Security Risks
Layered Solution Provides Acceptable Alternative

4 Shows strength of defense in depth

Challenges and Opportunities

Can enable automated data feeds and model execution from real-time assessment inputs

Model can also simulate loss scenarios associated with attack successes

Can model detailed attack types (think MITRE) and specific control technologies or methods

Can be used for ‘offline’ cyber resiliency testing

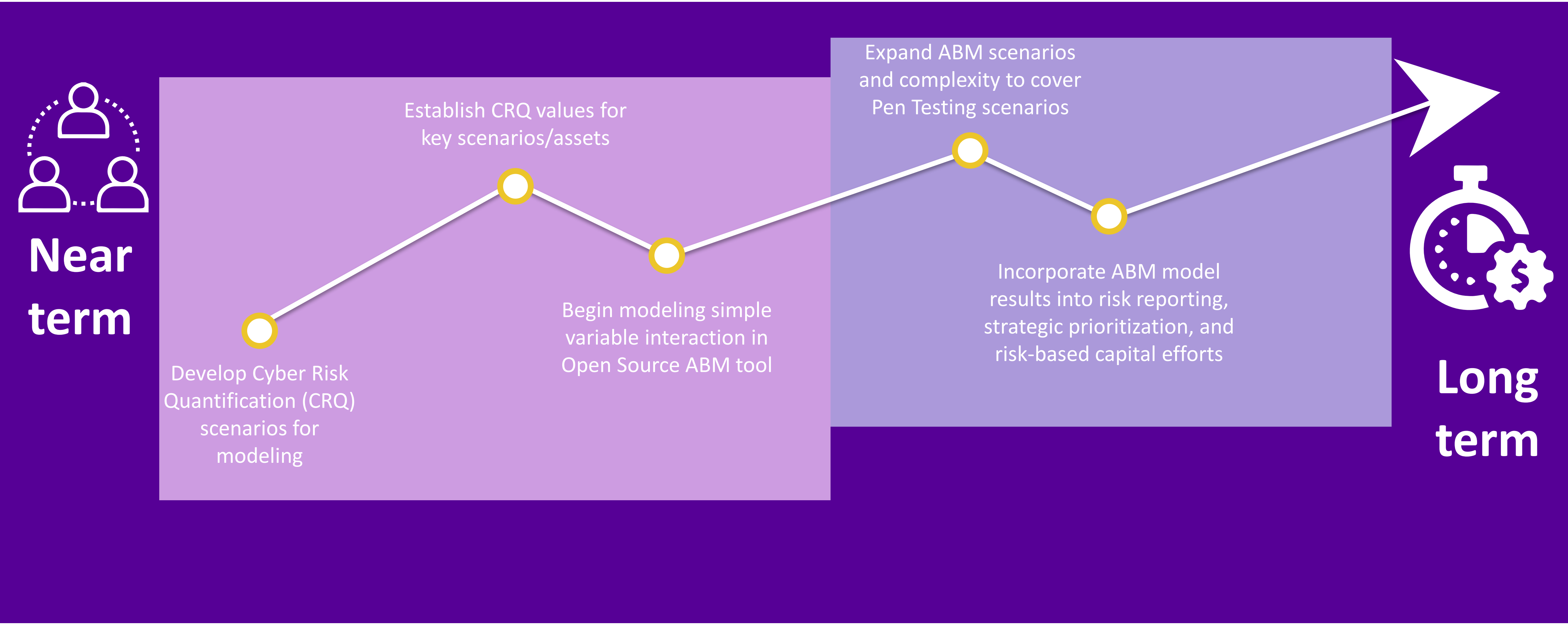
Opportunities

Challenges (Managing model complexity)

Network complexity requires either 1) thoughtful abstraction for simplistic modelling or 2) detailed development to appropriately articulate assumptions and behaviors to add

Multiple and overlapping exfiltration paths and attack scenarios are needed to fully represent attack surface (increased model complexity)

Apply What You Have Learned Today



Near term

Develop Cyber Risk Quantification (CRQ) scenarios for modeling

Establish CRQ values for key scenarios/assets

Begin modeling simple variable interaction in Open Source ABM tool

Expand ABM scenarios and complexity to cover Pen Testing scenarios

Incorporate ABM model results into risk reporting, strategic prioritization, and risk-based capital efforts

Long term