How to Quantify Cyber-Resilience?

A Managerial Framework

Ranjan Pal

Cybersecurity at MIT Sloan

Talk Outline

Cybersecurity at MIT Sloan

I. Conceptual Definition and Metrification

II. Fitting Cyber-Resilience Metrics to Dimensions

III. A Systematic Cyber-Resilience Quantification Framework

Cybersecurity at MIT Sloan

I. Conceptual Definition and Metrification

How Can We Define the Cyber-Resilience Concept?

Cybersecurity at MIT Sloan

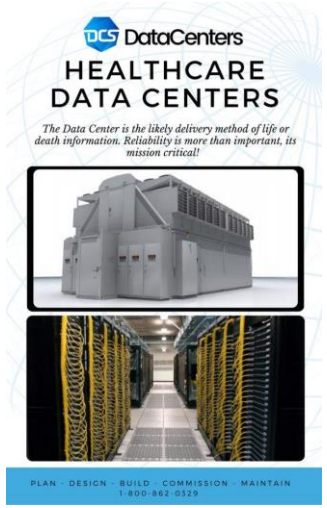
MITRE | National Academy of Sciences | NIST National Institute of Standards and Technology | informs Institute for Operations Research and the Management Sciences | pwc | EY Parthenon | BAIN & COMPANY | McKinsey & Company | Deloitte. | BCG | IBM

The ability for an enterprise to anticipate, absorb, adapt, and recover under cyber-threat environments

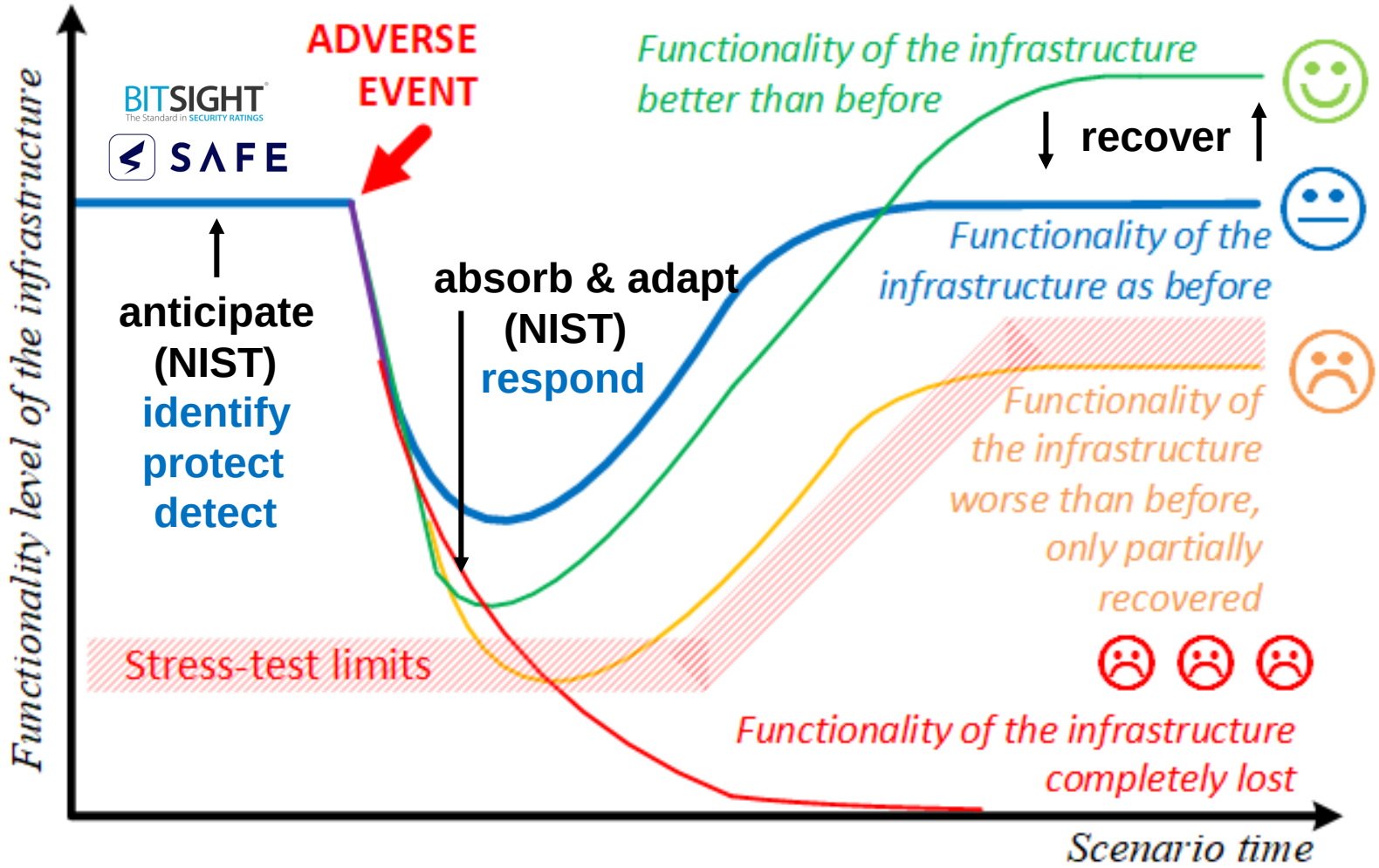
Conceptual Definition ≠ Metric Definition

