Cyber Resiliency Overview

January 11, 2020

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Topics

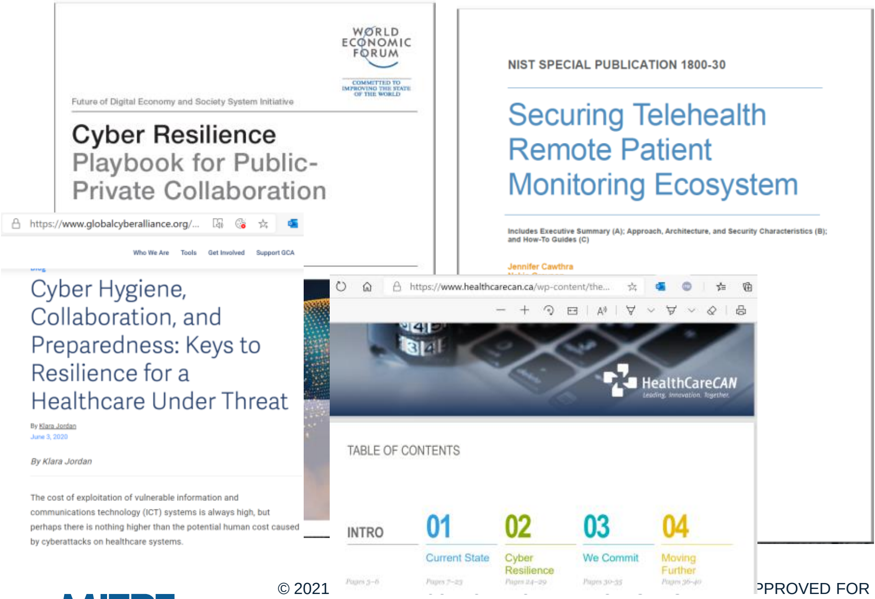
- Why talk about cyber resiliency?
- What is cyber resiliency?
- How does the concept of cyber resiliency translate into engineering decisions?
- How does cyber resiliency relate to cyber security?
- A notional example
- Resources

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Why Cyber Resiliency? Cyber Dependence and Cyber Threats

Increasing Recognition of the Need for Resilience in Cyberspace

Resilience against cyber attacks needed at multiple levels – ecosystem, organization, healthcare functions



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Future of Digital Economy and Society System Initiative

Cyber Resilience
Playbook for Public-Private Collaboration

NIST SPECIAL PUBLICATION 1800-30

Securing Telehealth Remote Patient Monitoring Ecosystem

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra

https://www.globalcyberalliance.org/...

Cyber Hygiene, Collaboration, and Preparedness: Keys to Resilience for a Healthcare Under Threat

By Klara Jordan
June 3, 2020

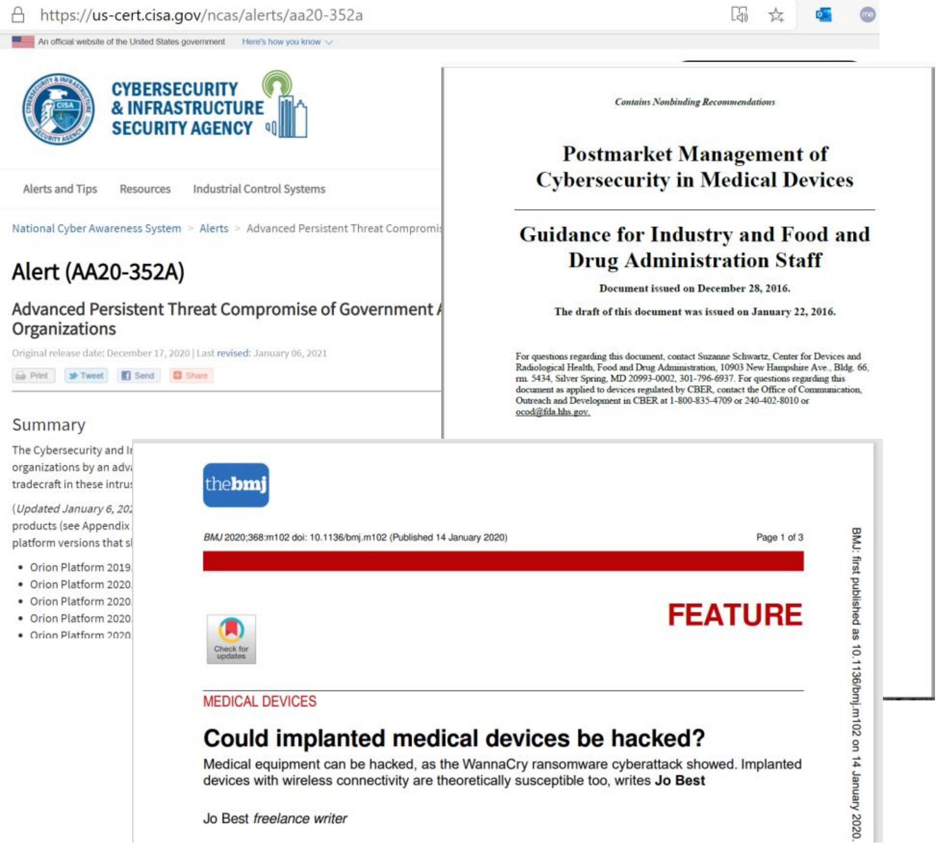
By Klara Jordan

The cost of exploitation of vulnerable information and communications technology (ICT) systems is always high, but perhaps there is nothing higher than the potential human cost caused by cyberattacks on healthcare systems.

https://www.healthcarecan.ca/wp-content/the...

HealthCareCAN
Leading. Innovation. Together.

TABLE OF CONTENTS



https://us-cert.cisa.gov/ncas/alerts/aa20-352a

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

National Cyber Awareness System > Alerts > Advanced Persistent Threat Compromis

Alert (AA20-352A)

Advanced Persistent Threat Compromise of Government A
Organizations

Original release date: December 17, 2020 | Last revised: January 06, 2021

Summary

The Cybersecurity and I
organizations by an adv
tradecraft in these intru

(*Updated January 6, 20*
products (see Appendix
platform versions that s

- Orion Platform 2019
- Orion Platform 2020
- Orion Platform 2020
- Orion Platform 2020
- Orion Platform 2020

Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

thebmj

BMJ 2020;368:m102 doi: 10.1136/bmj.m102 (Published 14 January 2020) Page 1 of 3

BMJ: first published as 10.1136/bmj.m102 on 14 January 2020.

FEATURE

Check for updates

MEDICAL DEVICES

Could implanted medical devices be hacked?

