

Cyber Security Economics:

Are you throwing good
healthcare IT money
after bad?

Jeff Hughes

Tenet3

Dayton, OH

jeff.hughes@tenet3.com

HiMSS

CENTRAL & SOUTHERN OHIO *Chapter*



Tenet3 Overview

- A cyber security analytics company
 - Visualizing “Big Cyber”
 - Providing strategic analysis
- We develop models and metrics to assess
 - Threat mitigation strategies
 - Security costs
 - » Defender vs. Adversary costs
 - Residual risks
 - Resiliency



Today's Learning Objectives

- 1) Cyber Security Market Fundamentals
 - The forces at play
- 2) Current State-of-the-Art Guidance in Cyber Risk Management
- 3) Cyber Security Economics Defined
- 4) A Quantitative Framework to Capture the “Time is Money” Trade Space
 - a. Characterizing the Threat
 - b. Addressing a Threat's Time-to-Compromise
 - c. Threat Driven Metrics: Compute Defender versus Adversary Work Factor
- 5) Getting Started on Your Solution

Cyber Security Market Fundamentals

The Forces at Play

Cyber Security Market Fundamentals

First

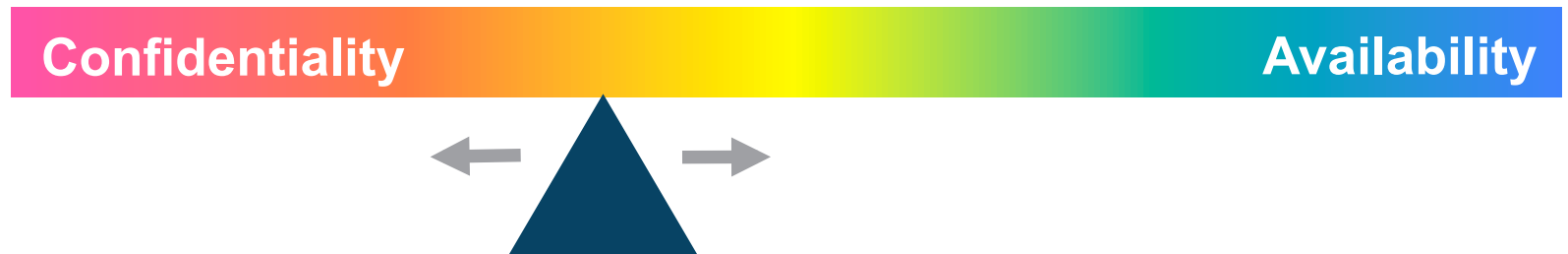
- Cyber Security is more than the information technology (IT) employed
 - It is a function of:
 - Business processes (both required and latent)
 - Personnel cyber-related work habits (both good and bad)
- Security “best practices” can be at odds with efficient operations
 - A complex and competing mix of technology, processes, and personnel

Cyber Security Market Fundamentals

Second

- Availability usually trumps Confidentiality and data Integrity concerns
- New IT technologies introduce new vulnerabilities
 - New software and hardware inevitably have new bugs
 - Secure coding and trusted hardware is a languishing desire
- “Time to market” and global economies of scale overtake security
 - especially when residual risk versus security impact or value is unclear

Cyber Security Market Fundamentals



Contrary to security dogma

- It's a Trade Space!

- The organizational mission drives the balancing point

Cyber Security Market Fundamentals

Third

- We rely too broadly on
 - Point solutions
 - Static compliance checklists

- You can't fix what you can't measure
 - Need quantitative metrics to guide a cyber security cost/benefit trade space

Our Approach to Metrics Builds on Published Results

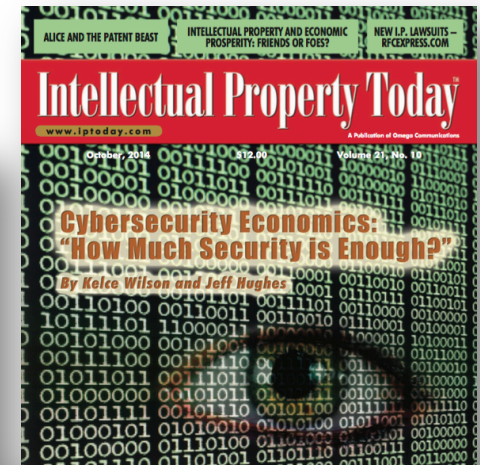
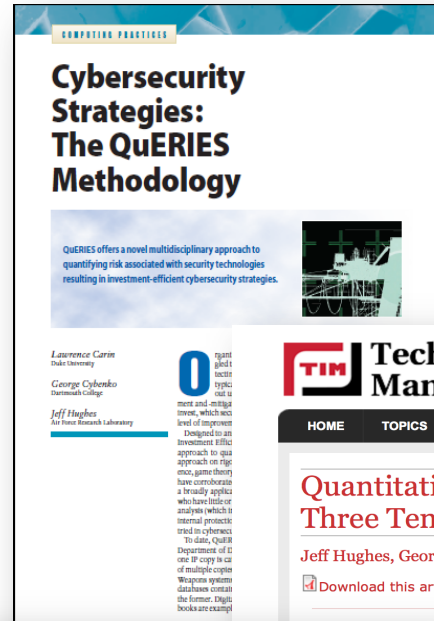
IEEE Computer Magazine
August 2008

Technology Innovation Management Review
Summer 2013

SPIE Defense+Security Conference
May 2014

Intellectual Property Today
October 2014

Moving Target Defense Workshop,
Association for Computing Machinery
November 2014



No Free Lunch in Cyber Security

George Cybenko
Thayer School of Engineering, Dartmouth
College
Hanover, NH 03755 USA
gvc@dartmouth.edu

Jeff Hughes
Tenet3
Dayton, Ohio USA
jeff.hughes@tenet3.com

ABSTRACT

Confidentiality, integrity and availability (CIA) are traditionally considered to be the three core goals of cyber security. By developing probabilistic models of these security goals we show that:

- the CIA goals are actually specific operating points in a continuum of possible mission security requirements;
- component diversity, including certain types of Moving Target Defenses, versus component hardening as security strategies can be quantitatively evaluated;
- approaches for diversity can be formalized into a rigorous taxonomy.

Such considerations are particularly relevant for so-called Moving Target Defense (MTD) approaches that seek to adapt or randomize computer resources in a way to delay or defeat attackers. In particular, we explore tradeoffs between confidentiality and availability in such systems that suggest improvements in one may come at the expense of the other. In other words, there is "No Free Lunch" in cyber security.

