ABCs of Operational Resilience

Nader Mehravari
Research Scientist, CERT® Division

Dr. Nader Mehravari is with the CERT® Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. His current areas of interest and research include operational resilience, protection and sustainment of critical infrastructure, preparedness planning, and associated risk management principles and practices.

Nader was with Lockheed Martin from 1992 through 2011. In his most recent assignment, he was the Director for Business Resiliency. In this capacity, he led and oversaw all preparedness planning and associated governance and compliance activities. He was responsible for building and leading Lockheed Martin's resiliency program where he successfully implemented a modern, integrated, risk management based approach to disaster recovery, business continuity, pandemic planning, crisis management, emergency management, and workforce continuity for all of Lockheed Martin.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
23 JAN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
ABCs of Operational Resilience	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**73**	

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0000900

Contents

Organizational Mission

"The American Red Cross prevents and alleviates human suffering in the face of emergencies by mobilizing the power of volunteers and the generosity of donors."

Disaster Relief

Safe and Adequate Blood Supply

Health and Safety Education

UNITED STATES POSTAL SERVICE

"To provide postal services to bind the Nation together … To provide prompt, reliable, and efficient services to patrons in all areas and … render postal services to all communities."

- Delivering Mail
- Selling Stamps
- Ensuring Mail Safety
- Operating a 37,000-node intranet
- ○ ○ ○

DISA

"Provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations."

DISN, NIPRNET, SIPRNET…	Enterprise Email Services	Spectrum	Tactical InfoSec Services

Contributing positively to the earth's natural ecosystem.

- Shade
- Habitat for Birds
- Climbing Opportunity
- Beauty

Operational Stress

Saturday, February 4, 2012 New York 89°|74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home ▾ | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life & Cu

Digits | Personal Technology | What They Know

TECHNOLOGY | February 4, 2012

Micron Chief Dies in Crash

Steve Appleton Loved Fast Jets, Cars; 'I'd Rather Die Living Than Die Dying'

Article | Stock Quotes | Comments (122)

By SHARA TIBKEN and DON CLARK

A A

Steven R. Appleton, chairman and chief executive of Micron Technology Inc. MU 0.00% and one of the most prominent figures in the semiconductor industry, died Friday when the high-performance airplane he was piloting crashed at Boise, Idaho's airport.

The death of the 51-year-old stunned Micron, the well-known maker of memory chips based in the same city, and comes at a time of rapid change for the company and its industry.

The National Transportation Safety Board is investigating the accident, which happened soon after Mr. Appleton took off alone in a single-engine Lancair. The plane, from a maker of aircraft kits, had taken off and landed once and was

Micron

MICRON TECHNOLOGY, INC.

Monday, April 16, 2012 As of 8:21 PM EDT New York 89° | 74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Comm

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life &

Small Business

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketin

BUSINESS | Updated April 16, 2012, 8:21 p.m. ET

Tornadoes Hamper Boeing Supplier

Spirit Says Output Suspended 'At Least' Through Tuesday, Deliveries Could Res of Week

Article | Stock Quotes | Comments

By JON OSTROWER

WICHITA, Kan.—A key Boeing Co. BA +2.51% supplier said it aims to res deliveries by the end of the week after tornadoes battered its factories here highlighting the fragility and resilience of the aerospace giant's global supp it works to sharply increase production.

The storms late Saturday caused significant-to-major damage to 10 buildin flagship campus of Spirit AeroSystems Inc., which makes fuselages and c for Boeing's hot-selling 737, 777 and 787 Dreamliner passenger jets. Spirit said production—which normally runs seven days a week—would be susp least" through Tuesday, and that it expects "near-term production disruptio including delivery impacts" to customers.

Spirit spokesman Ken Evans assessments found most of its machinery and inventory intact. "We believe we can use the facilities we've got," he said in an interview here in Wichita, a major manufacturing hub for the aerospace industry. "We don't

Tuesday, April 17, 2012 As of 8:36 PM EDT New York 89° | 74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Commu

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life

Small Business

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketing

AUTOS | Updated April 17, 2012, 8:36 p.m. ET

Nylon-12 Haunts Car Makers

Explosion at Big Supplier of Resin for Automotive Parts Has Indu
Shortages

Article | Stock Quotes | Comments (9)

By JEFF BENNETT And JAN HROMADKO

Production shortfalls at a single German auto-parts supplier are beginni
through the global auto business.