Medical equipment can be hacked, as the WannaCry ransomware cyberattack showed. Implanted devices with wireless connectivity are theoretically susceptible too, writes **Jo Best**

Jo Best *freelance writer*

Recognition that systems must be expected to include compromised or readily hacked components

© 2021

Cyber Resiliency – “Why” Drives What, How, When, and Where

WHY

The bad guys **WILL** get in and may not be detected in time

Critical functions and operations fail when attacked

WHAT

Keep service delivery going

Resilience of **critical cyber resources, functions, business processes** or organization in the face of cyber threats

HOW

Transformation of thought

Architect

Augment traditional approaches

Adopt mission-oriented threat-based system engineering processes

Define policies & practices

Design, build, integrate – engineer for cyber resiliency

WHEN & WHERE

Apply resiliency throughout the system lifecycle

(requirements, acquisition, training, operations)

and across the enterprise

(architecture, policy, operational procedures)

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

What Is Cyber Resiliency?
As Defined in NIST SP 800-160 Vol. 2

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

Cyber resiliency is not *just a new name for cyber security*
Nor is it a new name for COOP, conventional system resilience, or organizational resilience
The underlying assumption is that compromises will happen – and may go undetected for extended periods – but that if the right technologies, processes, and controls are in place, needs can still be met
Cyber resiliency builds on and integrates existing disciplines … and includes additional capabilities

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Cyber Resiliency Engineering Builds on Related Disciplines

Disciplines	Key Concepts	Cyber Resiliency Engineering Insights
Security, Information Assurance	Provide confidentiality, integrity, availability, accountability for information and services, despite threats (adversarial, accidental, structural, environmental)	Focus on mission assurance and risks to missions Advanced adversaries can emulate non-adversarial threats
Cybersecurity	Provide security despite adversarial threats via cyberspace	Advanced adversaries can establish and maintain a covert presence – boundary defenses and intrusion detection do not suffice
Resilience Engineering, COOP, Survivability	Provide system or operational resilience in the face of accidents and disruptions	Adversary can interfere with – or take advantage of – recovery efforts

Cyber resiliency is one quality property among many that systems engineers must consider. Quality properties typically overlap and interact.

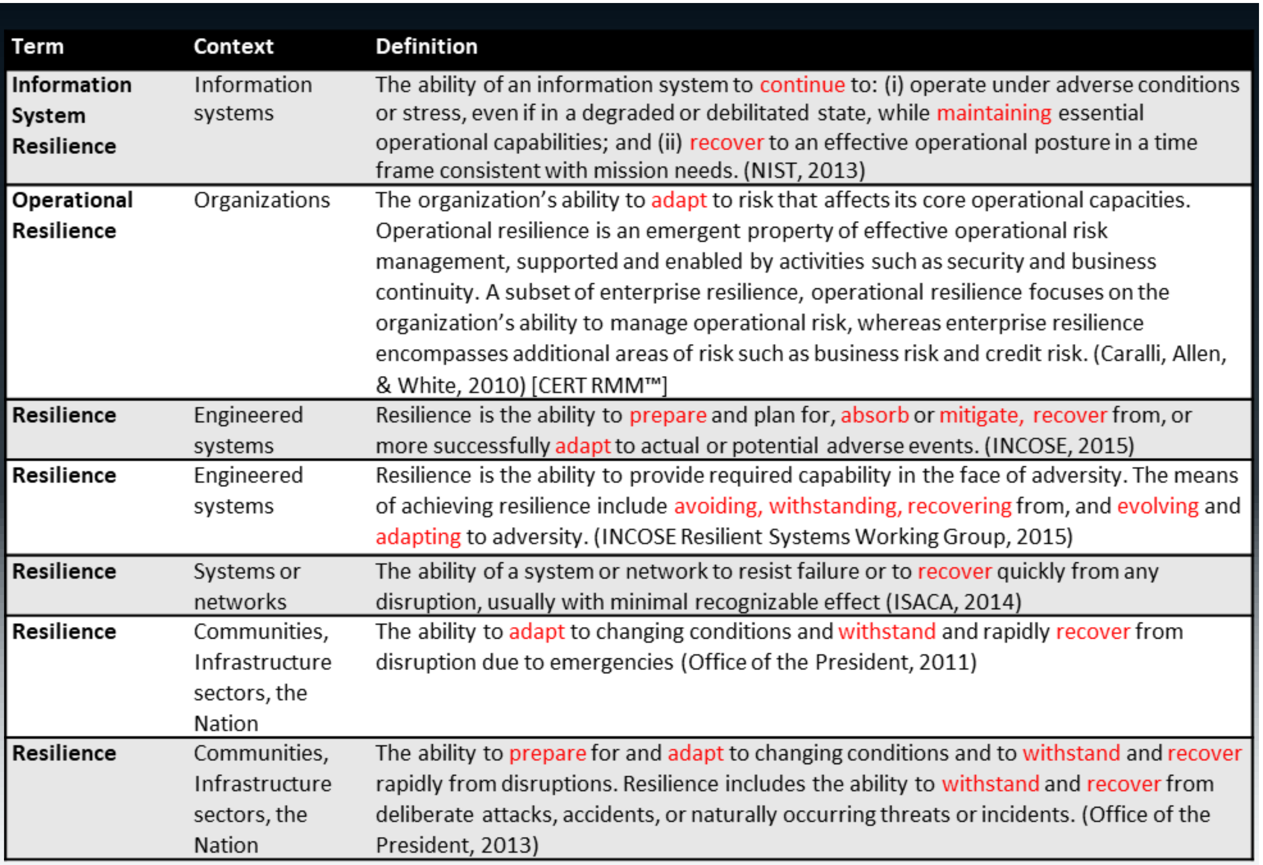
The systems engineering challenge is to understand and make trade-offs among the different properties, and the different ways to achieve those properties, in a cost-effective, risk-managed way.

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

How Does the Concept of Cyber Resiliency Translate into Engineering Decisions? Understand Overarching Goals

What

Cyber Resiliency Goals	
Anticipate	*"Be prepared"*
Withstand	*"Fight through"*
Recover	*"Bounce back"*
Adapt	*"Adapt to a changing world"*

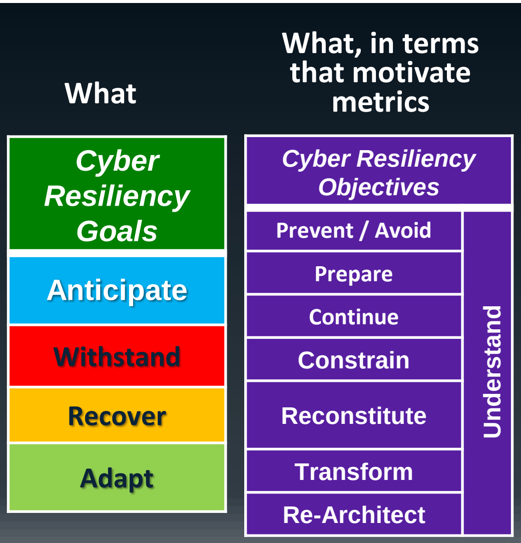


Term	Context	Definition
Information System Resilience	Information systems	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. (NIST, 2013)
Operational Resilience	Organizations	The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk. (Caralli, Allen, & White, 2010) [CERT RMM™]
Resilience	Engineered systems	Resilience is the ability to prepare and plan for, absorb or mitigate, recover from, or more successfully adapt to actual or potential adverse events. (INCOSE, 2015)
Resilience	Engineered systems	Resilience is the ability to provide required capability in the face of adversity. The means of achieving resilience include avoiding, withstanding, recovering from, and evolving and adapting to adversity. (INCOSE Resilient Systems Working Group, 2015)
Resilience	Systems or networks	The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect (ISACA, 2014)
Resilience	Communities, Infrastructure sectors, the Nation	The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies (Office of the President, 2011)
Resilience	Communities, Infrastructure sectors, the Nation	The ability to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Office of the President, 2013)

