RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Implementing a Quantitative Risk-Based Approach to Cyber Security

SESSION ID: STR-W01

Scott Borg

U.S. Cyber Consequences Unit
scott.borg@usccu.us

The main problem to overcome: the statistical techniques used for other risks won't work

- **Trend Lines**
- **Normal Distributions** (bell-shaped curves)
- **Statistical Significance Tests**
- **Independent Variable Probabilities**
- **Sampling Theory** (populations of known events)
- **Bayesian Corrections**
- **Any techniques that require assigning values to individual "assets"**

The Alternative: Investigate the *Mechanisms* Involved

If you know the **actual mechanism . . .**

that **connects two factors**,

you don't need to be looking for a correlation

that will **generate an event**,

you can watch for that mechanism, rather than trying to extrapolate from past events

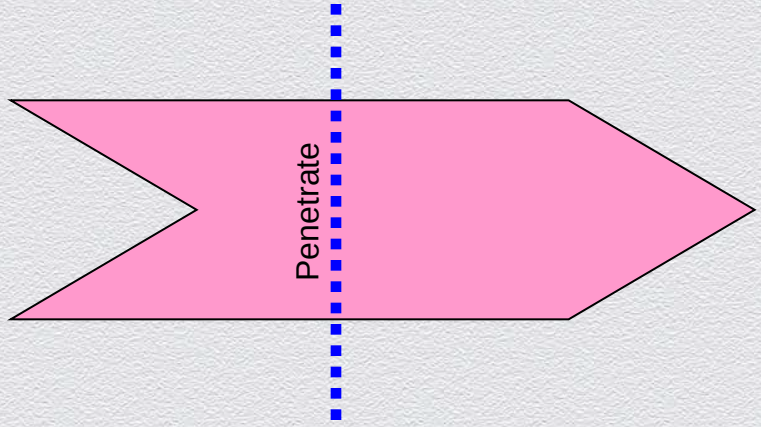
that produces **a consequence**,

you don't need a population of prior examples to estimate that consequence

Job One. Expanding the Cyber Risk Vision

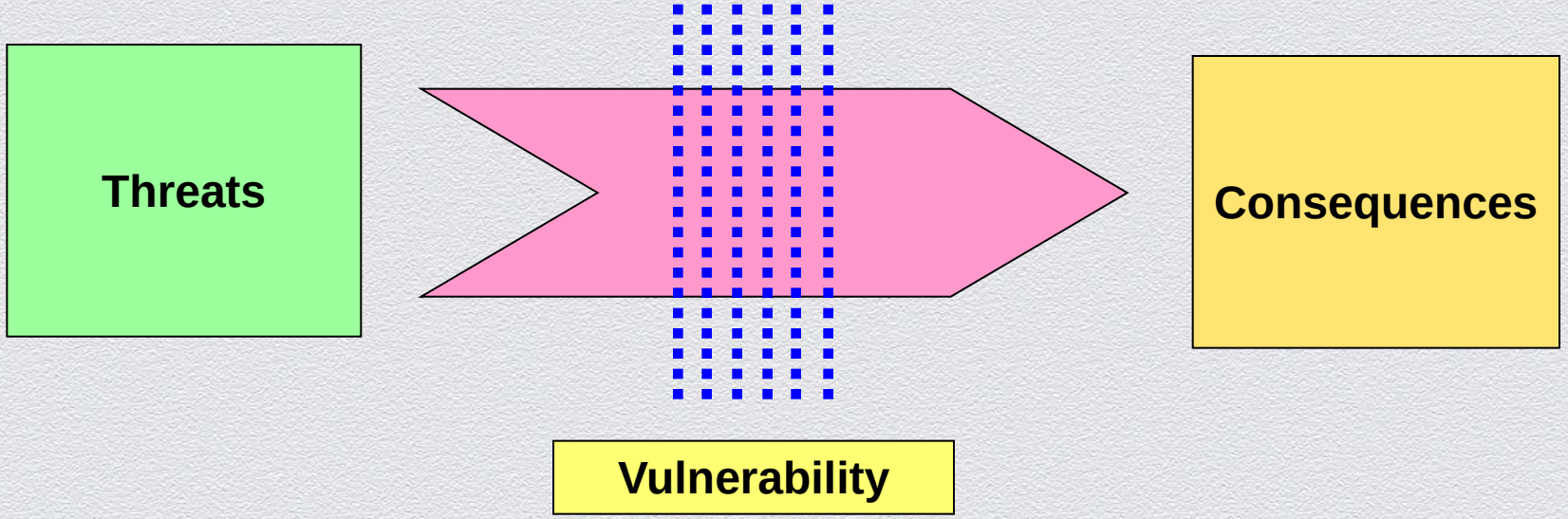
You can't see the mechanisms that drive cyber security if you're not looking in the places where they operate!

