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

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

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

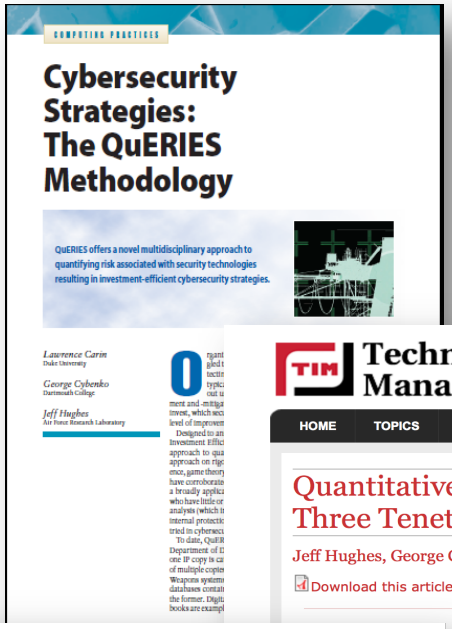
IEEE Computer Magazine
August 2008

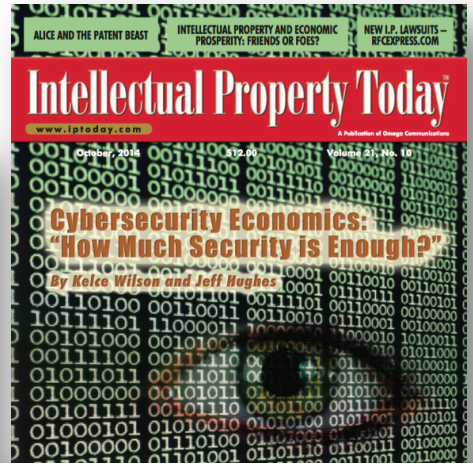
Technology Innovation Management Review
Summer 2013

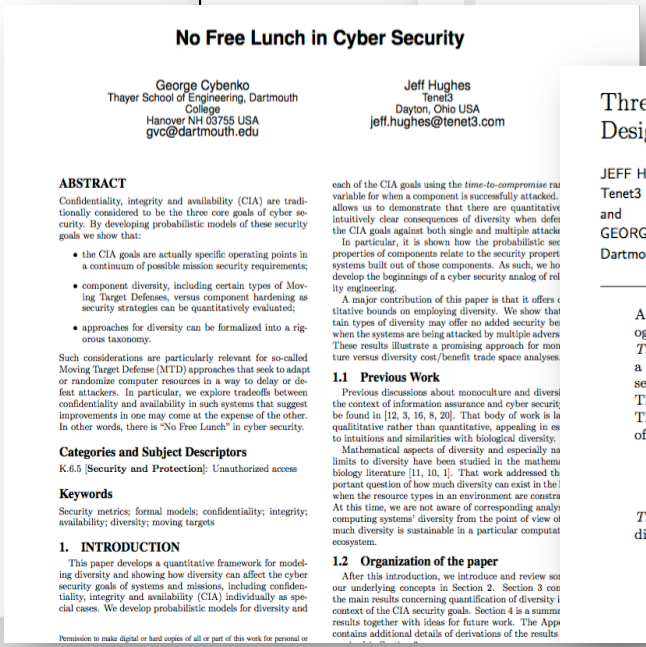
SPIE Defense+Security Conference
May 2014

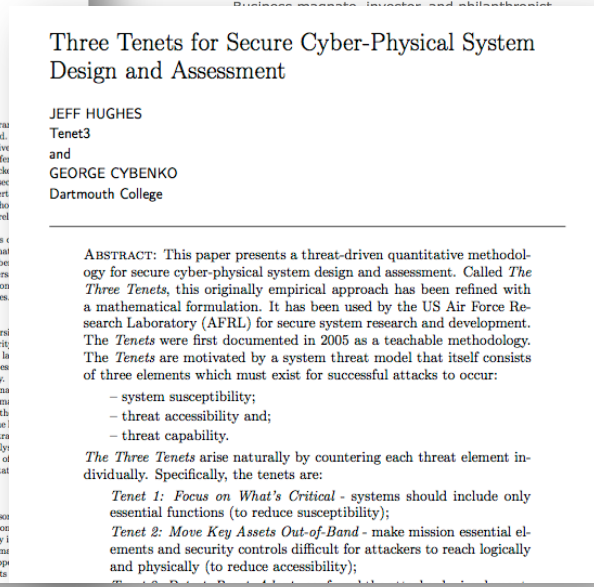
Intellectual Property Today
October 2014

Moving Target Defense Workshop, Association for Computing Machinery
November 2014