Categories and Subject Descriptors

K.6.5 [Security and Protection]: Unauthorized access

Keywords

Security metrics; formal models; confidentiality; integrity; availability; diversity; moving targets

1. INTRODUCTION

This paper develops a quantitative framework for modeling diversity and showing how diversity can affect the cyber security goals of systems and missions, including confidentiality, integrity and availability (CIA) individually as special cases. We develop probabilistic models for diversity and

each of the CIA goals using the *time-to-compromise* as a variable for when a component is successfully attacked, allows us to demonstrate that there are quantitative intuitively clear consequences of diversity when define the CIA goals against both single and multiple attacks. In particular, it is shown how the probabilistic see properties of components relate to the security proper systems built out of those components. As such, we develop the beginnings of a cyber security analog of reliability engineering.

A major contribution of this paper is that it offers a intuitive bounds on employing diversity. We show that certain types of diversity may offer no added security be when the systems are being attacked by multiple advers These results illustrate a promising approach for more pure versus diversity cost/benefit trade space analyses.

1.1 Previous Work

Previous discussions about monoculture and diverse the context of information assurance and cyber security be found in [12, 3, 16, 8, 20]. That body of work is a qualitative rather than quantitative, appealing in es to institutions and similarities with biological diversity.

Mathematical aspects of diversity and especially a limits to diversity have been studied in the mathema biology literature [11, 10, 1]. That work addressed the portant question of how much diversity can exist in the when the resource types in an environment are constra At this time, we are not aware of corresponding analy computing systems' diversity from the point of view of much diversity is sustainable in a particular comput ecosystem.

1.2 Organization of the paper

After this introduction, we introduce and review so our underlying concepts in Section 2. Section 3 con the main results concerning quantitative modeling of diversity context of the CIA security goals. Section 4 is a summary results together with ideas for future work. The App contains additional details of derivations of the results

Risk comes from not knowing what you're doing.

Warren Buffett

Three Tenets for Secure Cyber-Physical System Design and Assessment

JEFF HUGHES
Tenet3
and
GEORGE CYBENKO
Dartmouth College

ABSTRACT: This paper presents a threat-driven quantitative methodology for secure cyber-physical system design and assessment. Called *The Three Tenets*, this originally empirical approach has been refined with a mathematical formulation. It has been used by the US Air Force Research Laboratory (AFRL) for secure system research and development. The *Tenets* were first documented in 2005 as a teachable methodology. The *Tenets* are motivated by a system threat model that itself consists of three elements which must exist for successful attacks to occur:

- system susceptibility;
- threat accessibility and;
- threat capability.

The Three Tenets arise naturally by countering each threat element individually. Specifically, the tenets are:

- Tenet 1: Focus on What's Critical* - systems should include only essential functions (to reduce susceptibility);
- Tenet 2: Move Key Assets Out-of-Band* - make mission essential elements and security controls difficult for attackers to reach logically and physically (to reduce accessibility);
- Tenet 3: Diversify* - systems should include diverse components (to reduce threat capability).

Current State-of-the-Art Guidance in Cyber Risk Management

Current State-of-the-Art Guidance in Cyber Risk Management

Risk Management Framework

- 5 principal functions necessary to implement a strong security methodology:
 - identify, protect, detect, respond, recover.
- Associated with these 5 functions are:
 - 22 activity categories
 - 98 subcategories, and
 - 224 possible security controls to apply
- Controls are prioritized as P1, P2, P3, and P0
 - P1 meaning "priority one"
 - P0 meaning no priority specified
- **Out of the 224 itemized security controls:**
 - **121 controls are labeled as P1**

Beyond a Framework: Cost Effective Security Strategies

- Significant \$\$\$ in the industry is spent on cyber SA
 - It is important
 - It is typically a tactic
- Few \$ are spent on cyber strategy
 - At least as important
- Lessons learned from Department of Defense
 - Need both

Our Thesis:

Apply Quantitative Metrics to Assess Strategies

- Simple questions have been difficult to answer:
 - “How much security is enough?”
 - “Are you throwing good money after bad?”

- Without a “yardstick” it’s hard to measure progress
 - We need cyber security economic metrics

Cyber Security Economics Defined

Cyber Security Economics

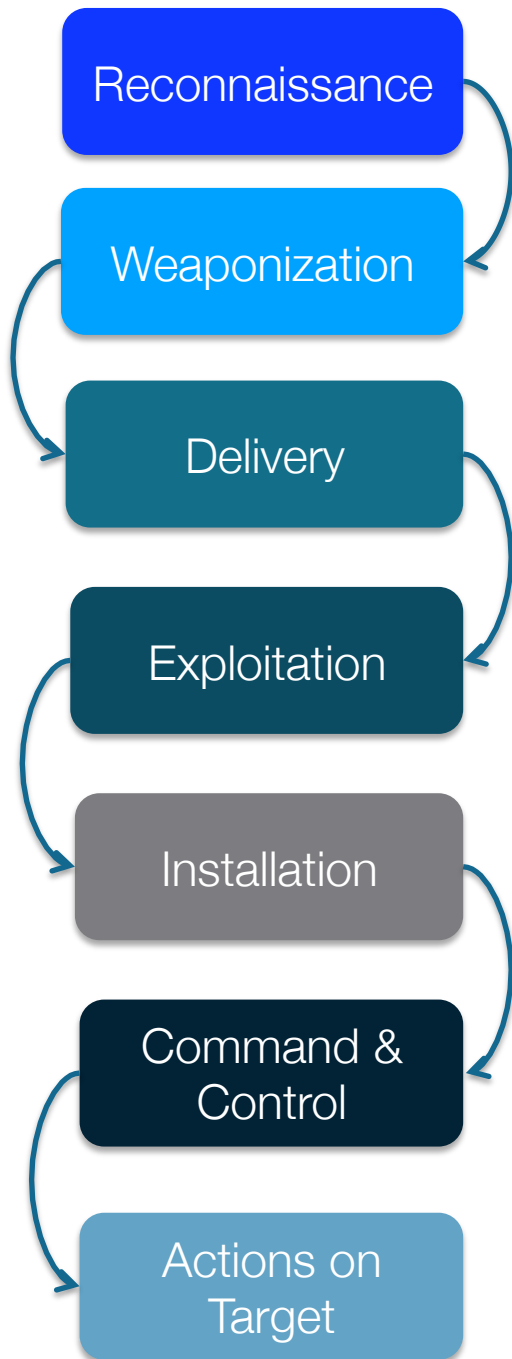
- Economics of Cyber Security
 - Time \propto Money