How many of you adhere to this definition in your organization?

Let's Illustrate the Concept Through a Figurative Example



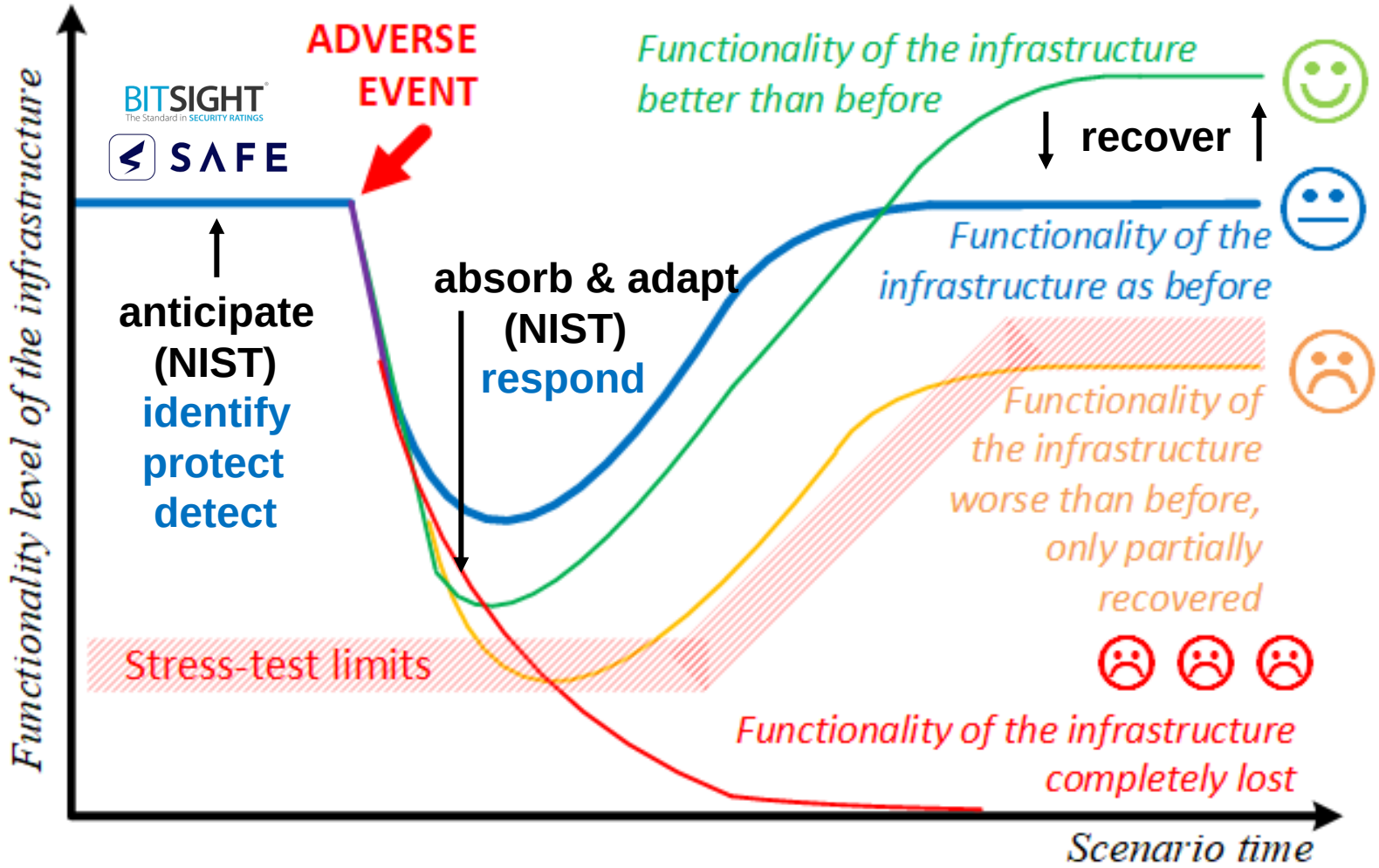
e.g., # 'Up'-Servers



What is an enterprise's ability to anticipate, absorb, adapt, and recover to given 'y'-axis demands?

Let's Illustrate the Concept Through Another Figurative Example

e.g., Battery Power



What is an enterprise's ability to anticipate, absorb, adapt, and recover to given 'y'-axis demands?

An Example Purpose of a Cyber-Resilience Metric

Cybersecurity at MIT Sloan

A cyber-resilience (CR) metric will drive enterprise/organization goals

Examples of Enterprise Management Goals

Achieve and sustain acceptable levels of (critical) mission function performance

e.g., the number of UP-servers should always be greater than K

Achieve acceptable levels of cyber-security

e.g., the number of financial impact causing cyber-incidents within time [T1, T2] should be less than A

'Minimize' adverse financial impact upon a cyber-attack

e.g., the monetary value of multi-party loss incurred due to business disruption should be less than $X

'Constrain' time to system recovery upon a cyber-attack