HIMSS
CENTRAL & SOUTHERN OHIO Chapter

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

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

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

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

Cyber Security Economics

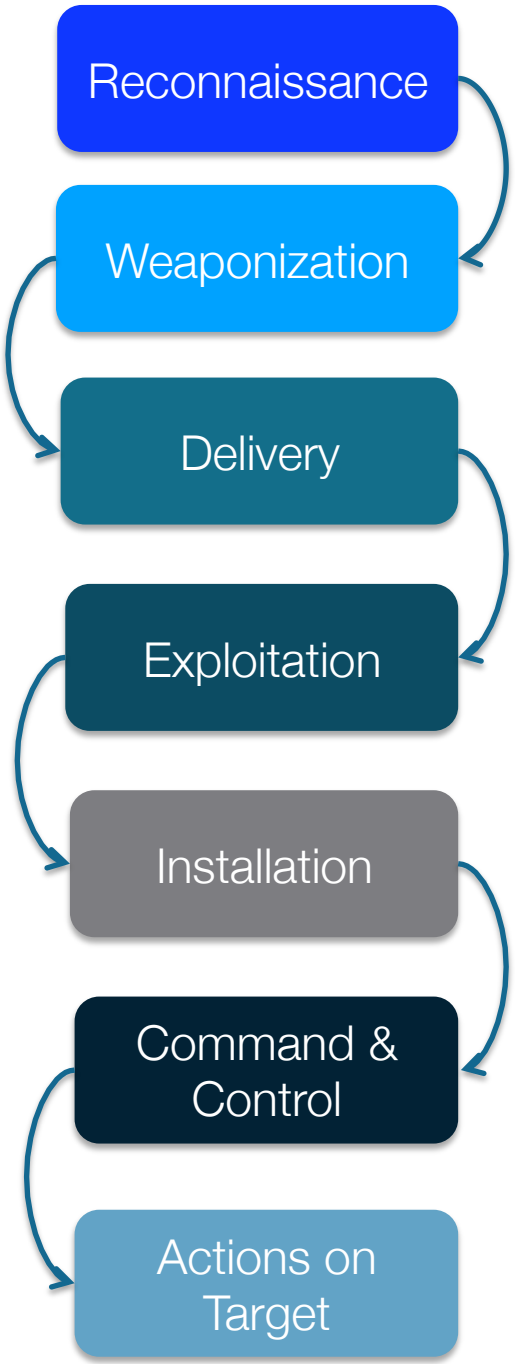
- Economics of Cyber Security
  - Time $\propto$ Money
- Once you can estimate Time, the economic analysis is straightforward:
  - Time to compromise
  - Time to maintain
  - Time to repair/recover