- Once you can estimate Time, the economic analysis is straightforward:
 - Time to compromise
 - Time to maintain
 - Time to repair/recover

A Quantitative Framework to Capture the “Time is Money” Trade Space

- a. Characterizing the Threat
- b. Addressing a Threat’s Time-to-Compromise
- c. Threat Driven Metrics: Compute Defender versus Adversary Work Factor

Cyber Kill Chain



Timeline

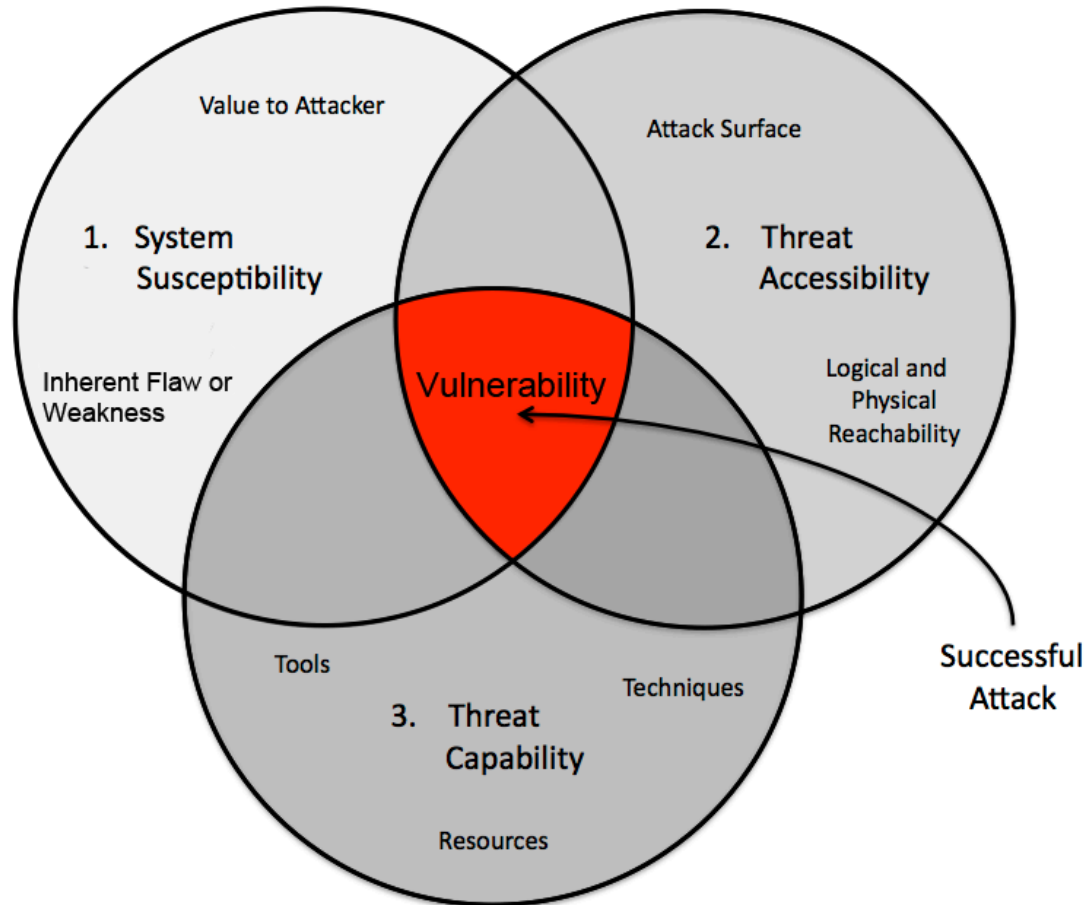


“Costing” the Kill Chain requires characterizing what enables the threat

Characterizing the Threat

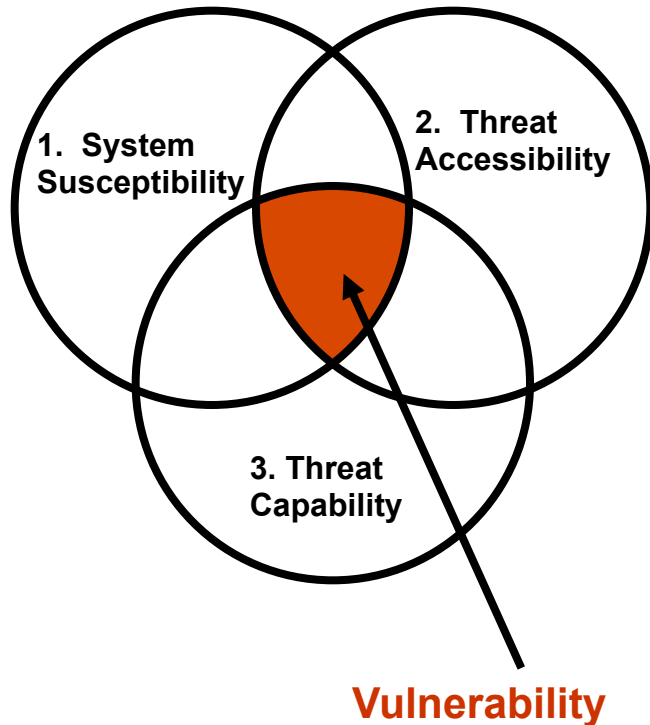
A system is vulnerable if:

- The system has points of **susceptibility** that can be attacked/exploited
- The threat can get **access** to one or more of these susceptibility points
- The threat has the **capability** to do harm to the system once they get access



Cost (and Time) Imposing Threat Mitigations

Threat Model



3 Tenets

- 1. Focus on what's critical**
 - Reduce scope of what to protect; Minimize # of system security elements; Match the tool to the job
- 2. Move it 'Out of Band'**
 - Make what's critical and associated security elements less accessible to adversary
- 3. Detect, React, Adapt**
 - Deny threat attack vectors & tools; Deny adversary reverse engineering capabilities; Impose hard penalties when detected (stay inside threat's OODA loop!)