THE TRADITIONAL VISION OF CYBER ATTACKS



Even traditional "threat analysis" is really penetration exploit analysis!

ADOPTING A BROADER VISION OF CYBER ATTACKS



Makes it possible to see the mechanisms driving events & reveals more opportunities for doing something about these

Job One: Getting to the Broader Vision

- Short, intensive **courses or workshops** for cyber-security personnel on the main risk components
- Overview briefings for **senior management**
- A senior management **endorsement** for the CISO to explore a broader approach to cyber security

Job One Output: A Plan of Action

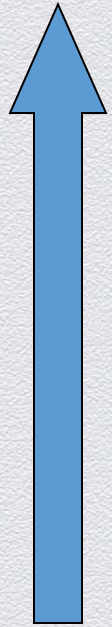
- A general plan for tackling the next two phases of this program
- The relevant personnel prepped
- Task leaders chosen for next two phases

Job Two. Mapping the Business from a Risk Standpoint

OUTPUTS TO CUSTOMERS

What is the business actually doing to create value?

Businesses take Inputs and turn them into Outputs



I. Management of Outputs

II. Management of Production

III. Management of Inputs

IV. Coordination Across Functions

INPUTS FROM SUPPLIERS

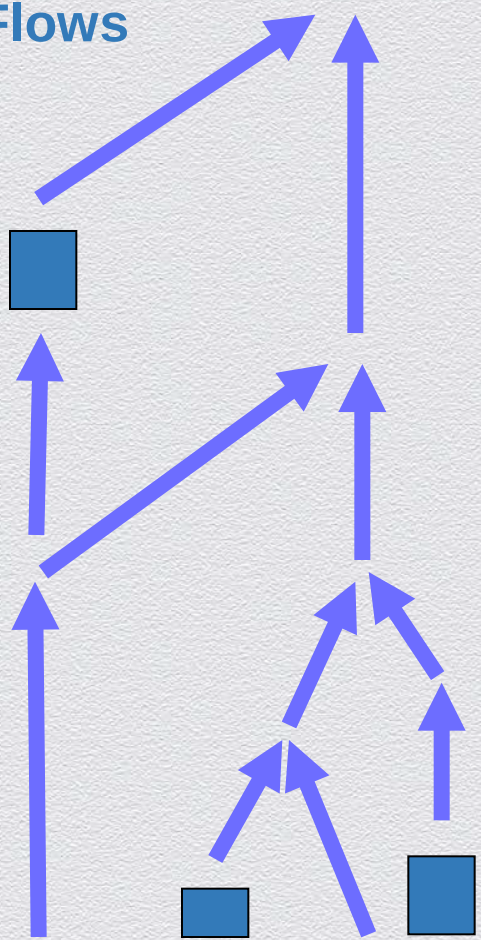
Job Two. Mapping Basic Work Flows

What **processes** supply what other processes?

What is the **capacity** of the facilities being utilized?

How large are the **inventories** between processes?