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

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

Cyber Kill Chain

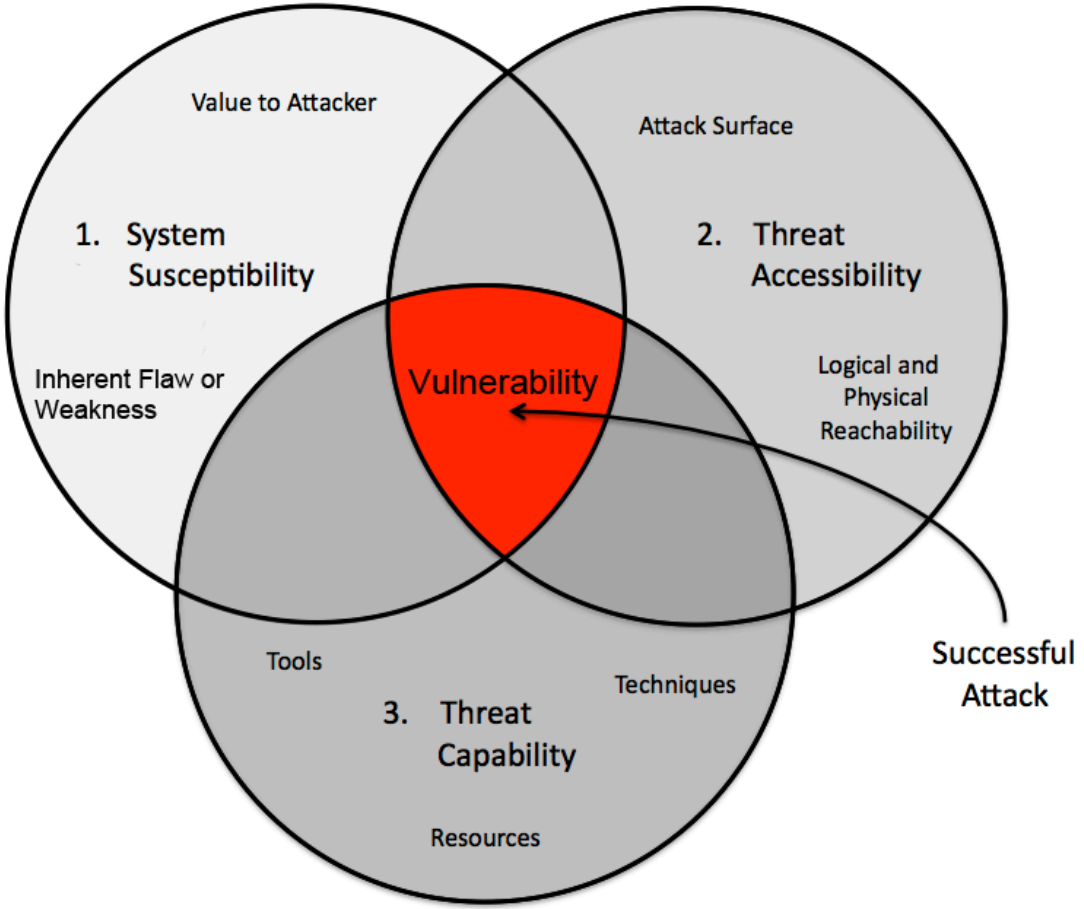


"Costing" the Kill Chain requires characterizing what enables the threat

Characterizing the Threat

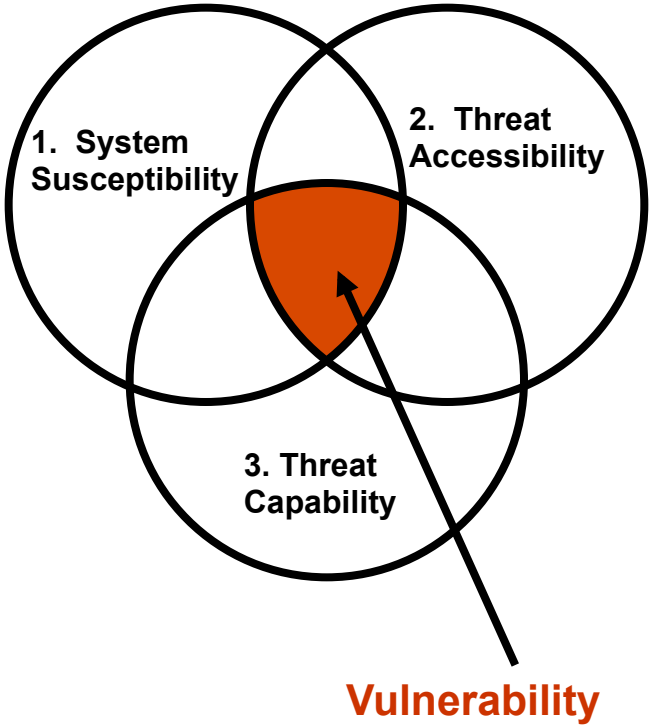
A system is vulnerable if:

- 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**

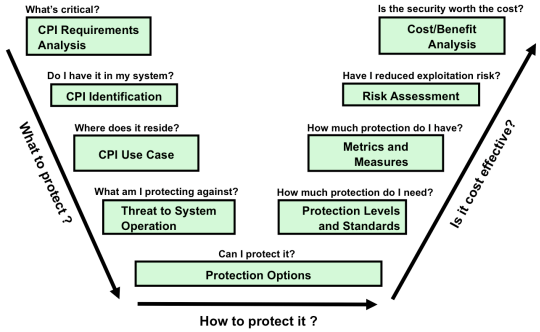
- Enable analysis showing ways to
  - **Lower defender** (‘composer’) **work factor**
  - **Increase adversary** (‘decomposer’) **work factor**

- Display the delta between defender and attacker work factors
  - In various parts of the system
  - For various defensive countermeasures

Estimating Adversary Work Factors

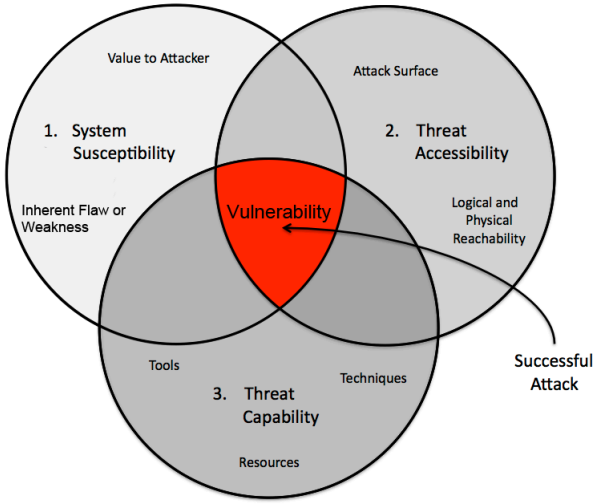
Blue Team uses threat model plus system engineering V-diagram to estimate work factor associated with security implementation:

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:

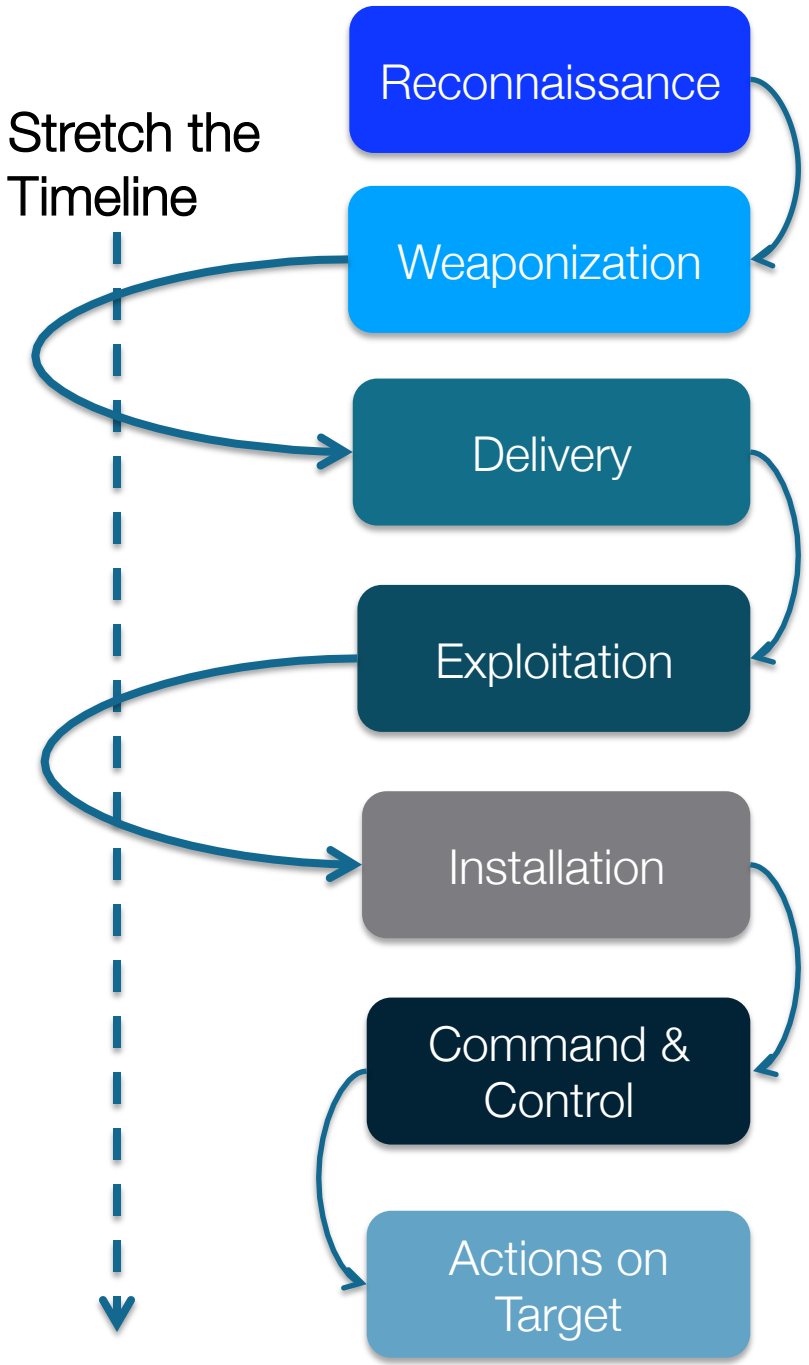
3) first time to break
4) n^{th} time to break for multiple system instantiations