The Cost of Risk Mitigation

- Economics of Cyber Security

Time \propto Money

- Once you can estimate Time, the economic analysis is straightforward:

- Time to compromise
- Time to maintain
- Time to repair / recover



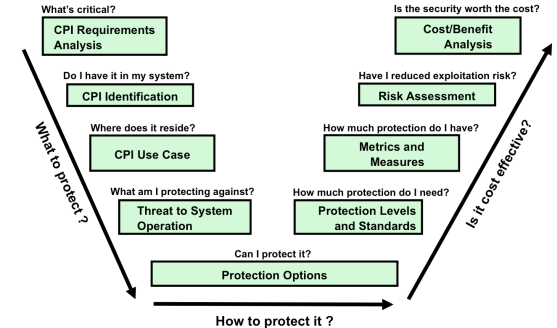
Defender vs. Adversary Work Factor

- Time spent by bad guys to break
 - **Adversary work factor**
- Time spent by good guys to build/maintain/recover
 - **Defender work factor**
- Enable analysis showing ways to
 - **Lower defender** ('composer') **work factor**
 - **Increase adversary** ('decomposer') **work factor**
- Display the delta between defender and attacker work factors
 - In various parts of the system
 - For various defensive countermeasures

Estimating Adversary Work Factors

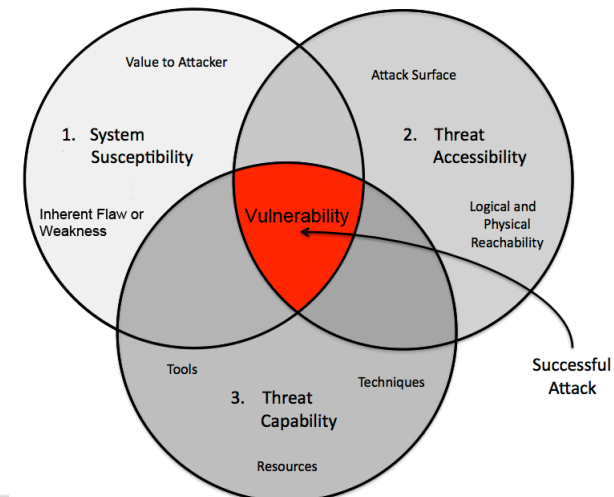
Blue Team uses threat model plus system engineering V-diagram to estimate work factor associated with security implementation:

- 1) time to protect
- 2) time to maintain once protected



Red Team uses threat model plus penetration testing and reverse engineering data to estimate adversary work factor:

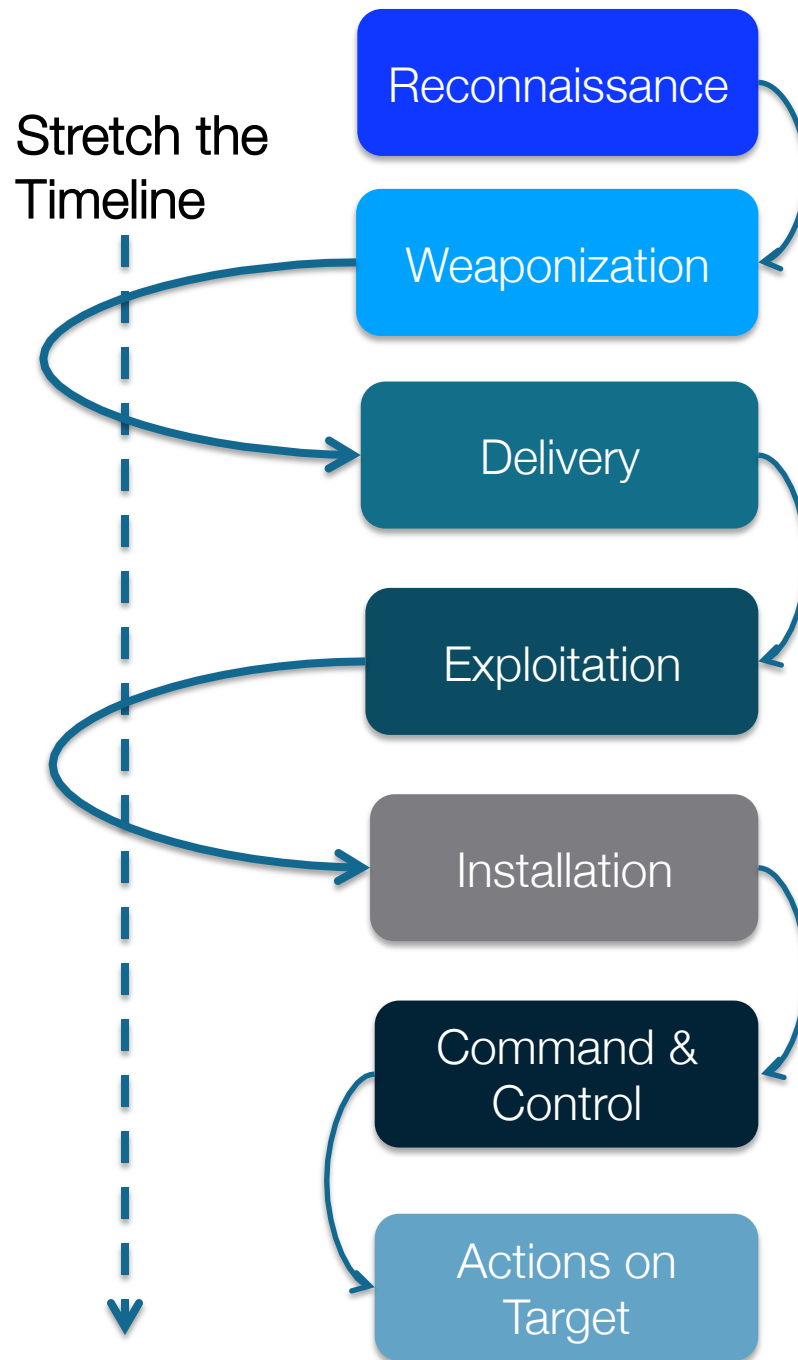
- 3) first time to break
- 4) n^{th} time to break for multiple system instantiations



Methods to Estimate Adversary Work Factor

- Reverse Engineering Exercises
 - Wall clock
- Penetration Testing
 - Wall clock
- Cryptographic Methods
 - Calculated time
- Information Markets
 - Relative time
- Heuristics
 - Relative time

