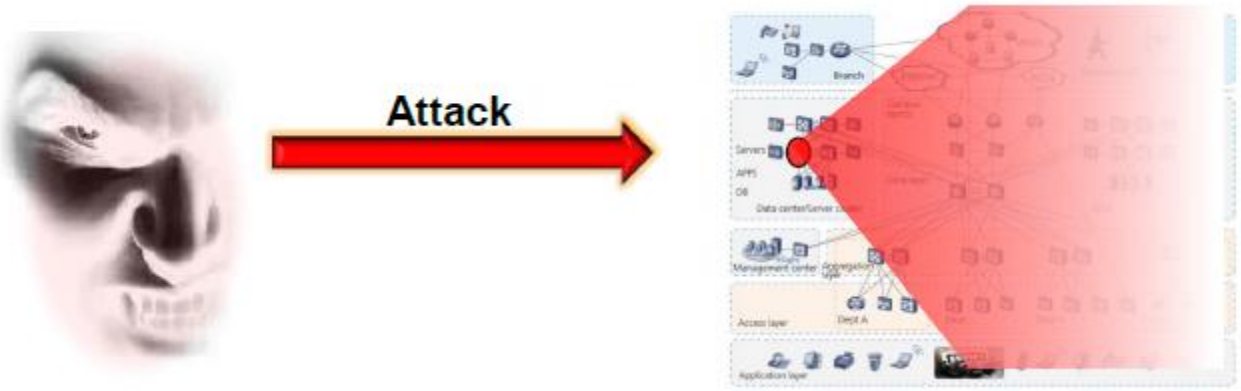
Cyber Security in the Agile Cloud



The Attack Surface

100,000 files per organization that represent risk

Number of files per organization stored in public cloud applications that violate corporate data security policy, amplifying the danger of exposing sensitive information.

4,000 exposed files per organization contain username & password information

Number of exposed files per organization stored in public cloud applications containing credentials to corporate systems, inviting cybercriminals to hijack corporate SaaS environments.

1 in 4 employees violating security policies

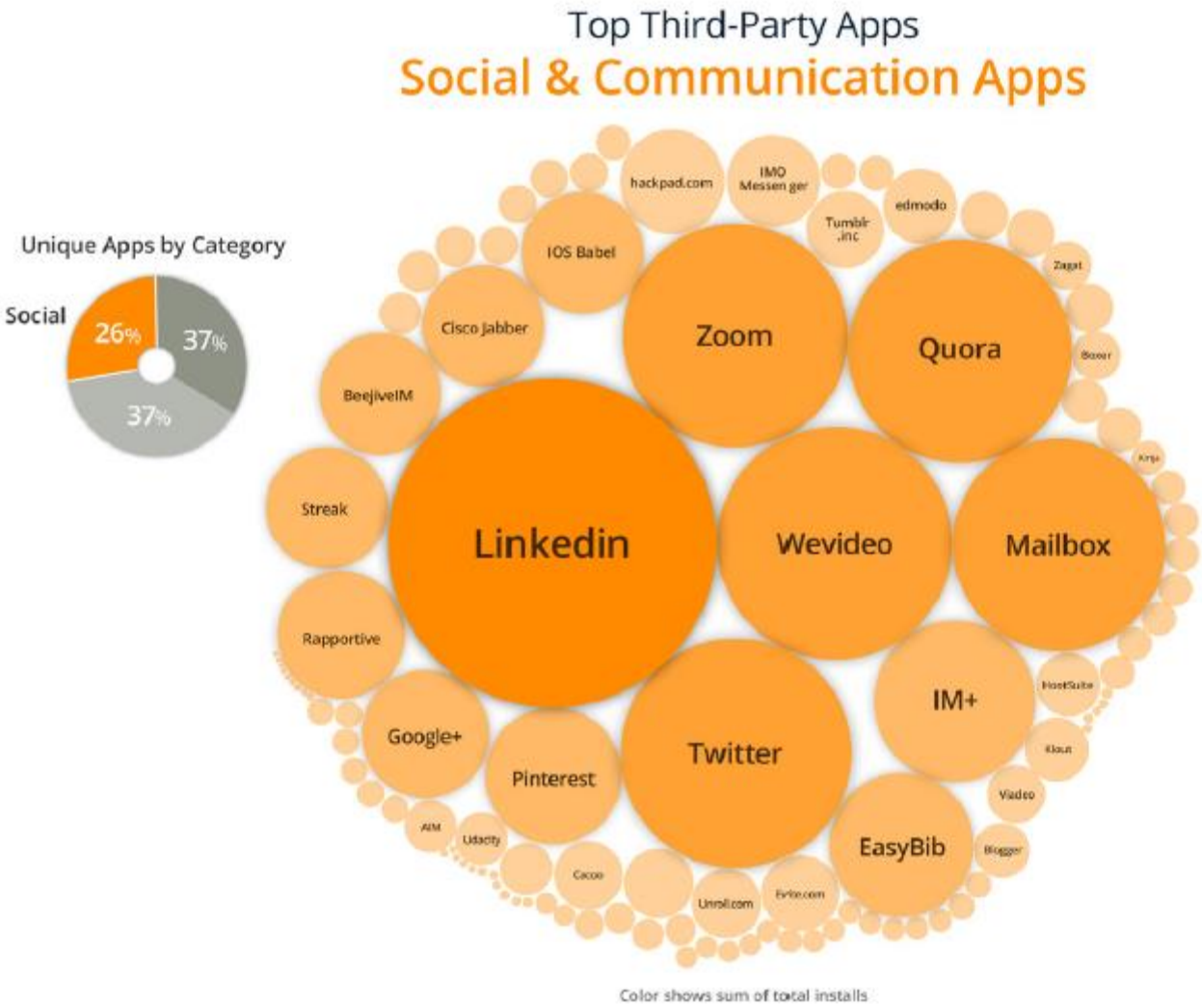
Number of employees that violate corporate data security policy in public cloud applications, opening organizations to risk of data breach and compliance concerns.