Cyber resiliency goals are based on a wide range of resilience-related definitions … this table is a sample, highlighting terms for goals

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

How Does the Concept of Cyber Resiliency Translate into Engineering Decisions? Define Objectives as a Basis for Assessment



What

What, in terms that motivate metrics

Cyber Resiliency Goals

Anticipate

Withstand

Recover

Adapt

Cyber Resiliency Objectives

Prevent / Avoid

Prepare

Continue

Constrain

Reconstitute

Transform

Re-Architect

Understand

How quickly, how long, how completely, how effectively, with how much confidence …

Prevent or Avoid: Preclude successful execution of an attack or the realization of adverse conditions

Prepare: Maintain a set of realistic cyber courses of action that address predicted or anticipated adversity

Continue: Maximize the duration and viability of essential mission or business functions during adversity

Constrain: Limit damage from adversity

Reconstitute: Restore as much mission or business functionality as possible subsequent to adversity

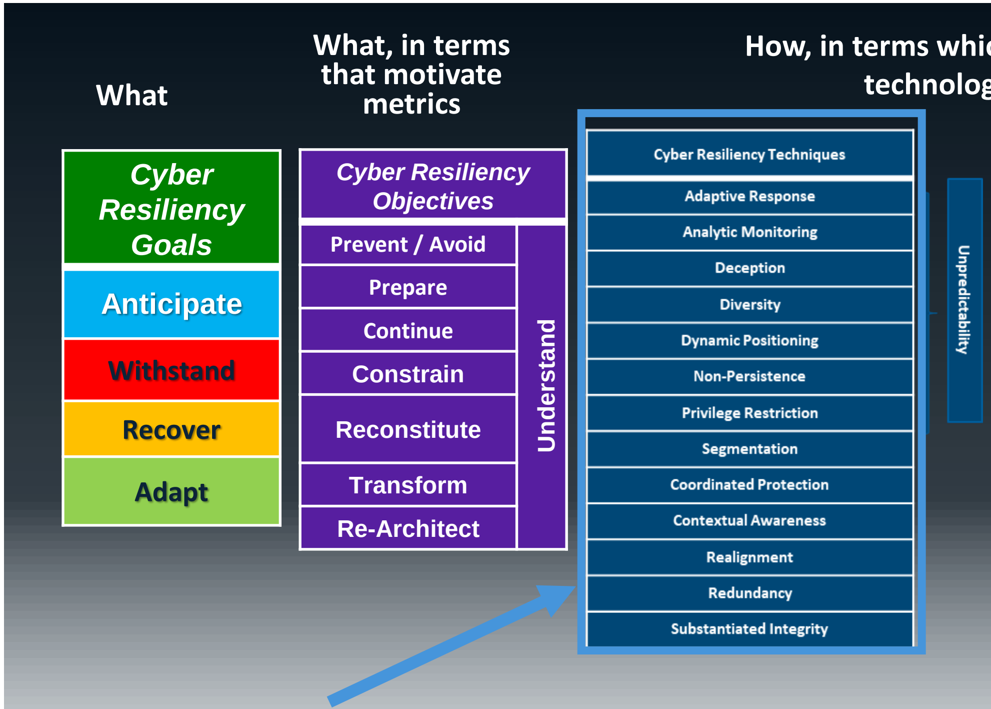
Understand: Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity

Transform: Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively

Re-Architect: Modify architectures to handle adversity and address environmental changes more effectively

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

How Does the Concept of Cyber Resiliency Translate into Engineering Decisions? Identify Technologies and Practices



What

What, in terms that motivate metrics

How, in terms which characterize solutions – technologies and practices

Cyber Resiliency Goals

- Anticipate
- Withstand
- Recover
- Adapt

Cyber Resiliency Objectives

- Prevent / Avoid
- Prepare
- Continue
- Constrain
- Reconstitute
- Transform
- Re-Architect

Understand

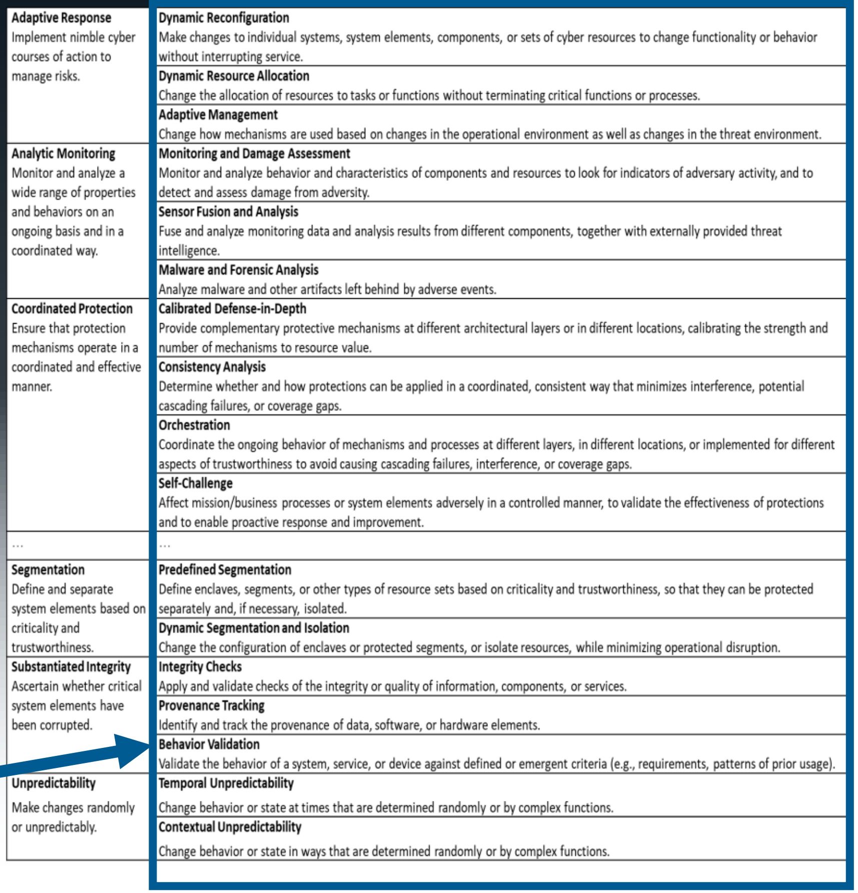
Cyber Resiliency Techniques

- Adaptive Response
- Analytic Monitoring
- Deception
- Diversity
- Dynamic Positioning
- Non-Persistence
- Privilege Restriction
- Segmentation
- Coordinated Protection
- Contextual Awareness
- Realignment
- Redundancy
- Substantiated Integrity

Unpredictability

Cyber resiliency techniques characterize technologies, practices, products, controls, or requirements, so that their contribution to cyber resiliency can be understood

A cyber resiliency implementation approach characterizes a subset of what a cyber resiliency technique includes, and is defined by how the capabilities are implemented.