Effect on Cyber Kill Chain



The Cost of Resilience

- Economics of Cyber Security

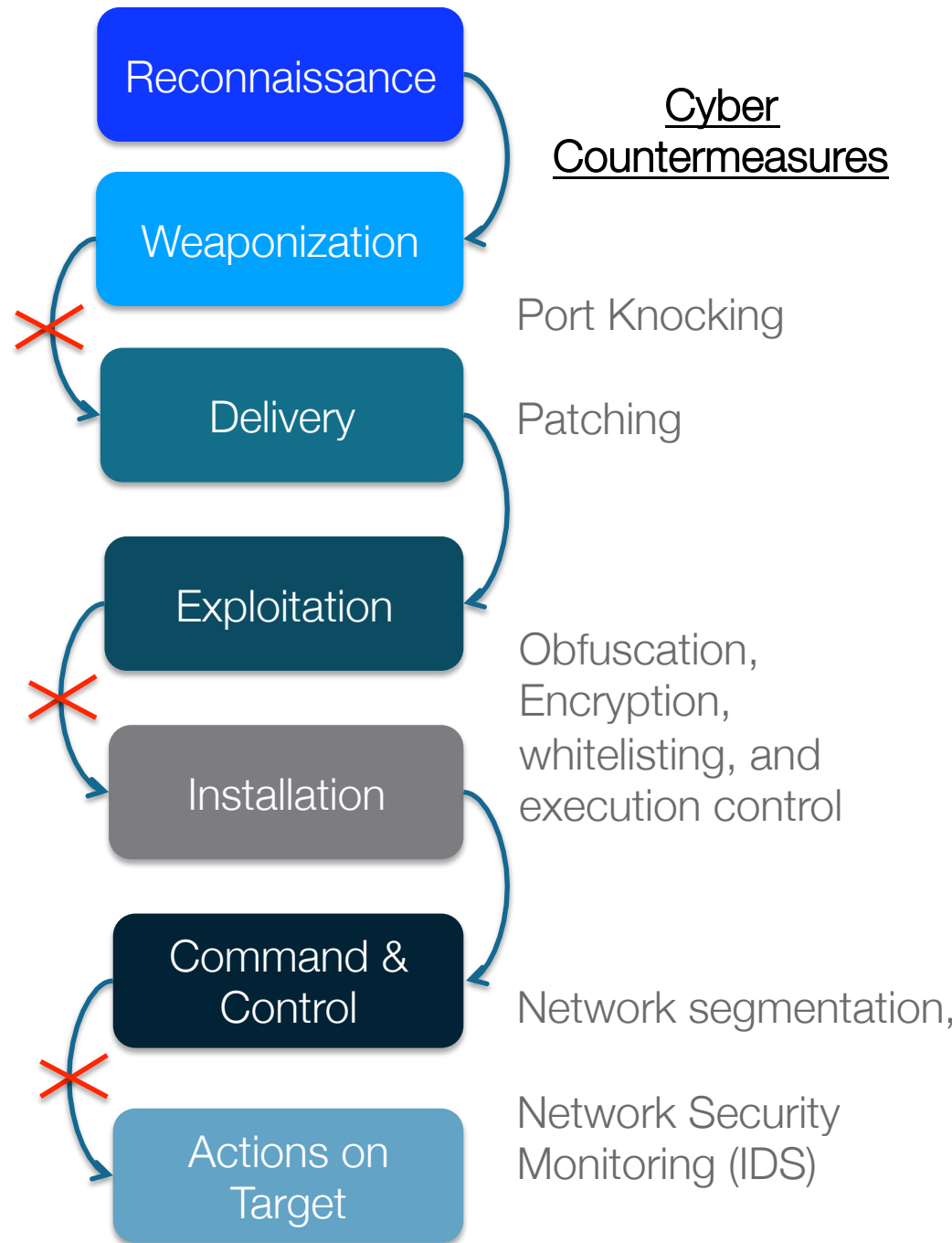
Time \propto Money

- Once you can estimate Time, the economic analysis is straightforward:
 - Time to compromise
 - Time to maintain
 - **Time to repair / recover**