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

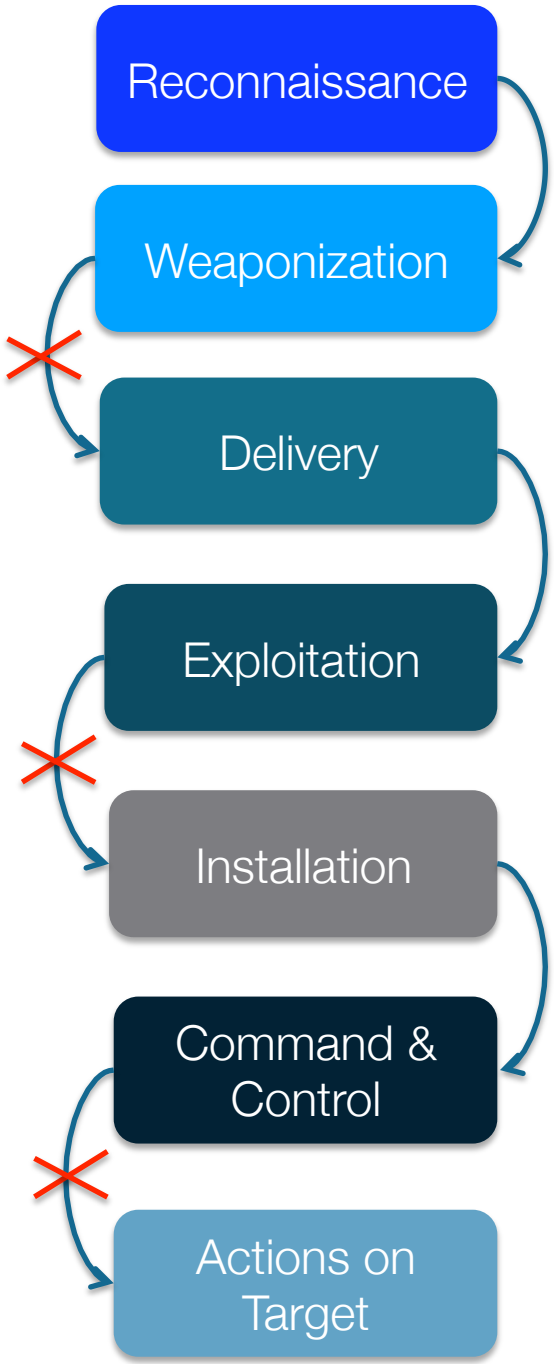
- Economics of Cyber Security

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



Cyber Countermeasures

Port Knocking

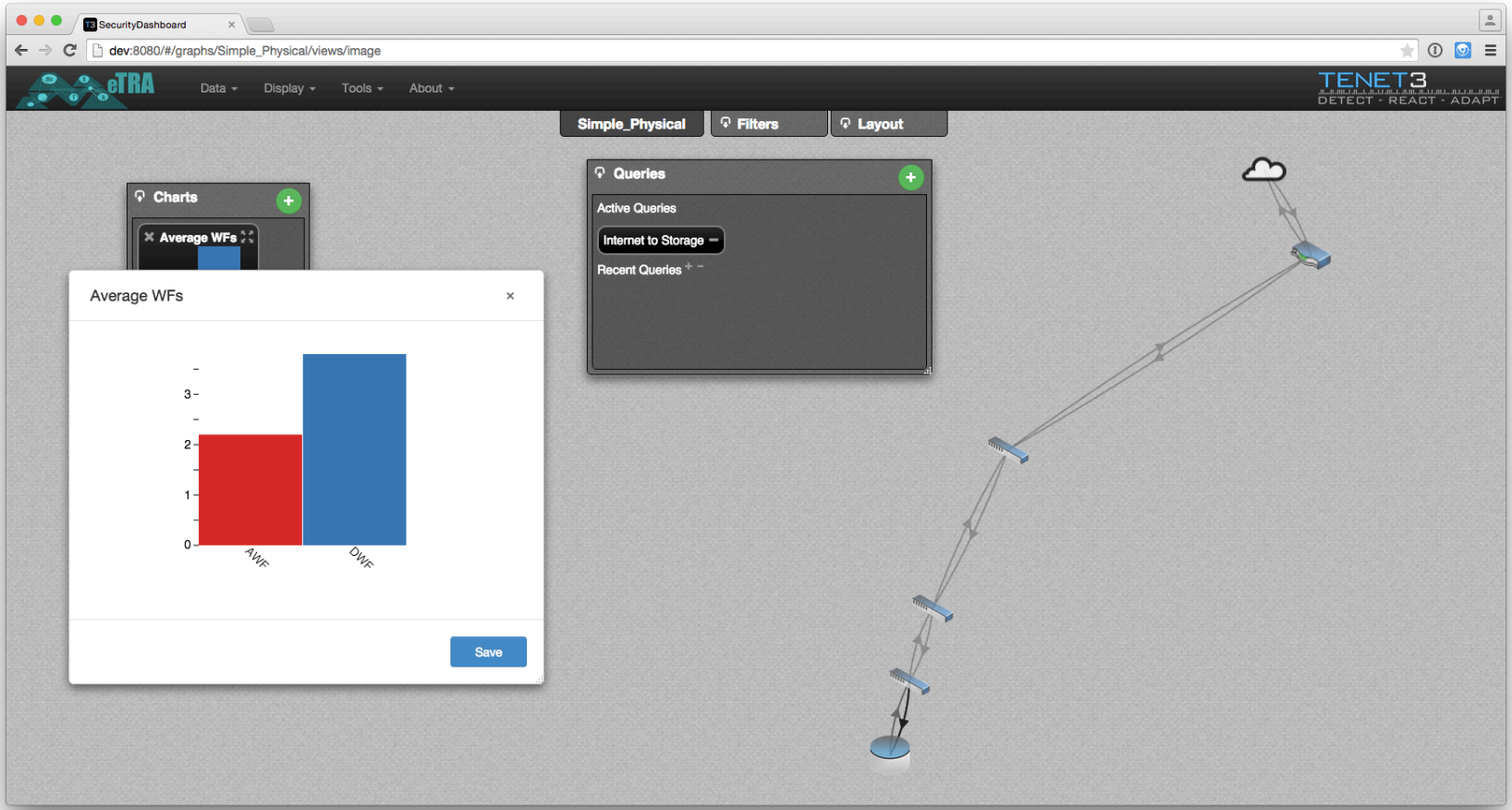
Patching

Obfuscation, Encryption, whitelisting, and execution control

Network segmentation,