Adaptive Response Implement nimble cyber courses of action to manage risks.	**Dynamic Reconfiguration** Make changes to individual systems, system elements, components, or sets of cyber resources to change functionality or behavior without interrupting service.
	Dynamic Resource Allocation Change the allocation of resources to tasks or functions without terminating critical functions or processes.
	Adaptive Management Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment.
Analytic Monitoring Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.	**Monitoring and Damage Assessment** Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, and to detect and assess damage from adversity.
	Sensor Fusion and Analysis Fuse and analyze monitoring data and analysis results from different components, together with externally provided threat intelligence.
	Malware and Forensic Analysis Analyze malware and other artifacts left behind by adverse events.
Coordinated Protection Ensure that protection mechanisms operate in a coordinated and effective manner.	**Calibrated Defense-in-Depth** Provide complementary protective mechanisms at different architectural layers or in different locations, calibrating the strength and number of mechanisms to resource value.
	Consistency Analysis Determine whether and how protections can be applied in a coordinated, consistent way that minimizes interference, potential cascading failures, or coverage gaps.
	Orchestration Coordinate the ongoing behavior of mechanisms and processes at different layers, in different locations, or implemented for different aspects of trustworthiness to avoid causing cascading failures, interference, or coverage gaps.
	Self-Challenge Affect mission/business processes or system elements adversely in a controlled manner, to validate the effectiveness of protections and to enable proactive response and improvement.
…	…
Segmentation Define and separate system elements based on criticality and trustworthiness.	**Predefined Segmentation** Define enclaves, segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated.
	Dynamic Segmentation and Isolation Change the configuration of enclaves or protected segments, or isolate resources, while minimizing operational disruption.
Substantiated Integrity Ascertain whether critical system elements have been corrupted.	**Integrity Checks** Apply and validate checks of the integrity or quality of information, components, or services.
	Provenance Tracking Identify and track the provenance of data, software, or hardware elements.
	Behavior Validation Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).
Unpredictability Make changes randomly or unpredictably.	**Temporal Unpredictability** Change behavior or state at times that are determined randomly or by complex functions.
	Contextual Unpredictability Change behavior or state in ways that are determined randomly or by complex functions.

Excerpts from NIST SP 800-160 V2

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

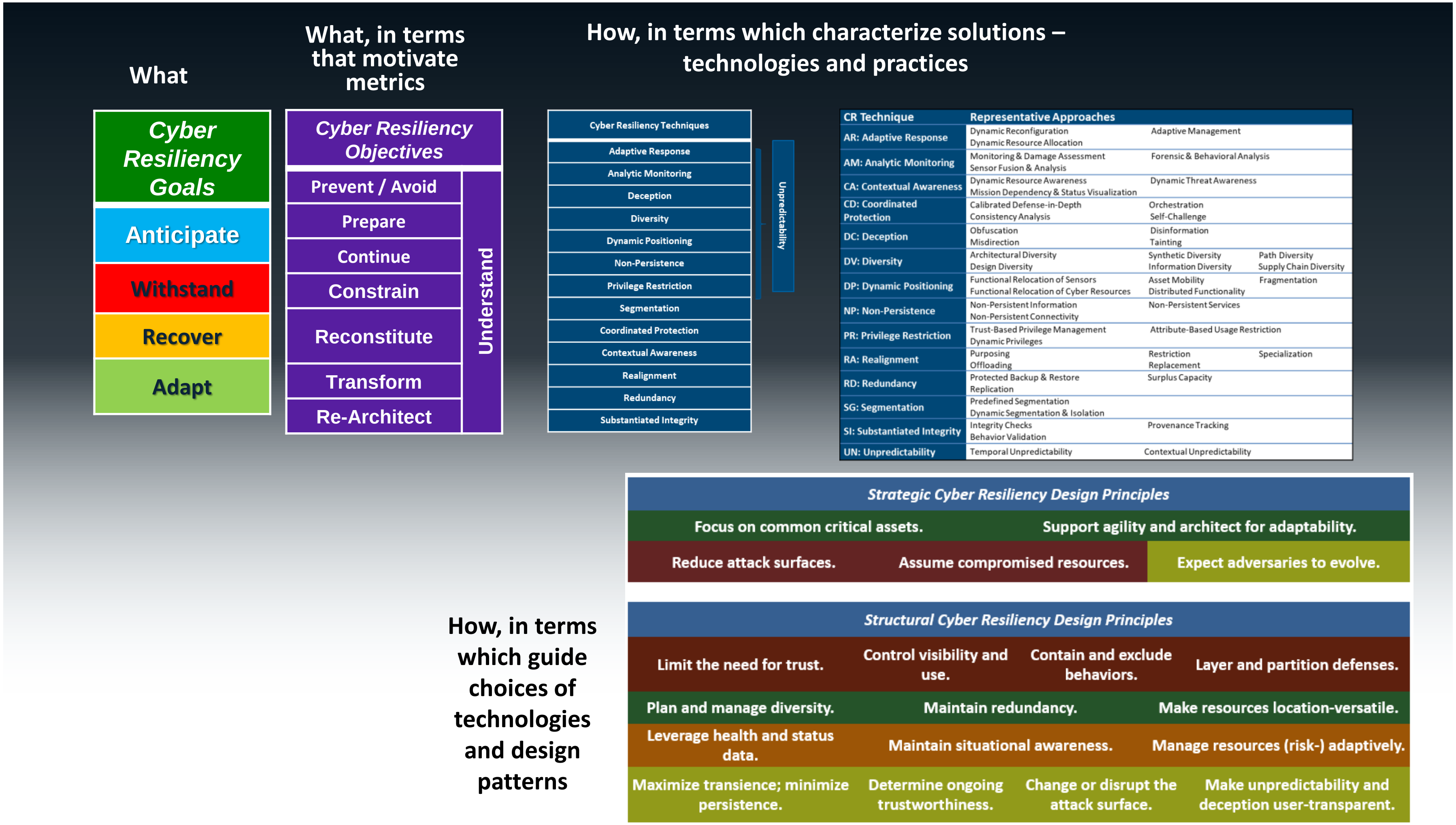
Identify Technologies and Practices Using Capability Categories and Approaches to Implementing Capabilities