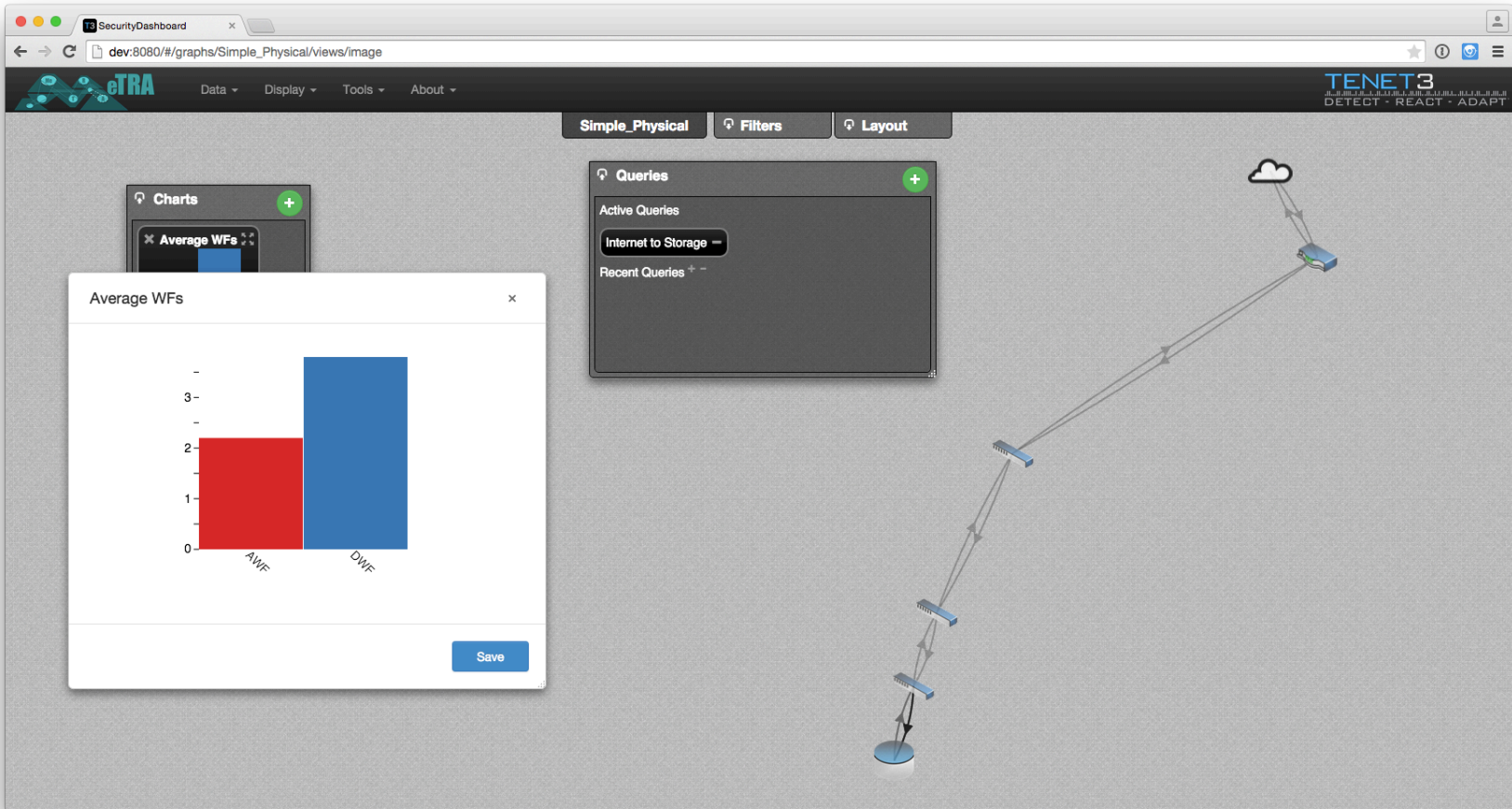


Effect on Cyber Kill Chain

Identify
“Work Factor”
Effective
Countermeasures

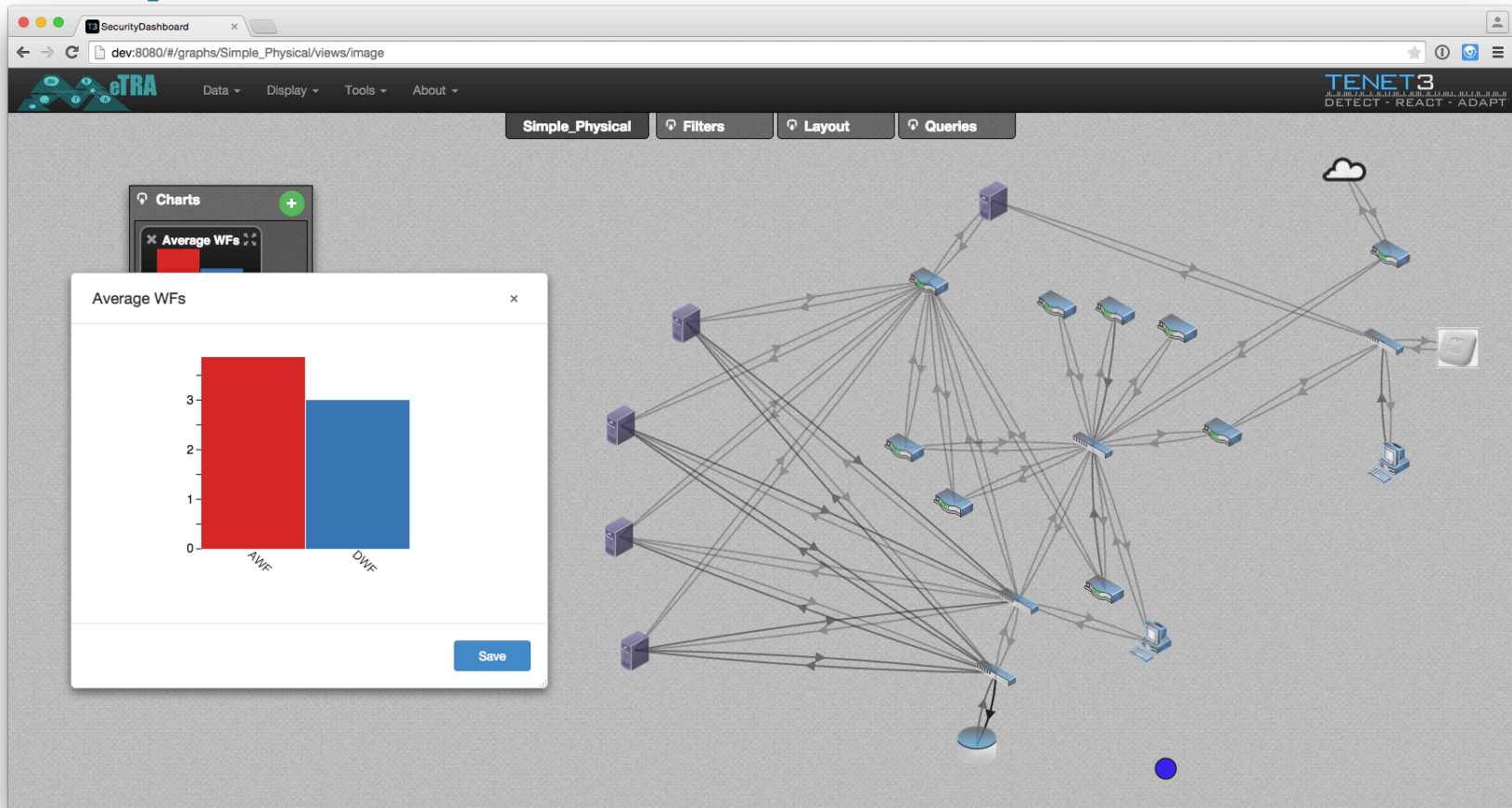


Compute Metrics Along an Attack Path



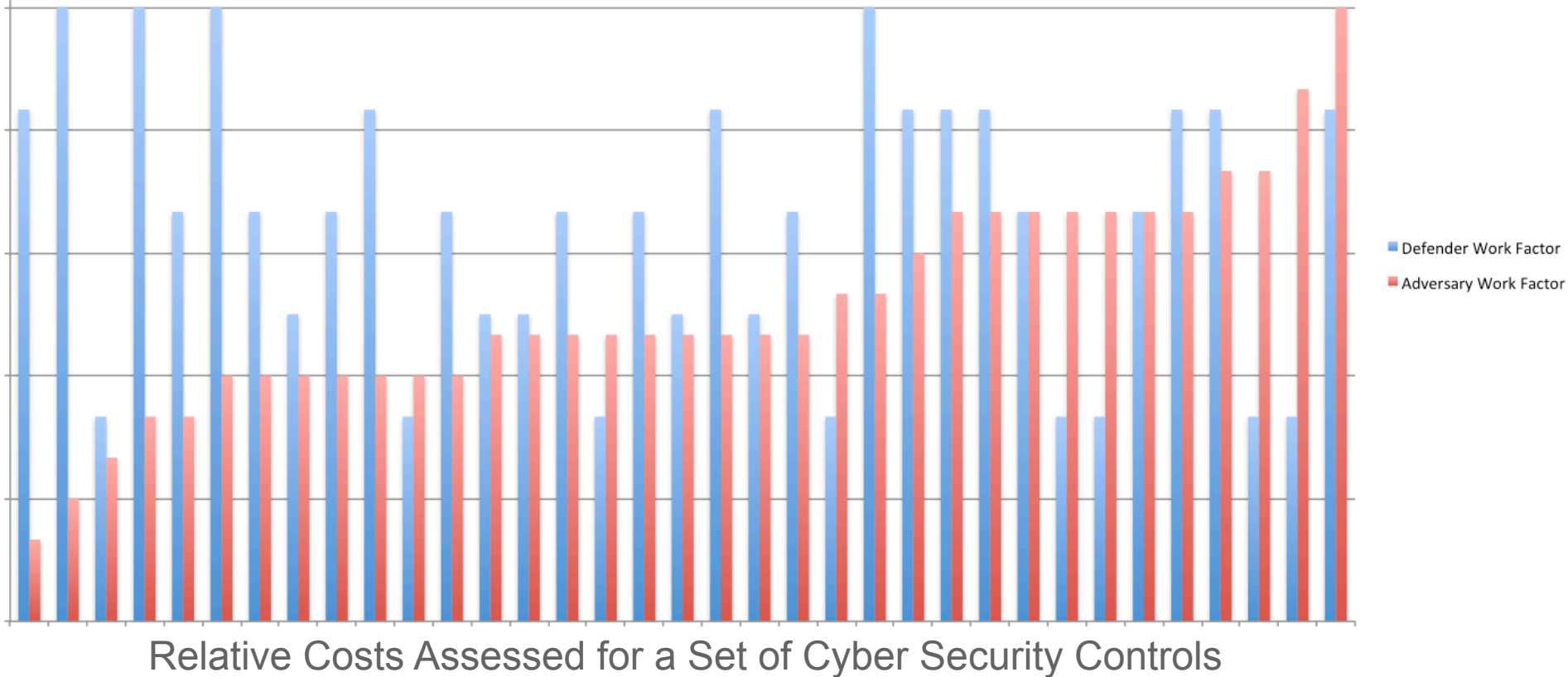
Here we track average adversary vs defender work factor along a specific attack path. This analysis highlights a case where the defender is spending more than the attacker. The defender return on investment is poor.

Compute Metrics Across an Entire Network



Here we track average adversary vs defender work factor. This type of analysis can associate threat time-to-breach, or time-to-move laterally within a network versus defender time-to-protect and maintain. Overall it costs the adversary more to attack.

Three Tenet Compliance Can Estimate Cost to Defend vs. **Cost to Hack**