45,000 third-party apps installs conducted by privileged users

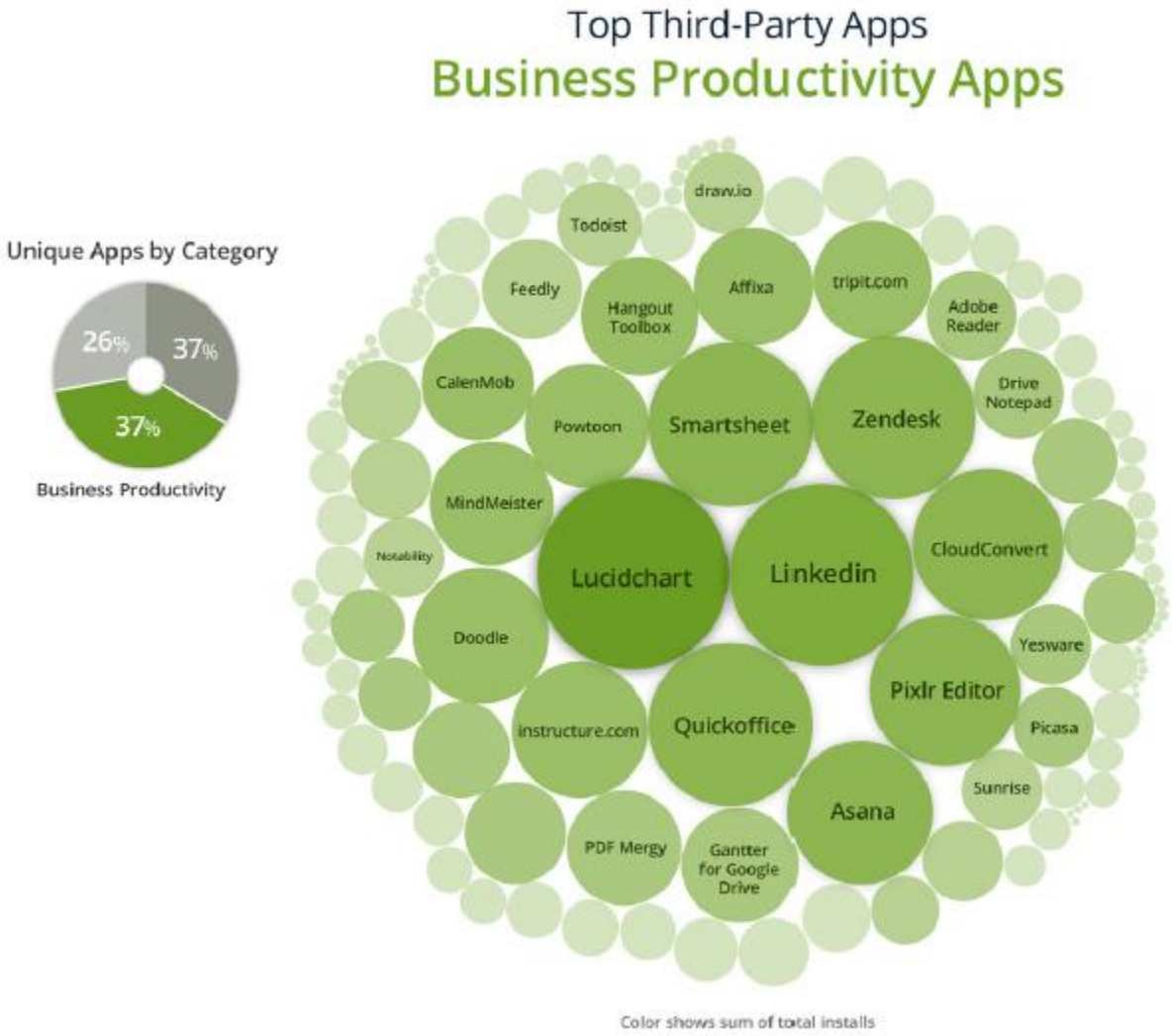
Third-party cloud applications with access to privileged users accounts significantly elevates organizational risk.