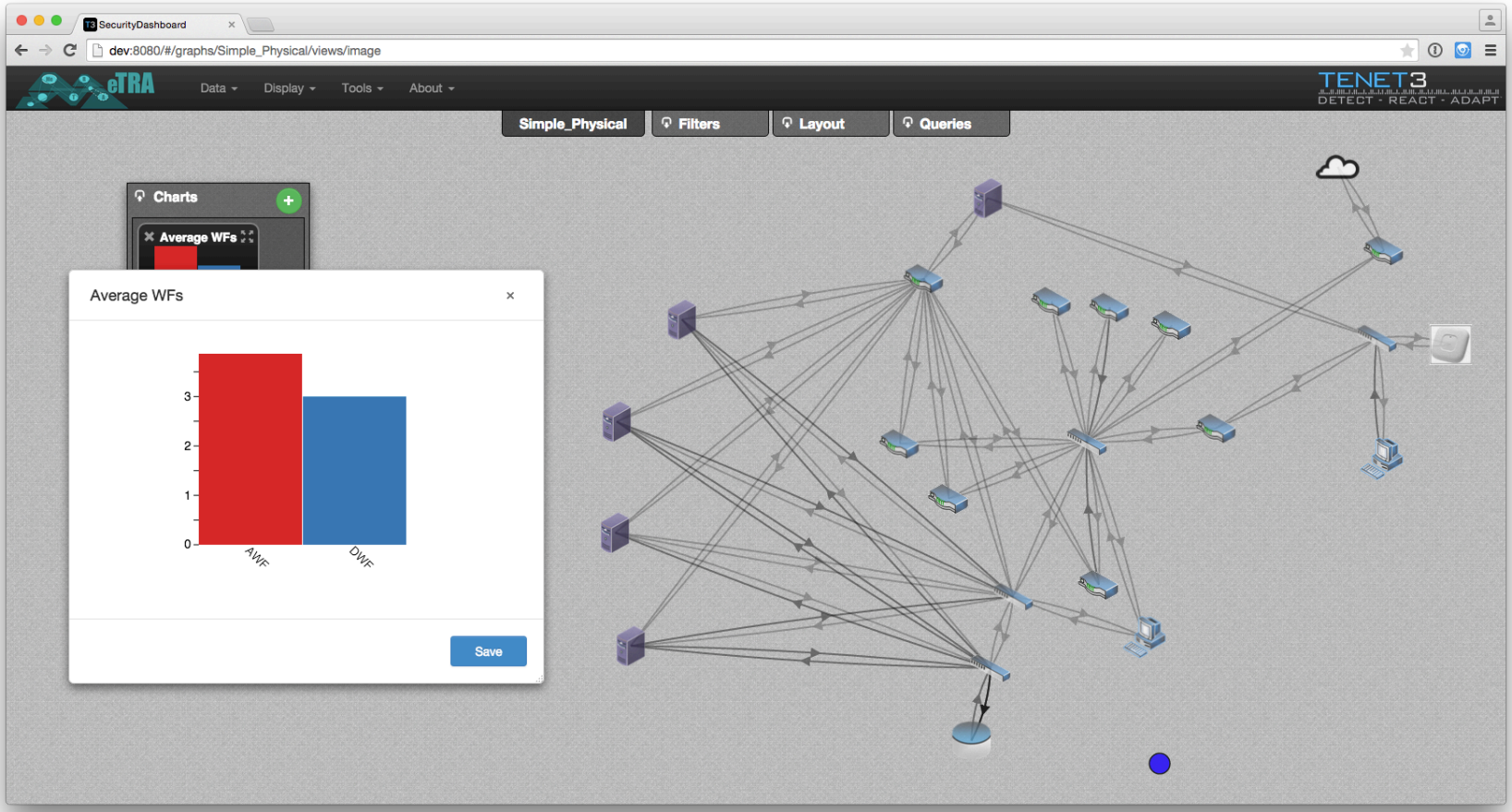
Network Security Monitoring (IDS)

Compute Metrics Along an Attack Path



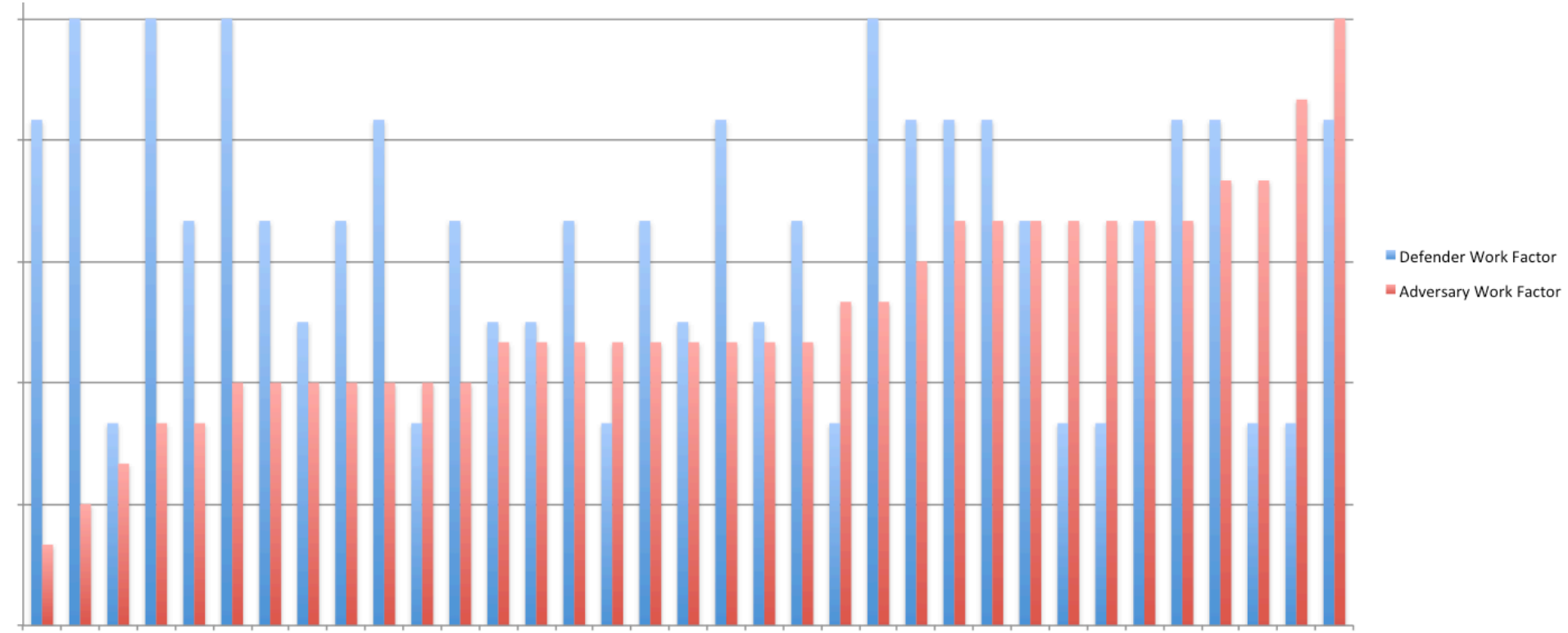
Here we track average adversary vs defender work factor along a specific attack path. This analysis highlights a case where the defender is spending more than the attacker. The defender return on investment is poor.