Getting Started on Your Solution

Strategy Begins with Taking Stock

- Inventory your stuff
- Organize it
- Show how it's connected

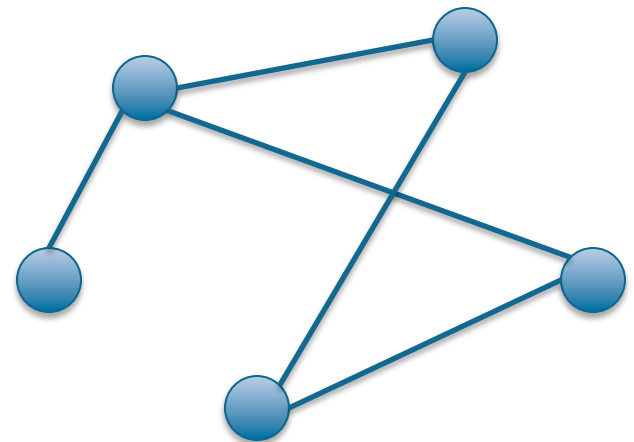
Strategy Begins with Taking Stock

- Inventory your stuff
- Organize it
- Show how it's connected

Count

Collect

Connect



Consider Resilience to the Future Threat

- Today's threat
 - Demonstrated exploits
 - Compliance based mitigations
 - Tactical response
- Tomorrow's threat
 - Zero day / postulated
 - “Work Factor” based resilience
 - Strategic planning

Extend Work Factor Assessment to the Enterprise

	Dependent	Independent
Homogeneous	No Diversity (Monoculture)	Artificial Diversity
Heterogeneous	Pseudo Diversity	Natural (True) Diversity

Is a Monoculture Secure?

There's a trade between maintainability and brittleness.