The Attack Surface

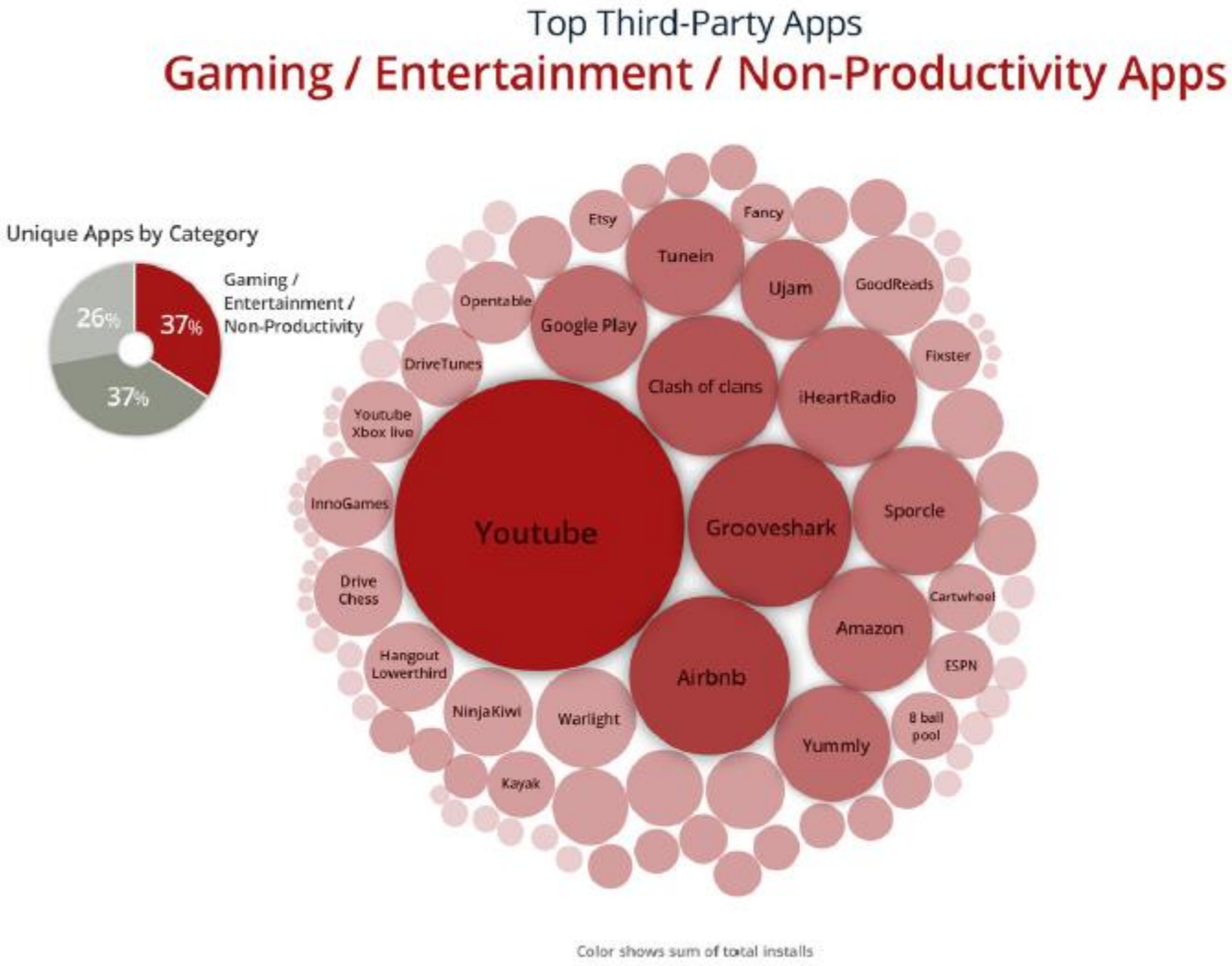
The Attack Surface



The Attack Surface



The Attack Surface



Cyber Resiliency Engineering Framework (CREF)