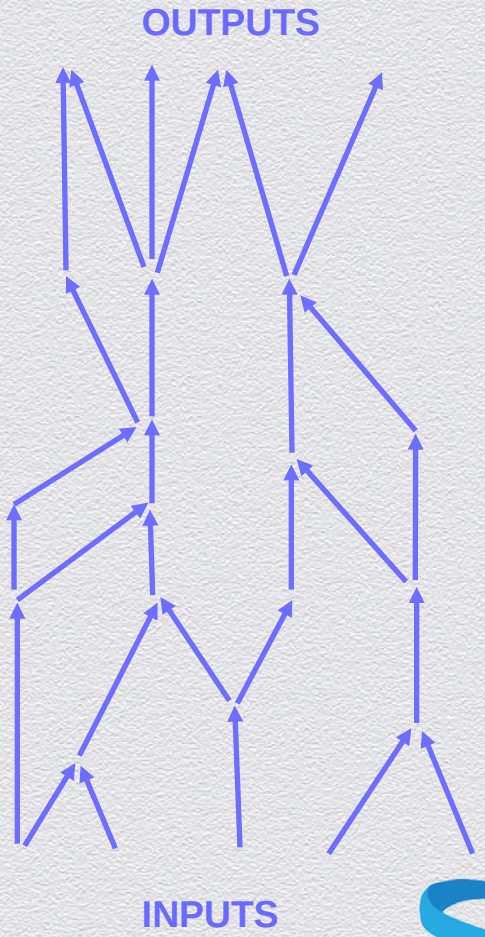
Which processes does the business do **especially well**?



Job Two Outputs: Work Flow Diagrams

Including:

- Estimates of **capacities**, **inventories**, and capacity **utilization**
- A general idea of where the outputs of a process most exceed the **value** of the inputs
- Identification of the possible **substitutes** for each process and the capacities of those substitutes

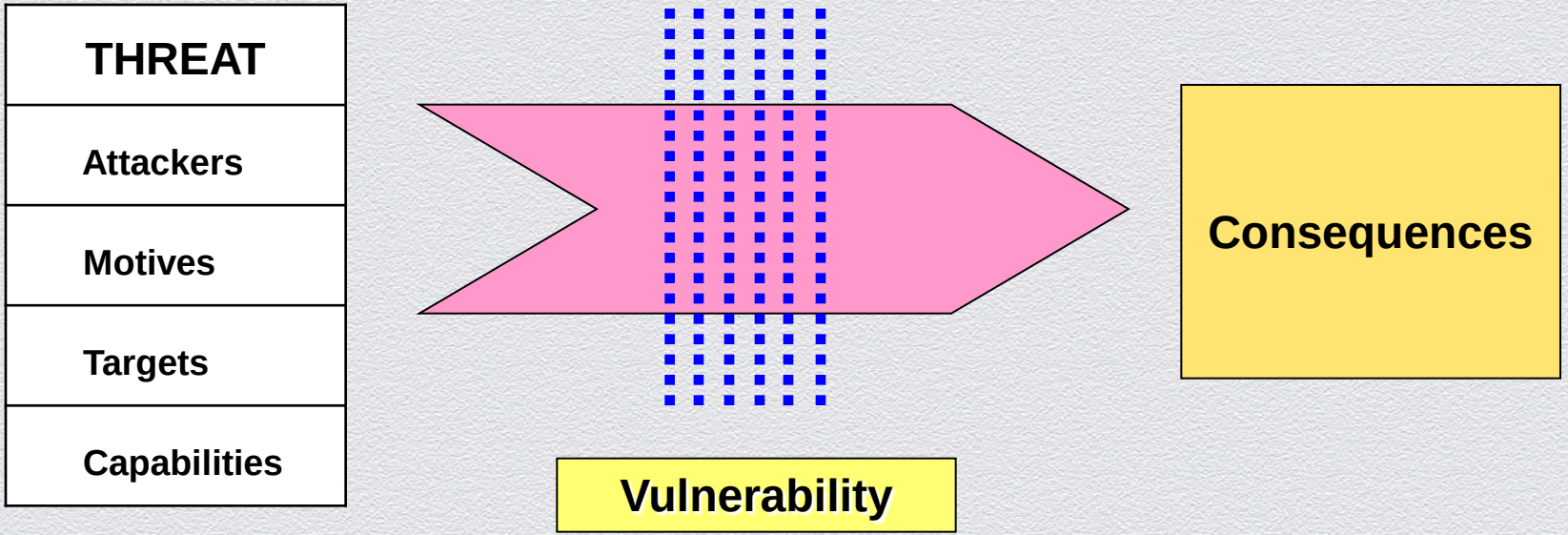


Job Three. Investigating the Three Attack Components

(actually, three overlapping jobs:)

- A. **Threat Analysis** ⟶ What kind of cyber attacks can we expect and how soon or how often?
- B. **Consequence Analysis** ⟶ What amount of loss can we expect from those attacks?
- C. **Vulnerability Analysis** ⟶ To what extent are we likely to suffer that loss, given a specified mitigation policy?