Cyber Resiliency Technique	Representative Implementation Approaches		
Adaptive Response	Dynamic Reconfiguration Dynamic Resource Allocation	Adaptive Management	
Analytic Monitoring	Monitoring & Damage Assessment Sensor Fusion & Analysis	Forensic & Behavioral Analysis	
Contextual Awareness	Dynamic Resource Awareness Mission Dependency & Status Visualization	Dynamic Threat Awareness	
Coordinated Protection	Calibrated Defense-in-Depth Consistency Analysis	Orchestration Self-Challenge	
Deception	Obfuscation Misdirection	Disinformation Tainting	
Diversity	Architectural Diversity Design Diversity	Synthetic Diversity Information Diversity	Path Diversity Supply Chain Diversity
Dynamic Positioning	Functional Relocation of Sensors Functional Relocation of Cyber Resources	Asset Mobility Distributed Functionality	Fragmentation
Non-Persistence	Non-Persistent Information Non-Persistent Connectivity	Non-Persistent Services	
Privilege Restriction	Trust-Based Privilege Management Dynamic Privileges	Attribute-Based Usage Restriction	
Realignment	Purposing Offloading	Restriction Replacement	Specialization
Redundancy	Protected Backup & Restore Replication	Surplus Capacity	
Segmentation	Predefined Segmentation Dynamic Segmentation & Isolation		
Substantiated Integrity	Integrity Checks Behavior Validation	Provenance Tracking	
Unpredictability	Temporal Unpredictability	Contextual Unpredictability	

For more information, see NIST SP 800-160 Vol. 2

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

How Does the Concept of Cyber Resiliency Translate into Engineering Decisions? Articulate Guiding Principles



What

Cyber Resiliency Goals

- Anticipate
- Withstand
- Recover
- Adapt

What, in terms that motivate metrics

Cyber Resiliency Objectives

- Prevent / Avoid
- Prepare
- Continue
- Constrain
- Reconstitute
- Transform
- Re-Architect

How, in terms which characterize solutions – technologies and practices

Cyber Resiliency Techniques

- Adaptive Response
- Analytic Monitoring
- Deception
- Diversity
- Dynamic Positioning
- Non-Persistence
- Privilege Restriction
- Segmentation
- Coordinated Protection
- Contextual Awareness
- Realignment
- Redundancy
- Substantiated Integrity

CR Technique	Representative Approaches		
AR: Adaptive Response	Dynamic Reconfiguration Dynamic Resource Allocation	Adaptive Management	
AM: Analytic Monitoring	Monitoring & Damage Assessment Sensor Fusion & Analysis	Forensic & Behavioral Analysis	
CA: Contextual Awareness	Dynamic Resource Awareness Mission Dependency & Status Visualization	Dynamic Threat Awareness	
CD: Coordinated Protection	Calibrated Defense-in-Depth Consistency Analysis	Orchestration Self-Challenge	
DC: Deception	Obfuscation Misdirection	Disinformation Tainting	
DV: Diversity	Architectural Diversity Design Diversity	Synthetic Diversity Information Diversity	Path Diversity Supply Chain Diversity
DP: Dynamic Positioning	Functional Relocation of Sensors Functional Relocation of Cyber Resources	Asset Mobility Distributed Functionality	Fragmentation
NP: Non-Persistence	Non-Persistent Information Non-Persistent Connectivity	Non-Persistent Services	
PR: Privilege Restriction	Trust-Based Privilege Management Dynamic Privileges	Attribute-Based Usage Restriction	
RA: Realignment	Purposing Offloading	Restriction Replacement	Specialization
RD: Redundancy	Protected Backup & Restore Replication	Surplus Capacity	
SG: Segmentation	Predefined Segmentation Dynamic Segmentation & Isolation		
SI: Substantiated Integrity	Integrity Checks Behavior Validation	Provenance Tracking	
UN: Unpredictability	Temporal Unpredictability	Contextual Unpredictability	

How, in terms which guide choices of technologies and design patterns

Strategic Cyber Resiliency Design Principles

Focus on common critical assets.	Support agility and architect for adaptability.	
Reduce attack surfaces.	Assume compromised resources.	Expect adversaries to evolve.

Structural Cyber Resiliency Design Principles

Limit the need for trust.	Control visibility and use.	Contain and exclude behaviors.	Layer and partition defenses.
Plan and manage diversity.	Maintain redundancy.	Make resources location-versatile.	
Leverage health and status data.	Maintain situational awareness.	Manage resources (risk-) adaptively.	
Maximize transience; minimize persistence.	Determine ongoing trustworthiness.	Change or disrupt the attack surface.	Make unpredictability and deception user-transparent.

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

How Does the Concept of Cyber Resiliency Translate into Engineering Decisions? Put the Pieces Together …