e.g., the time duration a (sub-)system is 'down' due to a cyber-incident should be less than T

How many of you have a cyber-resilience metric in your organization?

Our Goal

Cybersecurity at MIT Sloan

Many enterprises have cyber-resilience metrics mapping to multiple dimensions.
These dimensions fit the quantification framework we have developed in our research.

Cybersecurity at MIT Sloan

II. Mapping Cyber-Resilience Metrics to Dimensions

Dimensions that Cyber-Resilience Metrics Map To

Identified five dimensions to view a cyber-resilience metric

I. Management rank

(e.g., board/C-suite, technical lead)

II. Enterprise system complexity

(e.g., one component (server), network of components)

III. Network communication type

(e.g., physical, process, social)

IV. Enterprise type

(e.g., critical infrastructure, commercial business)

V. Manager risk tolerance

(e.g., low tolerance, high tolerance)

Listed dimensions based on a survey of approximately 50 research articles in engineering/social science/business, and 20 public website articles

Example Metrics in the 'Management Rank' Dimension

Source: *Library of Cyber-Resilience Metrics* (Lagarde et.al.)

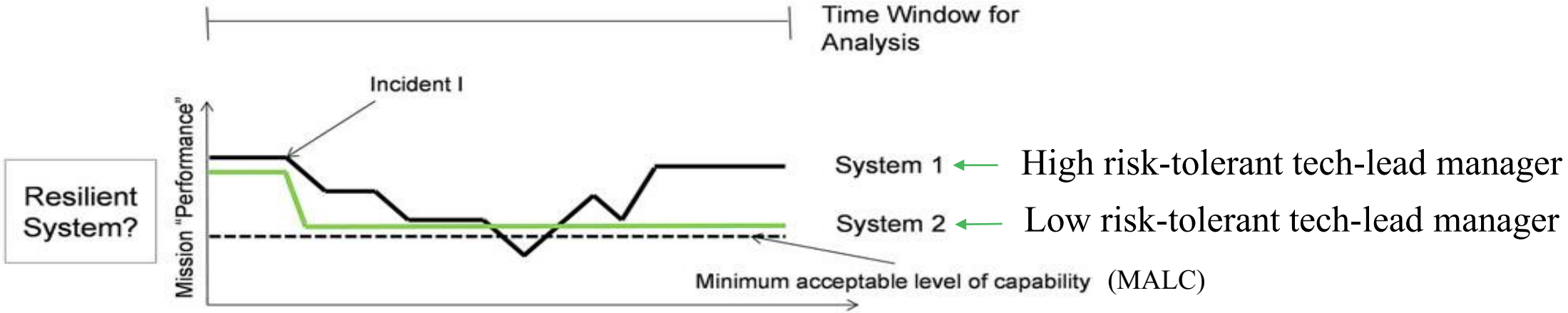
The **ability** to handle cyber-incidents