Job Three (A). Threat Analysis



Job Three (A). Threat Analysis

Predicting cyber attacks the way we would predict “black swans”

- What kind of creatures are out there?
  (The Attackers)
- What do those creatures need?
  (The Motives)
- What opportunities could those creatures exploit?
  (The Targets)
- What adaptations would allow them to exploit those opportunities?
  (The Capabilities)

Job Three (A). Threat Analysis

Tracking at least Four Types of Attacker Expertise:

Business, Vulnerabilities, Operations, Programming

EXPERTISE RATINGS FOR CYBER ATTACKS (BORG SCALE)	Comparative Score
Level Seven Expertise Nearly unique intellectual gifts or knowledge of highly secret systems	**1,000,000**
Level Six Expertise Deep insider experience or elite, specialized training	**100,000**
Level Five Expertise Substantial industry experience after a mid-level degree	**10,000**
Level Four Expertise Solid mid-level university degree in the relevant subject	**1000**
Level Three Expertise Relevant undergraduate coursework	**100**
Level Two Expertise Sustained interest in a relevant discipline	**10**
Level One Expertise A few days of web surfing by an intelligent student	**1**
Level Zero Expertise No special skill or knowledge whatsoever	**0**

Job Three (A).

Example of an American Electrical Company Assessing Likelihood of a Sophisticated Cyber-Attack on Its Large Generators

Identifying the key **thresholds** to watch!

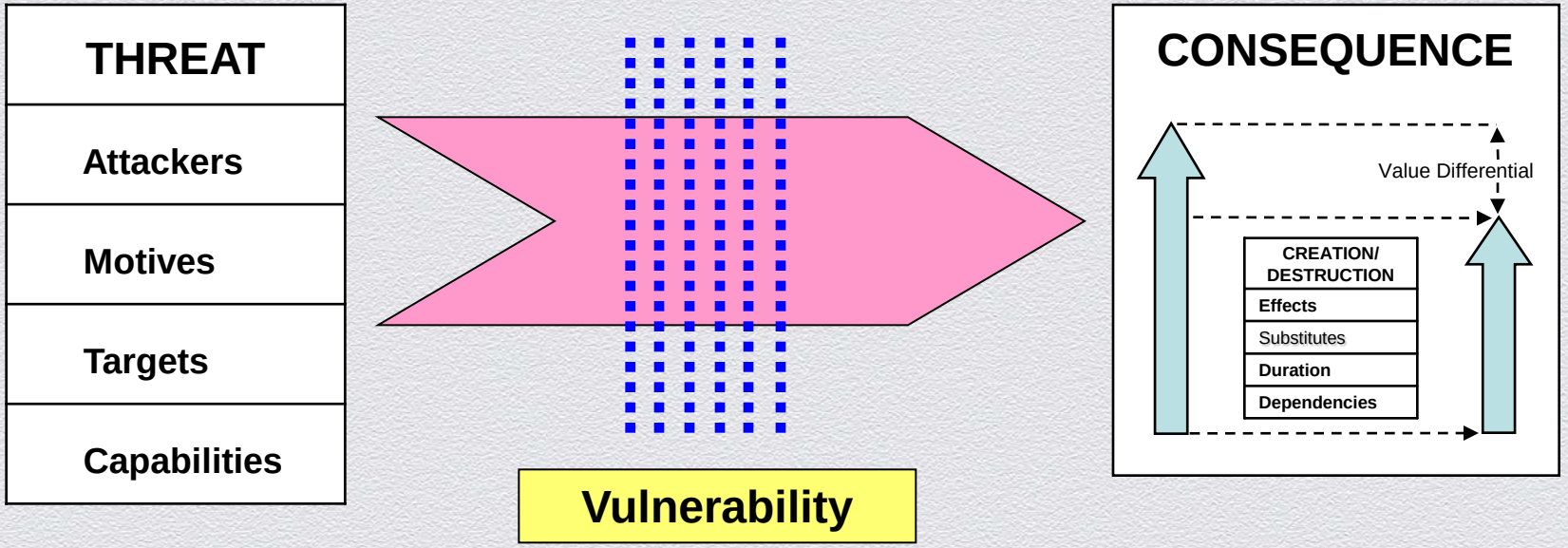
	Vindictive Insiders	Criminal Enterprises	Rogue Corporations	Ethno-nationalists	Ideological Militants	Nation States
Possible **attacker**?	Yes	Yes	Yes	Yes	Yes	Yes
Current **motivation**?	Yes	Some	**NO**	Some	Yes	**NO**
Reason to **target** this corporation?	Yes	**NO**	NO	**NO**	Some	Yes
Reason for this **type of attack**?	**NO**	Some	**NO**	Some	Yes	Some
Relevant **capabilities**?	Yes	Some	Yes	Some	**NO**	Yes
Signs of **preparation**?	NO	NO	NO	NO	Some	Yes