More than 200 auto executives met in a Detroit suburb on Tuesday to evaluate a looming shortage of a relatively obscure resin essential to modern auto production.

Inventories of the resin are being depleted a
Industries AG plant in Marl, Germany, that
itself as the only integrated maker of the re
lines.

production before the winter this year and expect that the works to fully repair the plant will take at least three months," an Evonik spokeswoman said. Several Evonik executives attended the meeting on Tuesday.

Chemical plant explosion brakes car makers

The explosion at a German chemicals plant two weeks ago which killed two workers, has thrown the global car industry into turmoil as manufacturers run short of a vital component, prompting an emergency meeting in Detroit.

WHAT 'OBSCURE' BUT ESSENTIAL COMPOUND SHORTAGE HAS THE AUTO INDUSTRY WORRIED ABOUT PRODUCTION?

Tuesday, July 31, 2012 As of 12:30 PM EDT New York 81°|71°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Cult

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketing

BUSINESS | Updated July 31, 2012, 12:30 p.m. ET

India's Power Grid Collapses Again

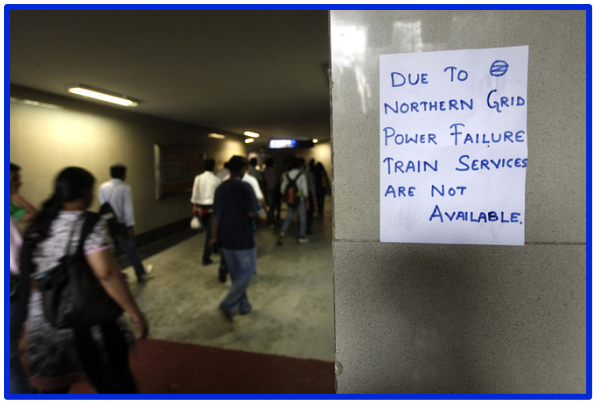
Article | Slideshow | Stock Quotes | Comments (120)

By SAURABH CHATURVEDI And SANTANU CHOUDHURY

A A

NEW DELHI--Much of India's electricity supply network collapsed Tuesday in the country's second major outage in two days, affecting more than 680 million people —double the population of the U.S.—and causing business losses estimated to run into the hundreds of millions of dollars.

Thousands of offices and factories had to switch to generators or shut shop, more than 200 trains were brought to a standstill while hospitals had to ask nurses to manually work critical equipment such as ventilators as 21 provinces experienced a near-total



India electricity grids fail leaves 620 million people without power

THE WALL STREET JOURNAL | News Alert

Computer Glitch Halts American Airlines Flights

The Federal Aviation Administration is holding all American Airlines flights at their origin airports until at least 5 p.m. Eastern time on Tuesday while the carrier tries to resolve a nationwide outage to its reservations system.

THE WALL STREET JOURNAL.

U.S. EDITION ▾ Tuesday, April 16, 2013 As of 5:28 PM EDT

Home | World | U.S. | New York | Business | Tech | Markets | Market Data | Opinion

BUSINESS | Updated April 16, 2013, 5:28 p.m. ET

Outage Snarls American Air Flights

By JACK NICAS And SUSAN CAREY

SANDY SHUTS DOWN THE CITY

By JOHN ANNESE
and JILLIAN JORGENSEN
STATEN ISLAND ADVANCE

The city is in a virtual lockdown as a storm of unprecedented character slammed into the East Coast,

Tracking the storm

The worst of the powerful hurricane is expected Monday night into Tuesday

Hospital evacuated

THE WALL STREET JOURNAL. ≡ WORLD

Powerful Typhoon Haiyan Hits Philippines

By CRIS LARANO and JOSEPHINE CUNETA

Nov. 7, 2013 10:44 a.m. ET

Week of 4/22/13

THE WALL STREET JOURNAL. | NEW YORK

April 19, 2013, 1:37 PM

Train Halt From Boston Stretches to Manhattan

SUBSCRIBE Magazine | Video | LIFE | TIME 100

TIME U.S.