(anticipate, adapt/absorb, recover)

- malware
- social engineering
- DDoS

Performance Measure (Tech Lead): #up-servers, #non-compromised sensors

Performance Measure (C-suite): financial impact upon a cyber-incident



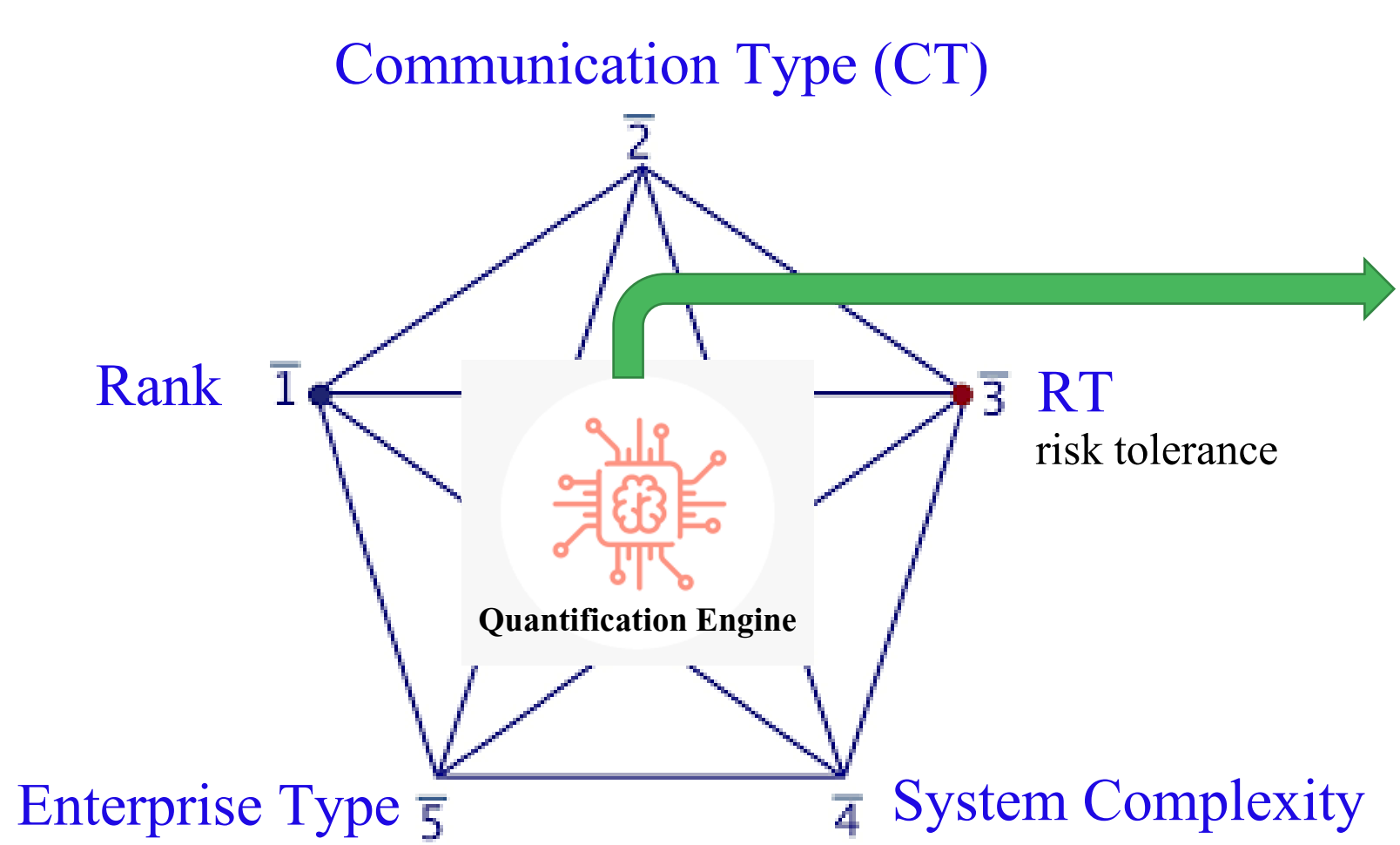
High risk-tolerant manager - will quantify ability to **maximize** mean performance per time interval