Job Three (A). Threat Analysis

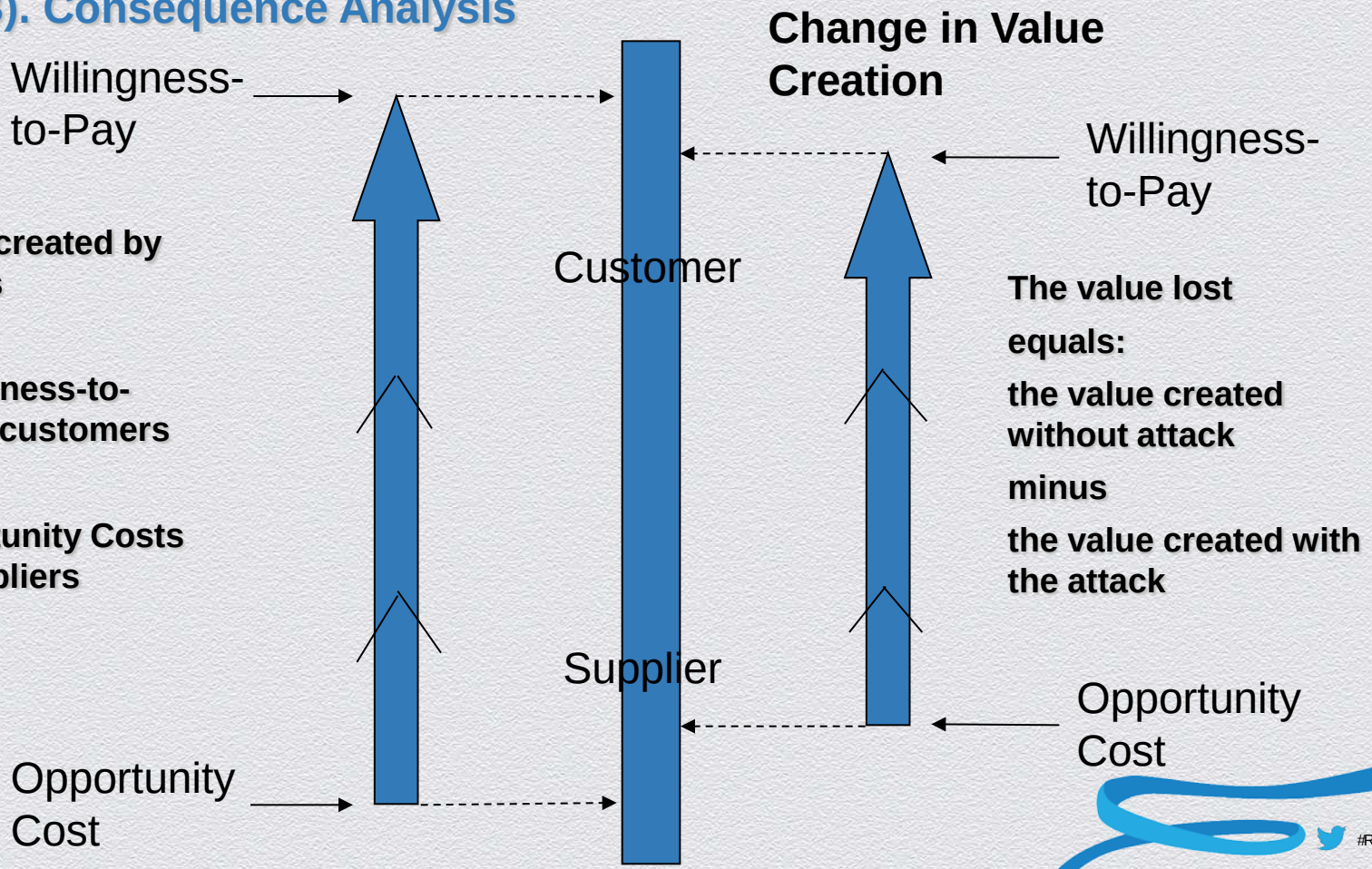
The Pivotal Timing Question:

How soon (or how often) will the mechanisms shaping the attackers activities allow the key thresholds to be crossed?

Job Three (B). Consequence Analysis

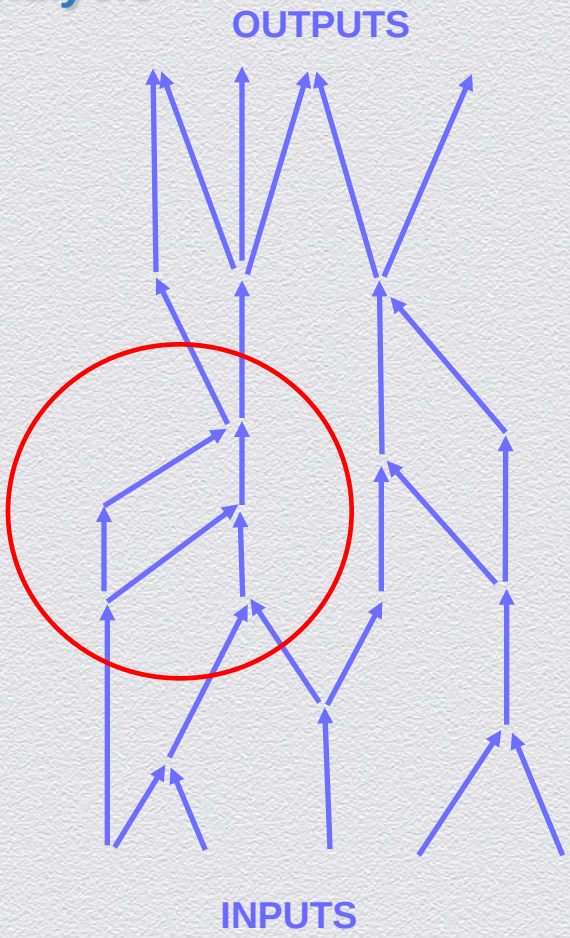


Job Three (B). Consequence Analysis

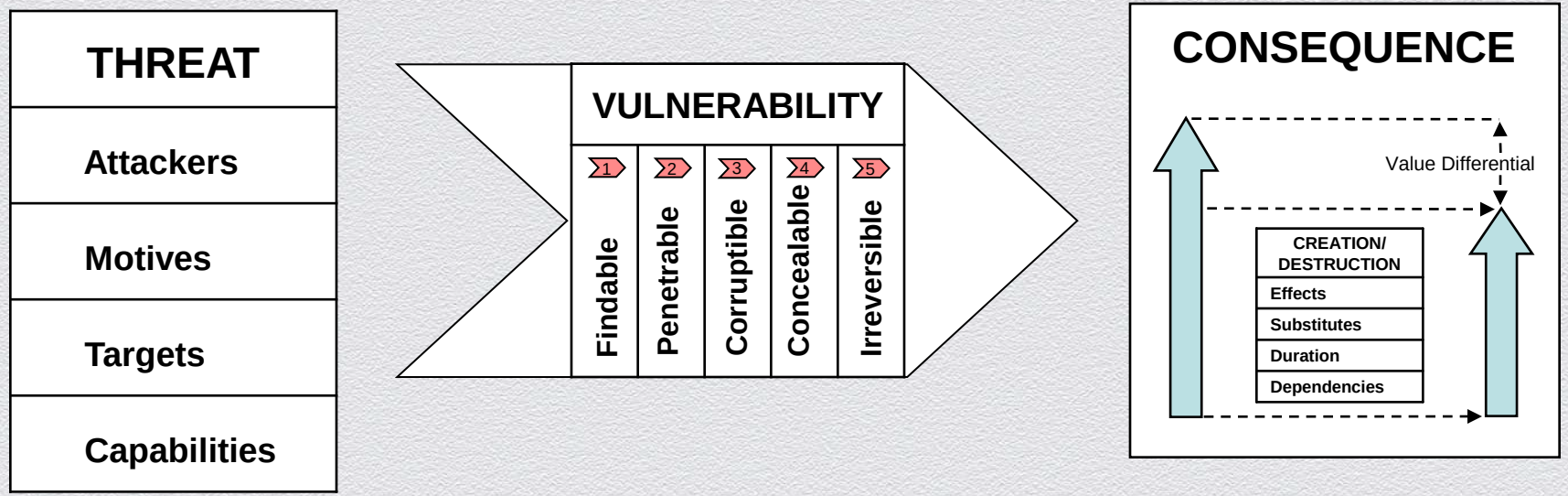


Job Three (B). Consequence Analysis

Value creation can be measured anywhere Inputs and Outputs can be measured



Job Three (C). Vulnerability Analysis



Job Three (C). Vulnerability Analysis

THE COMPREHENSIVE VULNERABILITY GRID

(BORG SYSTEM OF FIVE ATTACKER HURDLES AND SIX TYPES OF COMPONENTS)

	Findable	Penetrable	Co-optable	Concealable	Irreversible
I. Hardware Components					
II. Software Components					
III. Network Components					
IV. Automation Components					
V. Human Components					
VI. Supplier Components					

All the Potential Attack Techniques & All the Technical Counter-Measures

Job Three (C). Vulnerability Analysis

Key Factors

- The lowest-difficulty attacker path that the attackers can be expected to find
- The expertise level and duration of effort required for this attacker path
- The expected expertise level and duration of effort for a given attack attempt (from the Threat Analysis)
- The extent to which the consequence will occur, given the likely level of attacker success

Job Three Outputs: Cyber Attack Assessment Tables

Threat x Consequence x Vulnerability = Risk