Richard Graubart

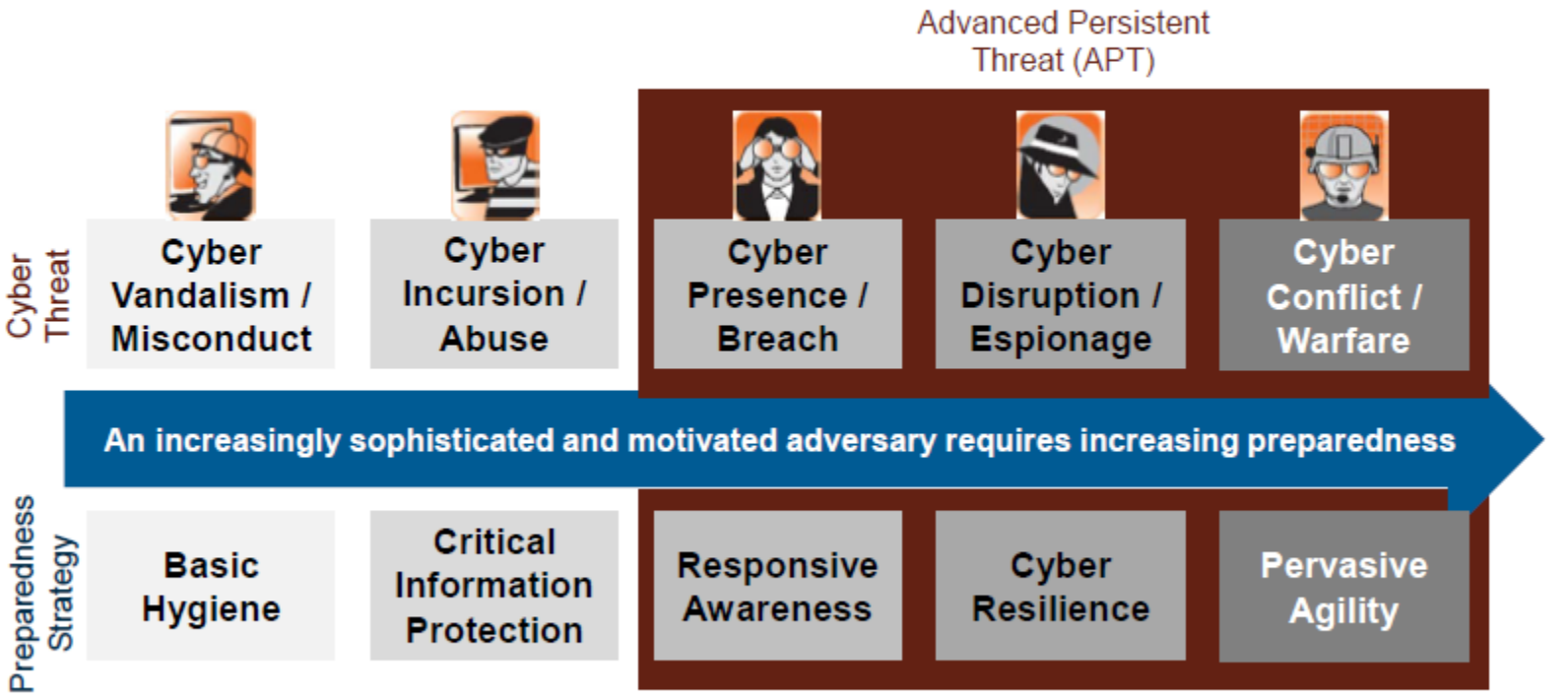
RDG@MITRE.ORG

November 17, 2015

MITRE is a not-for-profit organization that operates research and development centers sponsored by the federal government.

MITRE

Cyber Resiliency Takes the APT into Consideration



APT disrupts traditional resiliency (non-cyber) assumptions:

- Stealthy, embedded APT => multi-occurrence events
- Intelligent adversary => attack evolves in response to defender actions

Cyber Resiliency: Definition

The ability of cyber systems and cyber-dependent missions to

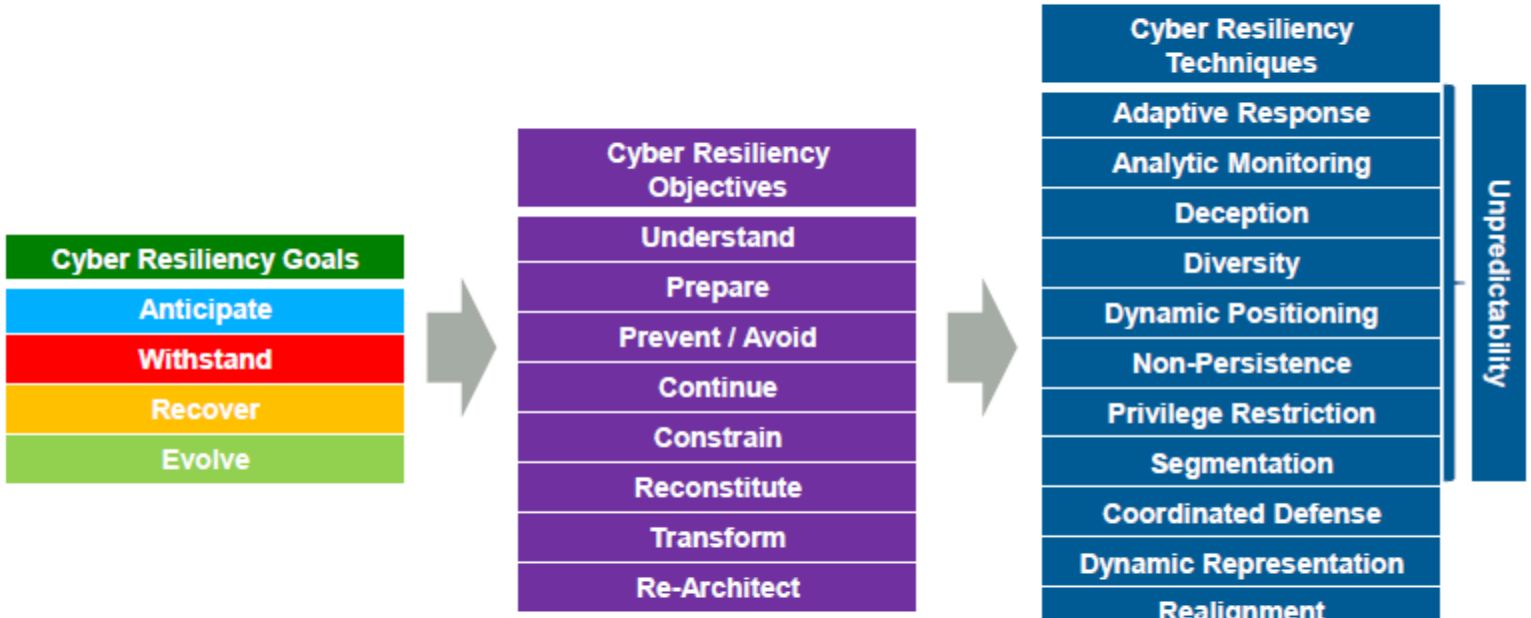
- anticipate,
- continue to operate in the face of,
- recover from, and
- evolve to better adapt to