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



Relative Costs Assessed for a Set of Cyber Security Controls

Getting Started on Your Solution

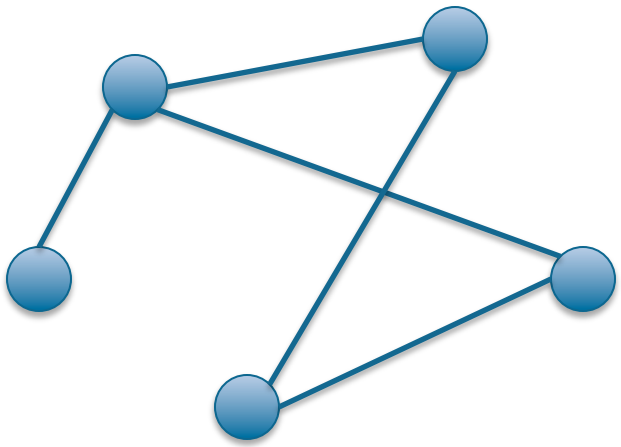
HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

Strategy Begins with Taking Stock

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

Strategy Begins with Taking Stock

- Inventory your stuff — Count
- Organize it — Collect
- Show how it's connected — 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.

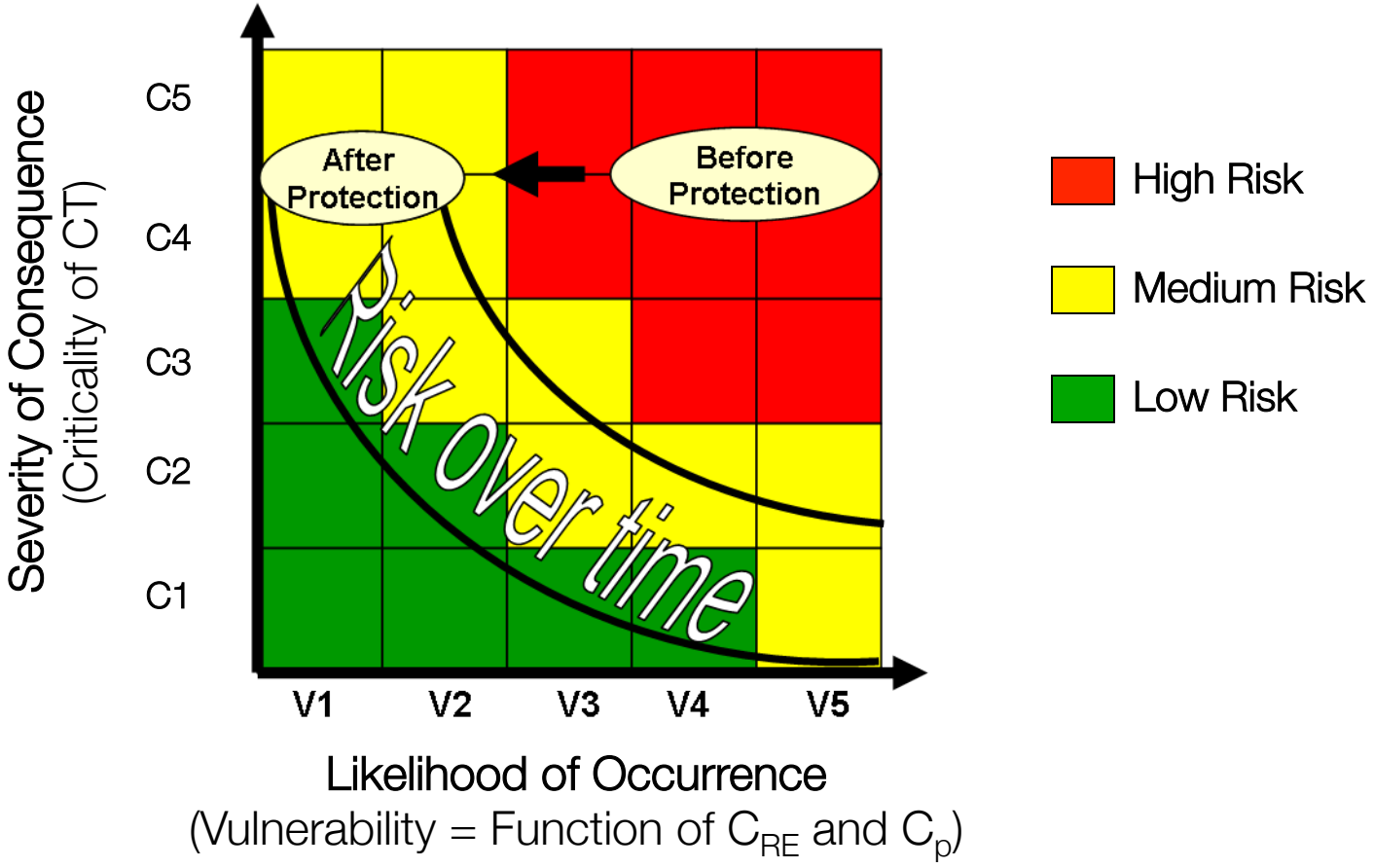
Extend Work Factor Assessment to the Enterprise