Frequency of a given attack type x Potential Loss x Extent to which the loss would occur = Annualized Expected Loss

Nature of Threatened Cyber Attack	Likelihood of Serious Attempts (%)	Potential Magnitude of Loss ($)	Degree of Vulnerability with Current Policy (%)	Expected Loss with Current Policy ($)

Job Four. Evaluating Cyber Policy Options

A) Revisiting the analyses of Threats, Consequences, and Vulnerabilities to identify possible policies for ***reducing each*** of these, then

B) Recalculating: Threat x Consequence x Vulnerability = Risk, but with different policies and counter-measures in place

Nature of Threatened Cyber Attack	Likelihood of Serious Attempts with a Given Policy (%)	Potential Magnitude of Loss with a Given Policy ($)	Degree of Vulnerability with a Given Policy (%)	Expected Loss with a Given Policy ($)

Job Four Outputs: Cost-Effectiveness Priority List

An ordered list of policies and counter-measures to be put into practice, determining for each:

- **What** should be done: the **actions** to be carried out and who should do it
- **How** it should be done: the **capabilities** that would make these measures feasible
- **Why** it should be done: the **expected benefit** and a way to track and measure it

Job Five. Launching Practical Risk Reduction Programs

Written Assign-Empower-Assess Orders That Provide:

The “What” from Phase IV ⟶ **ASSIGNMENTS, specifying:**

1) Tasks, 2) Position(s), 3) Motivation

The “How” from Phase IV ⟶ **EMPOWERMENTS, securing the needed:**

4) Expertise, 5) Information, 6) Resources, 7) Authority

The “Why” from Phase IV ⟶ **ASSESSMENTS, providing the means for:**

8) Scrutiny, 9) Evaluation, 10) Replacement

Reviewing: The Five Phases in Implementing Quantitative Risk-Based Approach

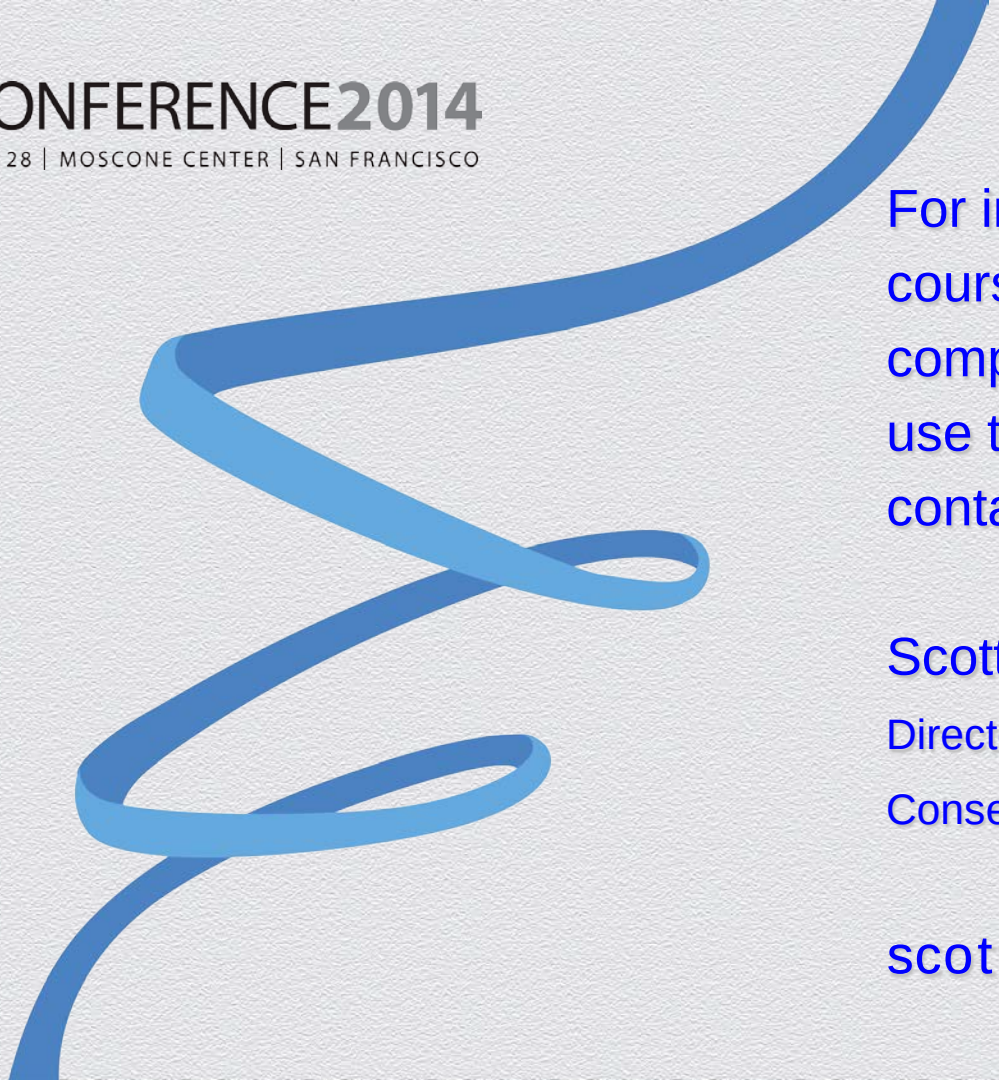
- **Phase I. Expanding the Vision**
  - → **A Plan of Action**
- **Phase II. Mapping the Business**
  - → **Work Flow Diagrams**
- **Phase III. Investigating the Three Risk Components**
  - → **Cyber Attack Assessment Tables**
- **Phase IV. Evaluating Policy Options**
  - → **Cost-Effectiveness Priority List**
- **Phase V. Launching Practical Programs**
  - → **Assign-Empower-Assess Orders**

Distinctive Features of This Overall Approach

- Completely transparent and publicly available
- Clear, demonstrably valid foundations
- Any scale of organization or system
- Any level of depth and detail (thoroughly iterative)
- Fully modular (alternative possibilities for every component)
- Realistic about available information
- Dynamic, process-oriented
- Produces many more options for policies and counter-measures
- Yields classic, quantitative, risk-analysis results

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



For information on day-long courses on the various components or permission to use this material, please contact:

Scott Borg

Director (CEO), U.S. Cyber Consequences Unit

scott.borg@usccu.us