advanced cyber threats

Cyber Resiliency Goals

Anticipate	Maintain a state of informed preparedness for adversity
Withstand	Continue essential mission/business functions despite adversity
Recover	Restore mission/business functions during and after adversity
Evolve	Adapt mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments

Cyber Resiliency Engineering Framework (CREF): Mapping the Landscape



Different objectives support different goals.
Different techniques support different objectives.
Different stakeholders will be more concerned about different goals & objectives.
Techniques vary in maturity, applicability to architectural layers, and suitability to operational environments – no system can (or should) apply them all.

Cyber Resiliency Objectives Provide Basis for Defining Cyber Resiliency MOEs

Objective	Representative Examples of MOEs
Understand	• Time to map network, % of network mapped • Time to assess health of network nodes, % assessed
Prepare	• % mission functions for which criticality is known • Time between ingest of threat intelligence and development or selection of cyber course of action
Prevent / Avoid	• % of network nodes, services with up-to-date patches & configuration settings
Continue	• % of mission-critical functions operating at acceptable level
Constrain	• Time between alert and successful change to network configuration
Reconstitute	• % of mission-essential functions restored to acceptable level of functioning within [specified] time
Transform	• % of contingency plans that consider cyber attack as a source or complicating factor
Re-Architect	• % of mission-critical components that have been designed, implemented, and configured to address advanced threats

Engineering Considerations for Selecting Techniques to Apply

- **Neither desirable nor feasible to apply all cyber resiliency techniques to an architecture**
  - Limited resources
  - Legacy components / interoperability with legacy
  - Implementation of some techniques makes implementations of others more difficult
- **Take the Advanced Persistent Threat into consideration**
  - Apply techniques to affect adversary activities throughout the cyber attack lifecycle
- **As feasible leverage existing capabilities, developed for other purposes (e.g., performance, stability, security)**

Cyber Resiliency Techniques (1 of 2)

Adaptive Response	Implement nimble cyber courses of action (CCoAs) to manage risks
Analytic Monitoring	Gather, fuse, and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities, and damage
Coordinated Defense	Manage multiple, distinct mechanisms in a non-disruptive or complementary way
Deception	Mislead, confuse, or hide critical assets from, the adversary
Diversity	Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities
Dynamic Positioning	Distribute and dynamically relocate functionality or assets
Dynamic Representation	Construct and maintain current representations of mission posture in light of cyber events and cyber courses of action

Cyber Resiliency Techniques (2 of 2)

Non-Persistence	Generate and retain resources as needed or for a limited time
Privilege Restriction	Restrict privileges required to use cyber resources, and privileges assigned to users and cyber entities, based on the type(s) and degree(s) of criticality
Realignment	Align cyber resources with core aspects of mission/business functions
Redundancy	Provide multiple protected instances of critical resources
Segmentation	Define and separate (logically or physically) components on the basis of criticality and trustworthiness
Substantiated Integrity	Ascertain whether critical services, information stores, information streams, and components have been corrupted
Unpredictability	Make changes randomly or unpredictably

Cyber Resiliency: The Bottom Line

Why	The bad guys *will* get in
What	Keep the mission going
How	Architect for resilience Change how we respond to attacks Integrate organizational structures
When	*Now* – build on existing people, processes, and products


THANK
YOU!