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

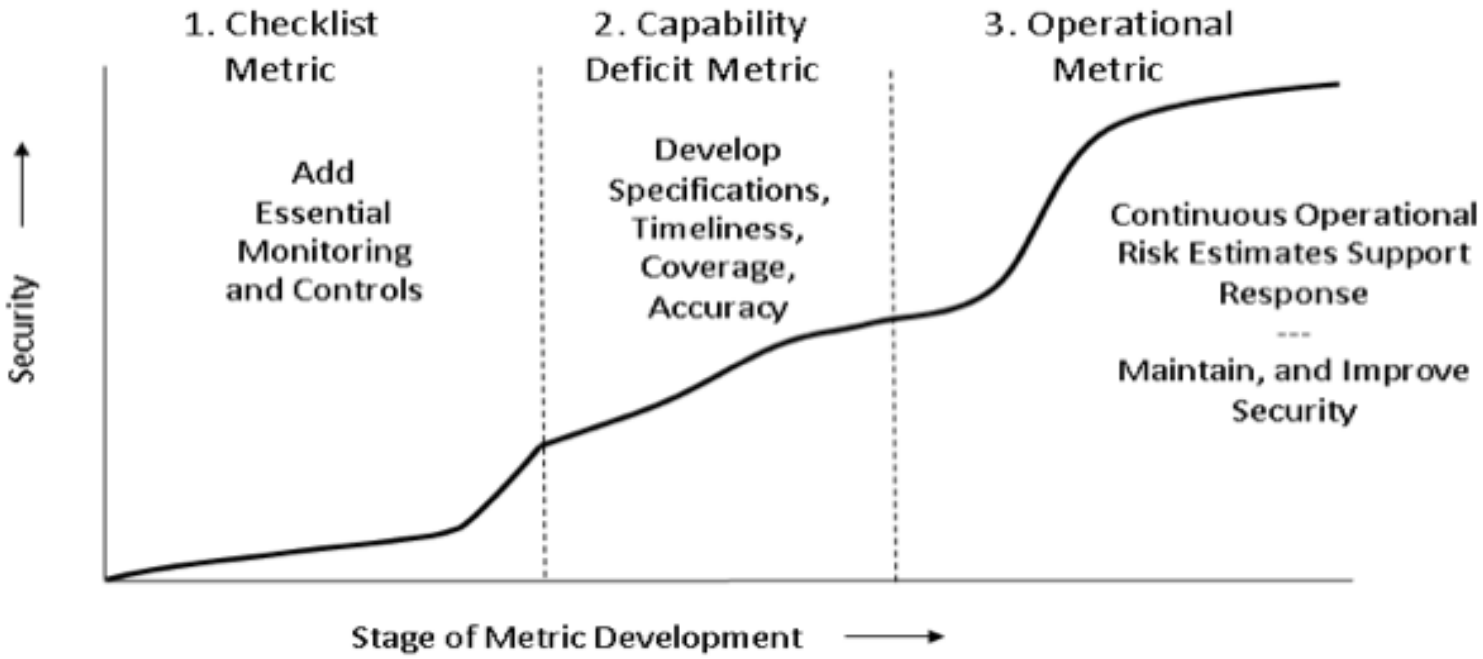
Is a Monoculture Secure?

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