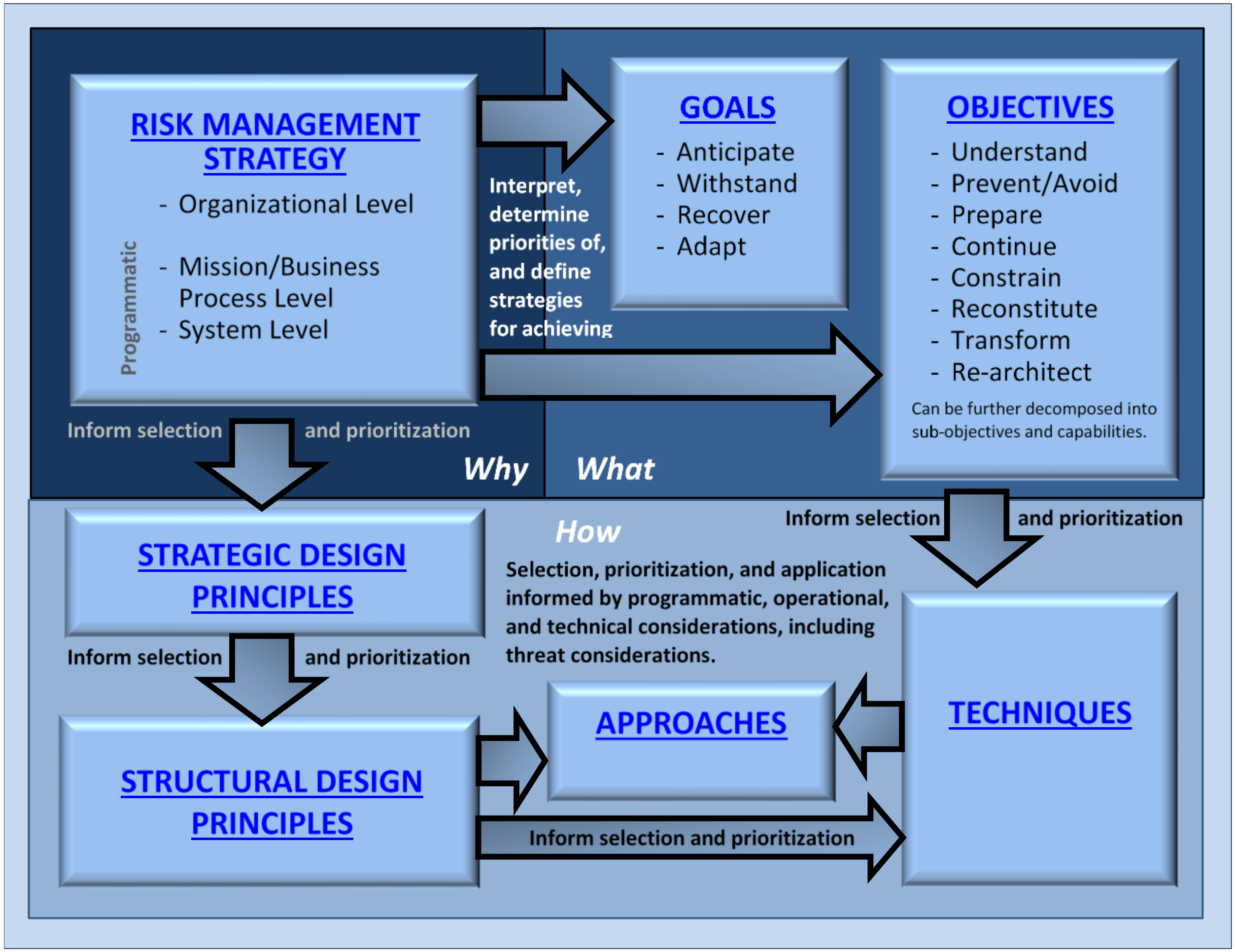
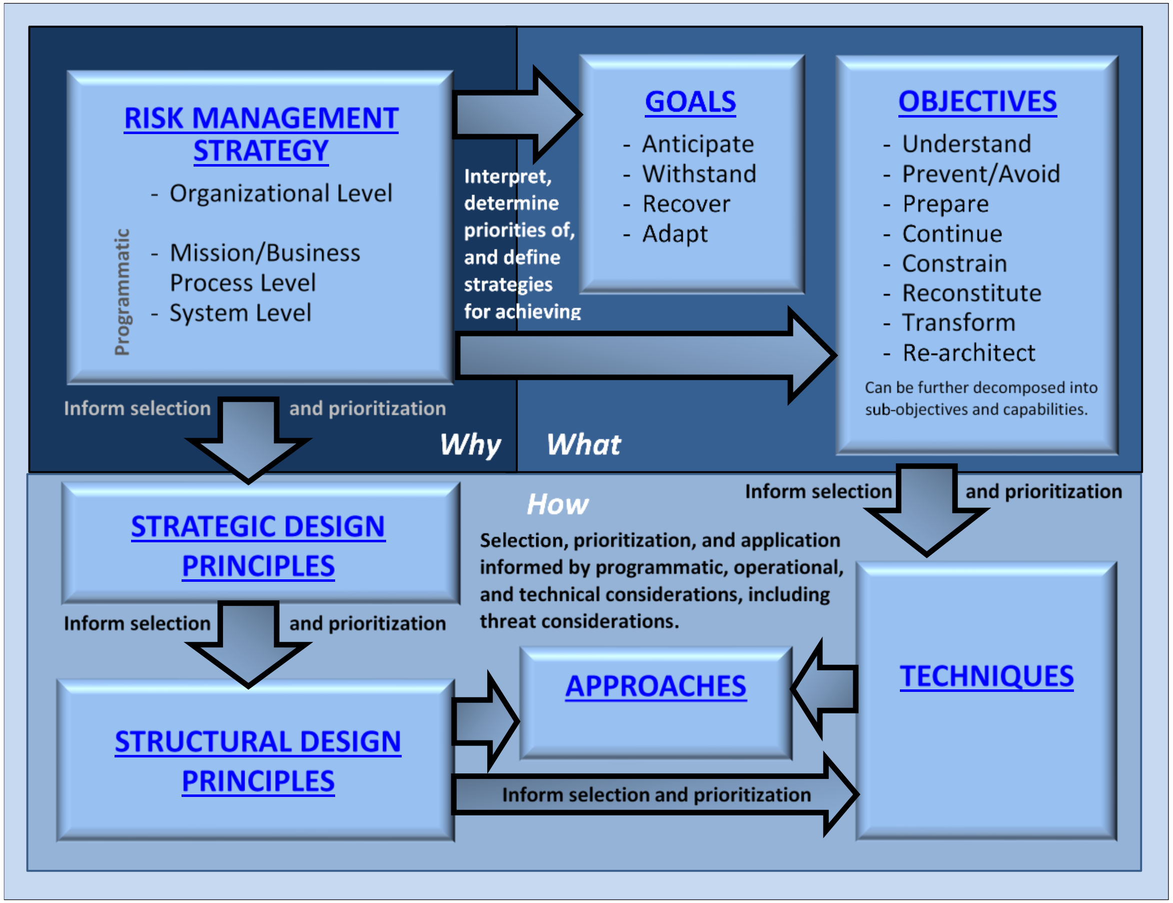

RISK MANAGEMENT STRATEGY
- Organizational Level
- Mission/Business Process Level
- System Level
Programmatic
Interpret, determine priorities of, and define strategies for achieving
GOALS
- Anticipate
- Withstand
- Recover
- Adapt
OBJECTIVES
- Understand
- Prevent/Avoid
- Prepare
- Continue
- Constrain
- Reconstitute
- Transform
- Re-architect
Can be further decomposed into sub-objectives and capabilities.
Inform selection
and prioritization
Why
What
How
Selection, prioritization, and application informed by programmatic, operational, and technical considerations, including threat considerations.
Inform selection
and prioritization
STRATEGIC DESIGN PRINCIPLES
Inform selection
and prioritization
STRUCTURAL DESIGN PRINCIPLES
APPROACHES
TECHNIQUES
Inform selection and prioritization

Figure from NIST SP 800-160 Volume 2 – Developing Cyber Resilient Systems: *A Systems Security Engineering Approach*

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

… Using Good Systems Engineering Judgment


RISK MANAGEMENT STRATEGY
- Organizational Level
- Mission/Business Process Level
- System Level
Programmatic
Interpret, determine priorities of, and define strategies for achieving
GOALS
- Anticipate
- Withstand
- Recover
- Adapt
OBJECTIVES
- Understand
- Prevent/Avoid
- Prepare
- Continue
- Constrain
- Reconstitute
- Transform
- Re-architect
Can be further decomposed into sub-objectives and capabilities.
Inform selection and prioritization
Why
What
How
Inform selection and prioritization
STRATEGIC DESIGN PRINCIPLES
Selection, prioritization, and application informed by programmatic, operational, and technical considerations, including threat considerations.
Inform selection and prioritization
STRUCTURAL DESIGN PRINCIPLES
APPROACHES
TECHNIQUES
Inform selection and prioritization

***Apply selectively* – based on stakeholder priorities, risk management strategy, operational considerations, legacy investments, etc.**

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

What Is the Relationship Between Cybersecurity and Cyber Resiliency?

