Cyber Resiliency: A Systems Engineering Perspective

Deb Bodeau

November 9, 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 22 02047 11

Pervasive Dependence on Cyber → Pervasive Risk

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 22 02047 11

Cyber Resiliency – Why, What, How

Why?

Adversaries
WILL get in and may not be detected in time
Critical components WILL be flawed or unable to handle changing uses

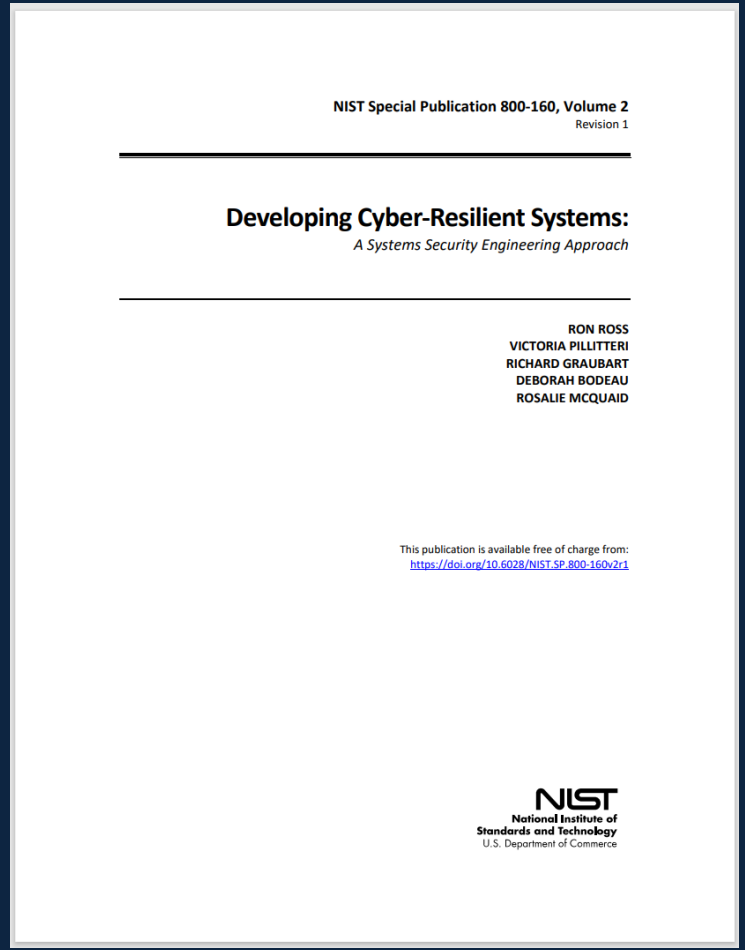
Critical functions
and operations fail
when attacked or challenged

Informal Definition

The ability to deliver a service or perform a function, possibly at a **reduced but effective level**, in spite of ongoing cyber attacks

Formal Definition

The ability to **anticipate, withstand**, **recover** from, and **adapt** to adverse conditions, stresses, attacks, or compromises on cyber resources


NIST Special Publication 800-160, Volume 2
Revision 1

Developing Cyber-Resilient Systems:
A Systems Security Engineering Approach

RON ROSS
VICTORIA PILLITTERI
RICHARD GRAUBART
DEBORAH BODEAU
ROSALIE MCQUAID

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v2r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 22 02047 11

How Does Cyber Resiliency Relate to Cybersecurity?

Intersect

- Adversarial threats
- Underlying functionality

Enhance

- Make critical security functions cyber-resilient

Differ

- Threat assumptions
- Role of detection

Cybersecurity focuses on information and authorized use
Cyber resiliency focuses on assuring critical functions and properties

Cyber Resiliency Goals
Anticipate
Withstand
Recover
Adapt

MITRE

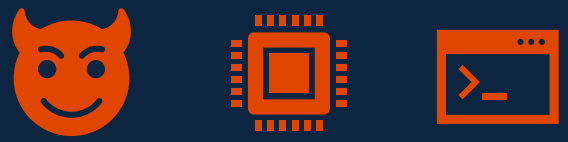
© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 22 02047 11

Assuring Adequate Cyber Resiliency

Determine what matters

Cyber Resiliency Goals	Cyber Resiliency Objectives	
Anticipate	Prepare	Understand
	Prevent / Avoid	
Withstand	Continue	
	Constrain	
Recover	Reconstitute	
	Transform	
Adapt	Re-Architect	

Think about risks due to cyber dependence



Leverage operational practices as well as technology

Cyber Resiliency Techniques	
Adaptive Response	Unpredictability
Analytic Monitoring	
Deception	
Diversity	
Dynamic Positioning	
Non-Persistence	
Privilege Restriction	
Segmentation	
Coordinated Protection	
Dynamic Representation	
Realignment	
Redundancy	
Substantiated Integrity	

Interpret and apply to any environment that involves critical functions and includes cyber elements

...

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 22 02047 11