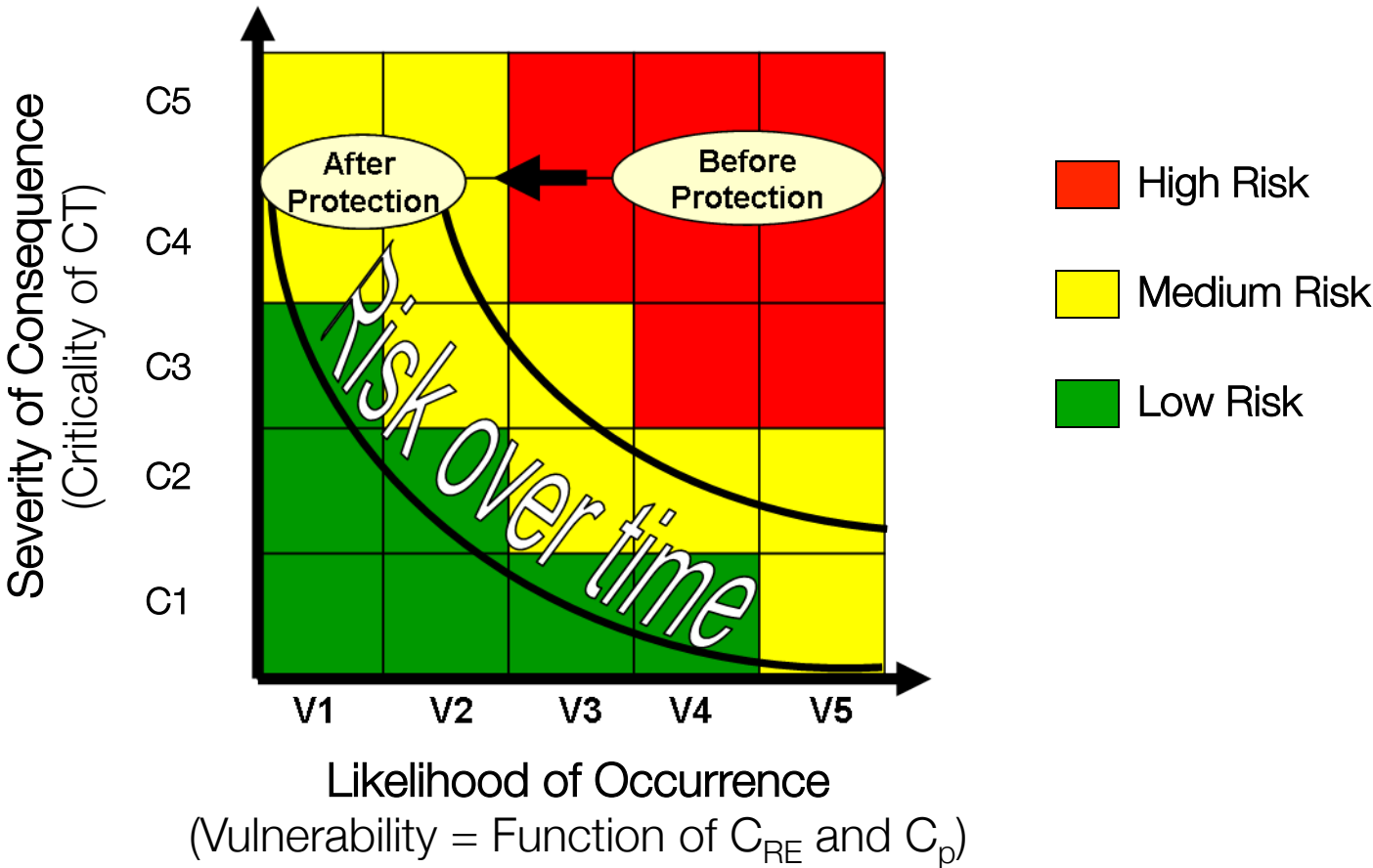
Extend Work Factor Assessment to the Enterprise

	Dependent	Independent
Homogeneous	No Diversity (Monoculture)	Artificial Diversity
Heterogeneous	Pseudo Diversity	Natural (True) Diversity

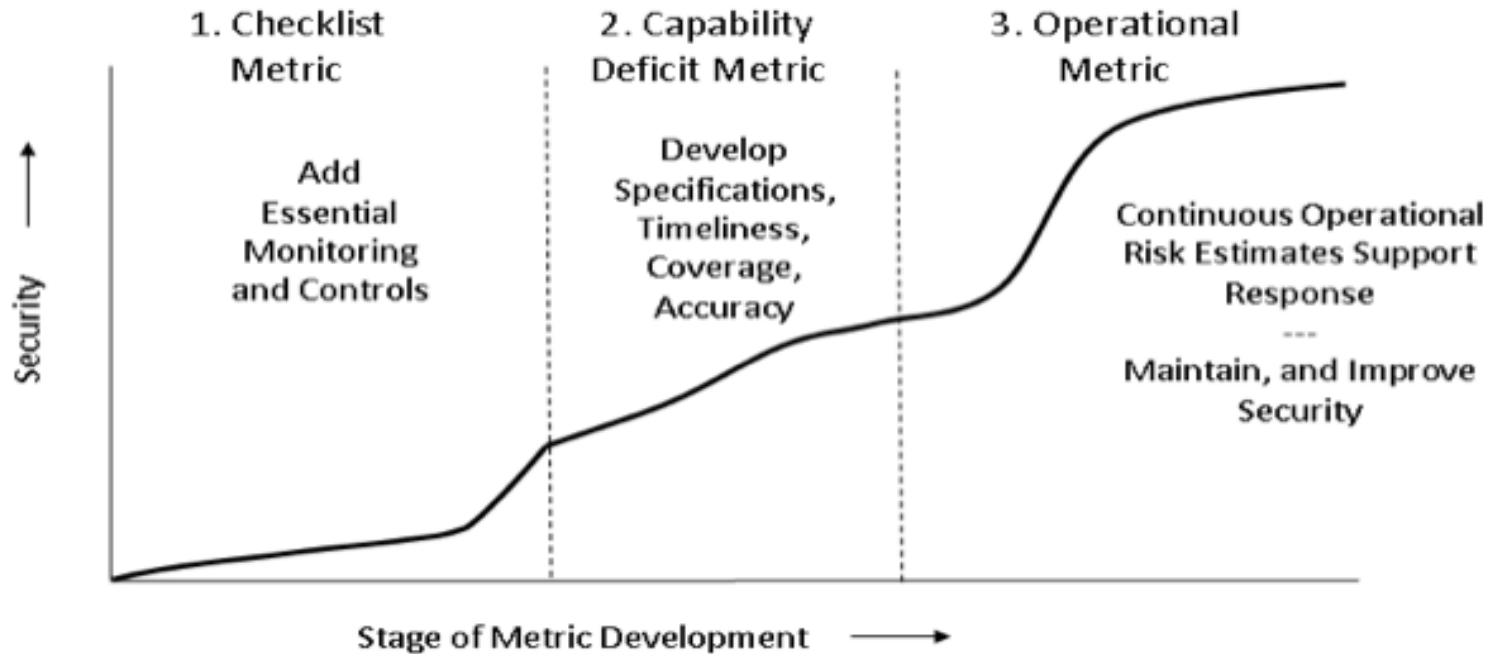
Is a Monoculture Secure?

There's a trade between maintainability and brittleness.

Consider the Value Proposition “Over Time”



Evolve Your Security Metrics



MIT/LL Metric Maturity Model

Summary: Cyber Security Economics

- Cyber security economics largely depends on:
 - Time spent by the bad guys to break
 - Time spent by the good guys to maintain / recover

Explicit time assessments and
quantitative security metrics clarify your
investment cost / benefit trades

Final Take Away

- Count, Collect, Connect to understand your current risk posture
- Develop “Work Factor” strategy
- Estimate “Work Factor” costs
- Quantify your value proposition