Limitations with Conventional Cyber Security Practices

Traditional Cyber Security Practices	Limitations
Establish an effective security perimeter	No perimeter is 100% effective at keeping adversaries out
Use up-to-date A/V s/w to detect malware	A/V is ineffective against new zero-day attacks
Encrypt data while at rest and in transit	Encrypted traffic is a great place for adversary activity to hide
Monitor and audit all user activity	Audit logs are rarely checked due to lack of time and resources and moreover they are often focused on individual components and do not provide a big picture view of adversary activities
Develop and maintain backup plans, contingency plans, IA policies, accreditations, etc.	Redundant servers and data are designed to deal with natural disasters; they are ineffective against the APT who will apply the same attacks against backups

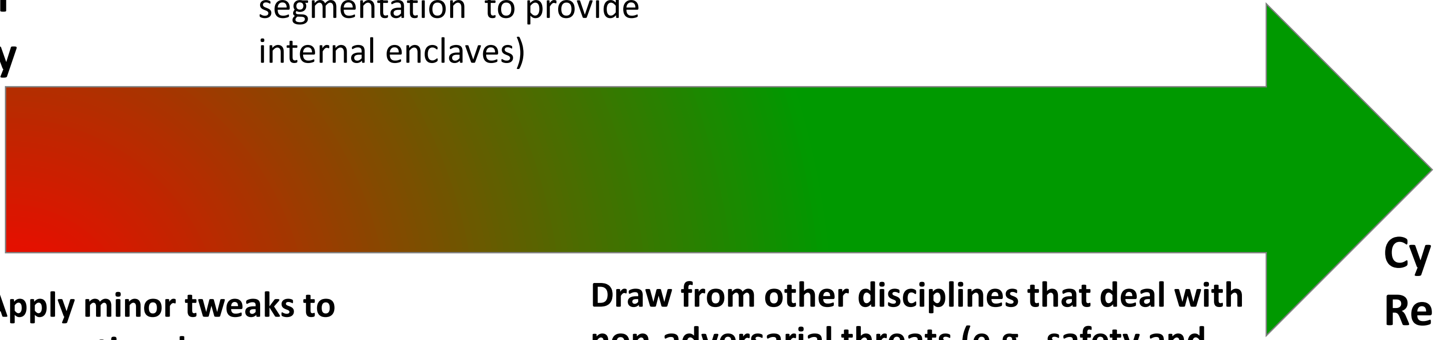
Threat assumptions, adversary presence, compromise focus differ for resiliency

	Conventional Cyber Security	Cyber Resiliency
Threat Assumptions with respect to Adversary	Capabilities: Limited Intent: Self aggrandizement, personal benefits Targeting: Targets of opportunity Timeline: Episodic Stealthy: No	Capabilities: Sophisticated, well resourced Intent: Establish & maintain ability to undermine mission Targeting: High value targets, very persistent Timeline: Long term campaigns Stealthy: Very
Adversary Presence	Assumes can be kept out or can quickly be detected and removed	Assumes adversary has established a foothold
Focus of Type of Compromises	Limited duration events, natural disasters	Ongoing attacks, long term adversary presence, organization must “fight thru”
Recovery	Adversary is not present to impede recovery	Recovery must be done despite presence of adversary
Goals	Protect, Detect, React	Anticipate, Withstand, Recover, Evolve

Cyber resiliency measures can complement or sometimes replace conventional cyber security measures

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

What Is the Relationship Between Cybersecurity and Cyber Resiliency? Transition Along a Continuum



Conventional Cybersecurity

Apply minor tweaks to conventional cybersecurity and resilience (e.g., COOP) (e.g., ensure backups are protected, rather than being a back door)

Implement conventional cybersecurity / resilience capabilities in a novel or enhanced ways (e.g., use AI to enhance intrusion detection, employ firewalls or micro-segmentation to provide internal enclaves)

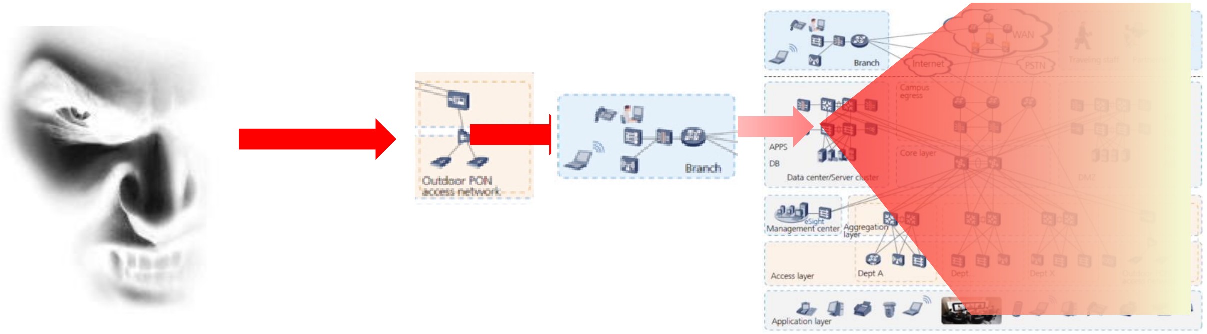
Draw from other disciplines that deal with non-adversarial threats (e.g., safety and survivability) (e.g., use randomizing compilers, multiple OSs, alternate protocols to provide diversity; employ virtualization to support non-persistent services to flush out malware; employ voting on multiple systems to detect corrupted outputs)

Draw from other disciplines that deal with active threats (e.g., sports and military) (e.g., provide misleading information and use deception environments to confuse adversaries, employ moving target defenses, change behavior or states at random times)

Cyber Resiliency

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Example Scenario



Attacker uses 0-day exploit to penetrate systems at local facility

Malware spreads within local facility; user accounts compromised

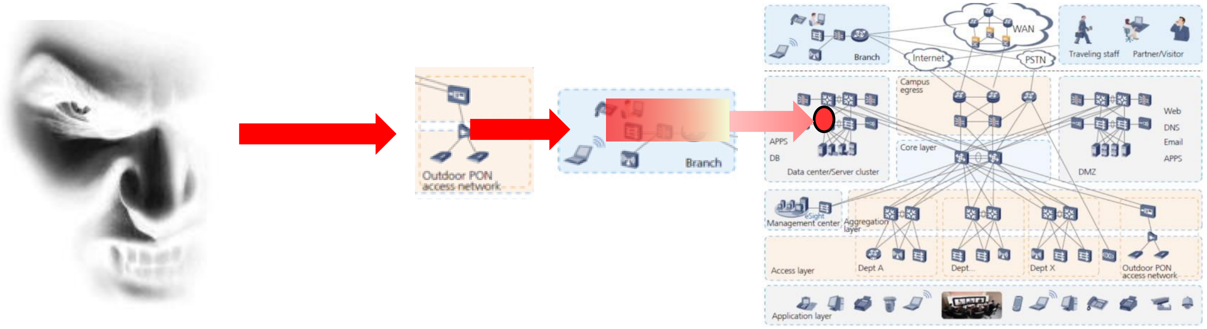
Malware takes advantage of homogeneous software environment, compromised accounts to spread to corporate network

Static host environment enables attacker to maintain foothold

Traditional defenses (boundary protection and patching) are insufficient

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Example Scenario with Cyber Resiliency Applied



Resiliency enables the enterprise to complete missions, provide essential services, or perform essential functions *despite* successful attacks.