Low risk-tolerant manager - will quantify ability to **minimize** #times performance falls below MALC

Cybersecurity at MIT Sloan

III. Our Cyber-Resilience Quantification Framework

The SIMPLEX Cyber-Resilience (CR) Quantification Framework



The FIVE dimensions in a **simplex**

A ‘toolbox’ of situational CR metrics

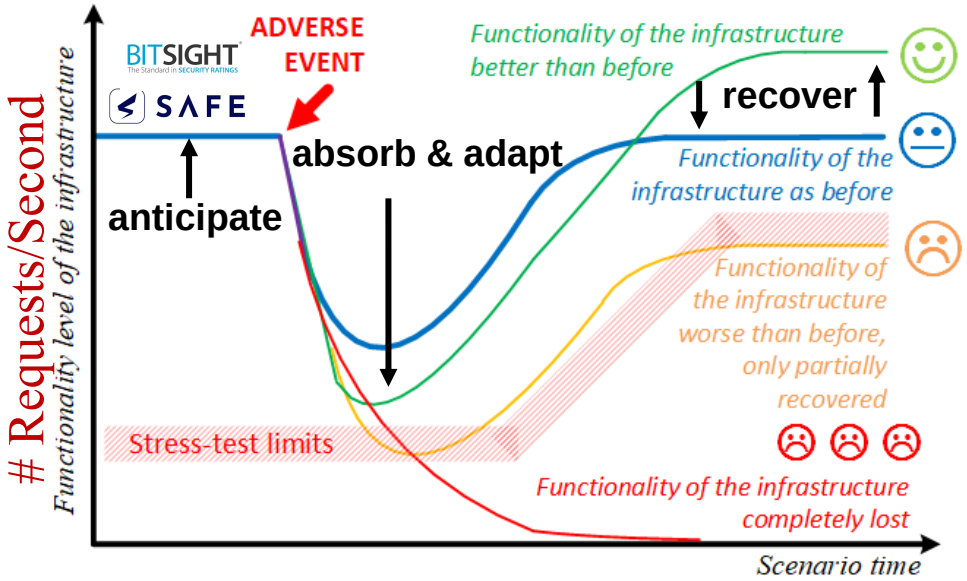
We adopt the term ‘simplex’ as a mashup between the ‘simplicity’ of our quantification framework and the simplex mathematical object

Let Us Work Through One Dimension Mapping Example

We need to quantify the metric: the **ability** to handle DDoS attacks

Dimension Configuration #1

Dimension	Value
Management Rank	*Technical Lead*
System Complexity	*One Server*
Communication Type	*Process*
Enterprise Type	*Commercial*
Risk Tolerance	*H(green), L(blue)*



Performance Metric
Requests/Second

X-axis values (time)

Desired Y-axis values

Desired time till attack

Anticipation Ability
NIST – I,P,D

X

Adapt & Absorb Ability
NIST - Respond

X

Recovering Ability
NIST - Recover

CR Score

Dragos's CR Equation is an Instance of SIMPLEX Quantification

Cyber-Resilience = Consequence x (Threat x Vulnerability) x (Cyber-Risk)$^{-1}$

$\propto$ ability to absorb $\rightarrow \frac{P_d}{P_0}$ $\cdot$ R $\propto$ ability to plan & prevent

$RF(\vec{T} = [t_d, t'_d, t_\delta, t_r]) \cdot \frac{P_r^*}{P_0}$ $\propto$ ability to recover $\propto$ ability to adapt

$$CR = R \cdot RF(\hat{T} = [t_d, t'_d, t_\delta, t_r]) \cdot \frac{P_r^*}{P_0} \frac{P_d}{P_0}$$

Key Takeaways from the Discussion

Cybersecurity at MIT Sloan

Many enterprises have cyber-resilience metrics

These metrics map to multiple dimensions

Enterprises often do not account for these dimensions to quantify cyber-resilience metrics

We developed a quantification framework where the dimensions fit a quantified metric

ranjanp@mit.edu