- **Segmentation: distinct internal enclaves** → ***Contain adversary's advance***
- **Diversity: run IE, Chrome, Firefox, etc.** → ***Negate adversaries assumptions***
- **Non-Persistence: reimage software periodically** → ***Expunge malware (foothold lost)***
- **Substantiated Integrity: quality / consistency checks** → ***Detect corruption, limit its effects***
- **Deception: detonation chambers, honeynets** → ***Detect malware, divert adversary***
- **Unpredictability: ASLR, randomizing compiler, …** → ***Delays attack progression***

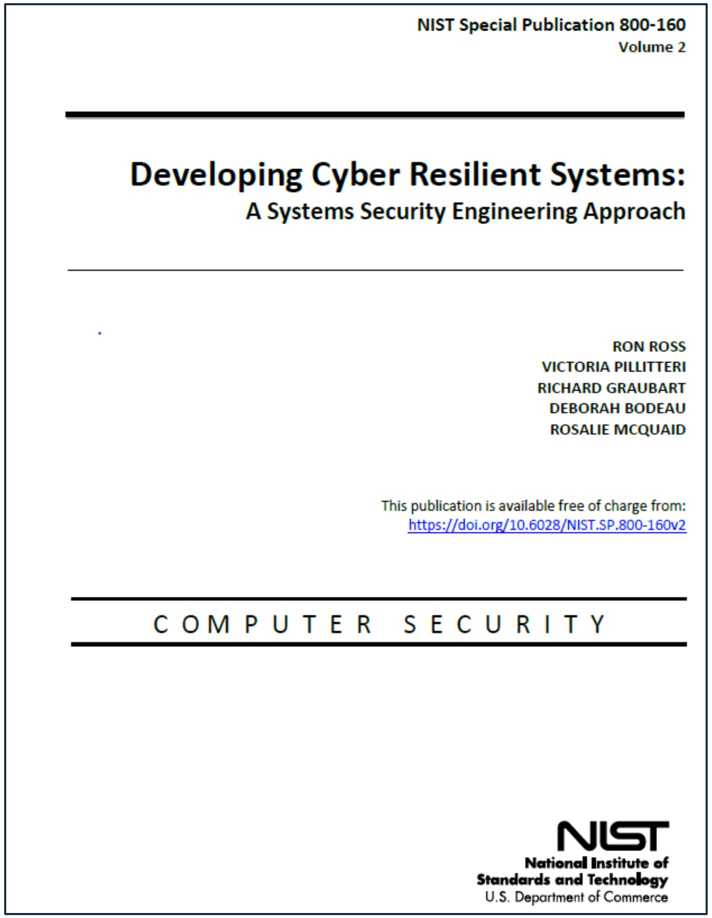
Knowledge of specific attack not required
Patching of vulnerabilities not the focus
Detection of adversaries is helpful but not required
AND It's not just about technology – includes defender TTPs

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Cyber Resiliency Resources (1 of 3)

NIST SP 800-160 Volume 2, Final– Developing Cyber Resilient Systems: *A Systems Security Engineering Approach*

- Includes definitions of the cyber resiliency goals, objectives, techniques, implementation approaches, design principles … and describes how they relate and how they are used
- Identifies cyber resiliency controls in NIST SP 800-53R5
- Provides systems engineering guidance for applying cyber resiliency
- Provides notional worked examples



NIST Special Publication 800-160
Volume 2

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.800-160v2

COMPUTER SECURITY

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

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Cyber Resiliency Resources (2 of 3)

Start with the most recent resources

Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring (2018)
https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-measures-of-effectiveness-and-scoring

Cyber Resiliency Metrics Catalog (2018)
https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-catalog

Cyber Resiliency Metrics and Scoring in Practice: Use Case Methodology (2018)
https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-and-scoring-in-practice-use-case-methodology

Cyber Resiliency Design Principles (2017)
https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf

Augment with resources which answer specific questions

Cyber Resiliency Metrics: Key Observations (2016)
https://www.mitre.org/sites/default/files/publications/pr-16-0779-cyber-resilience-metrics-key-observations.pdf

The Risk Management Framework and Cyber Resiliency (2016)
https://www.mitre.org/sites/default/files/publications/pr-16-0776-cyber-resiliency-and-the-risk-management-framework.pdf

Resiliency Mitigations in Virtualized and Cloud Environments (2016)
https://www.mitre.org/sites/default/files/publications/pr-16-3043-virtual-machine-attacks-and-cyber-resiliency.pdf

A Measurable Definition of Resiliency Using "Mission Risk" as a Metric (2014)
https://www.mitre.org/sites/default/files/publications/resiliency-mission-risk-14-0500.pdf

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Cyber Resiliency Resources (3 of 3)

Get a sense of the area

Cyber Resiliency FAQ (2017)
https://www.mitre.org/sites/default/files/PR_17-1434.pdf

Cyber Resiliency Resource List (2016)
http://www2.mitre.org/public/sr/Cyber-Resiliency-Resources-16-1467.pdf

Industry Perspectives (2015)
http://www2.mitre.org/public/industry-perspective/

Situate in terms of cyber preparedness

Short summary (2017)
https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-motivating-organizational-cyber-strategies.pdf

Extended version (2017)
https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2

Additional References – Cited on Slide 2 (Representative Examples of Publications Motivating Consideration of Cyber Resiliency)

World Economic Forum, "Cyber Resilience Playbook for Public-Private Collaboration," 9 August 2018. [http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf.

K. Jordan, "Cyber Hygiene, Collaboration, and Preparedness: Keys to Resilience for a Healthcare Under Threat," Global Cyber Alliance, 3 June 2020. https://www.globalcyberalliance.org/cyber-hygiene-collaboration-and-preparedness-keys-to-resilience-for-a-healthcare-under-threat/.

NIST, "NIST SP 1800-30 (DRAFT): Securing Telehealth Remote Patient Monitoring Ecosystem," 16 November 2020. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/rpm-nist-sp1800-30-draft.pdf.

"Cybersafe Healthcare: Options for strengthening cybersecurity in Canada's healthcare sector," 27 March 2018. https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf.

CISA, "Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," Cybersecurity and Infrastructure Security Agency, 17 December 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

FDA, "Postmarket Management of Cybersecurity in Medical Devices," 28 December 2016. https://www.fda.gov/media/95862/download.

J. Best, "Could implanted medical devices be hacked?," The British Medical Journal, 14 January 2020. https://www.bmj.com/content/bmj/368/bmj.m102.full.pdf.

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-2