NEWSFEED | U.S. | POLITICS | WORLD | BUSINESS | TECH | HEALTH | SCIENCE | ENTE

NATIONAL

The Marathon Bombing: Gunfights, Blasts and a Manhunt Shut Down Boston

By Jay Newton-Small / Watertown | April 19, 2013 | 0

U.S. NEWS on NBC NEWS.com

Compare hundreds of

Updated 3 days ago

Boston transit shut down, nearly 1 million sheltering in place amid terror hunt

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article

Article | Talk

Advanced persistent threat

From Wikipedia, the free encyclopedia

Advanced persistent threat (APT) usually refers to a group, such as a foreig
effectively target a specific entity. The term is commonly used to refer to cyb
intelligence gathering techniques to access sensitive information[1], but app
Other recognized attack vectors include infected media, supply chain compro
usually referred to as an APT as they rarely have the resources to be both ad
a specific target.[3]

The Washington Post | Politics | Opinions | Local | Sports | National | World | Business | Tech

More companies reporting cybersecurity incidents

By Ellen Nakashima and Danielle Douglas, Published: March 1

At least 19 financial institutions have disclosed to investors in
computers were targets of malicious cyberassaults last year, a
among corporations about the breadth of cybersecurity incide
sector.

In their annual financia
such as Bank of Americ
institutions, have repor
intrusions.

THE WALL STREET JOURNAL.

U.S. EDITION | Saturday, March 16, 2013 As of 4:17 PM EDT | New York 38° | 28°

Home | World | U.S. | New York | Business | Tech | Markets | Market Data | Opinion

DDoS Attacks on U.S. Banks: Worst Yet to Come?

February 19, 2013, 12:01am

against U.S. banks last fall
bilities, whereas the intent of
e been to simply cause

Gartner

WHY GARTNER | ANALYSTS | RESEARCH | EVENTS | CONSULTING | ABOUT

Are the ongoing DDoS attacks against U.S. banks just the calm before the storm?

by **Avivah Litan** | March 14, 2013 | 1 Comment

That's a viable hypotheses after hearing that the attackers only used one third of the bandwidth they had staged for their latest round of attacks against U.S. banks last Tuesday. Reportedly, on Tuesday the total size of the DDoS attack was 190 gigabits at one time, with the largest attack against a single bank at 110 gigabits.

Interestingly, the attackers could have easily done even more damage but they chose not to. 9200 bots were identified as attack-capable but the total number of bots actually involved in sending the DDoS traffic to the banks numbered only about 3200. The other 6000 bots sat there doing nothing.

April 23, 2013

THE WALL STREET JOURNAL.

U.S. EDITION

Home | World | U.S. | New York | Business | Tech | Markets | Market Data | Opinion | Life & Culture | Real Estate | Managemen...

TECHNOLOGY | April 23, 2013, 2:19 p.m. ET

False AP Twitter Message Sparks Stock-Market Selloff

By SHIRA OVIDE

The Associated Press said Tuesday its Twitter account was compromised, resulting in a false message on the service that explosions in the White House had injured President Barack Obama. The message briefly sparked selloff on U.S. stock markets.

"The Twitter account has been hacked," the AP said in a statement Tues... tweet about an attack on the White House is false."

Other Twitter accounts associated with Associated Press were quick to ... false Twitter message, which was posted just after 1 p.m. Eastern time. ... afterward, the news organization's main Twitter account was suspended ...

CSO | SECURITY AND RISK Newsletters Dashboard RSS Research Centers White P

Pacemaker hack can deliver deadly 830-volt jolt

Pacemakers and implantable cardioverter-defibrillators could be manipulated for an anonymous assassination

By Jeremy Kirk

October 17, 2012 — IDG News
a deadly, 830-volt shock from so
medical device companies.

SCIENTIFIC AMERICAN™

Sign In / Register

Search ScientificAmerican.com

Health :: News :: June 25, 2013 :: 5 Comments :: Email :: Print

A New Cyber Concern: Hack Attacks on Medical Devices

THE WALL STREET JOURNAL.

U.S. EDITION Thursday, June 13, 2013 As of 7:33 PM EDT

Home World U.S. Business Tech Markets Market Data Your Money Opinion Life &

U.S. NEWS | June 13, 2013, 7:33 p.m. ET

Patients Put at Risk By Computer Viruses

By CHRISTOPHER WEAVER

The Food and Drug Administration is warning makers of heart monitors, mammogram machines and myriad other medical devices that their gear is at risk of

Challenges to Organizational Mission

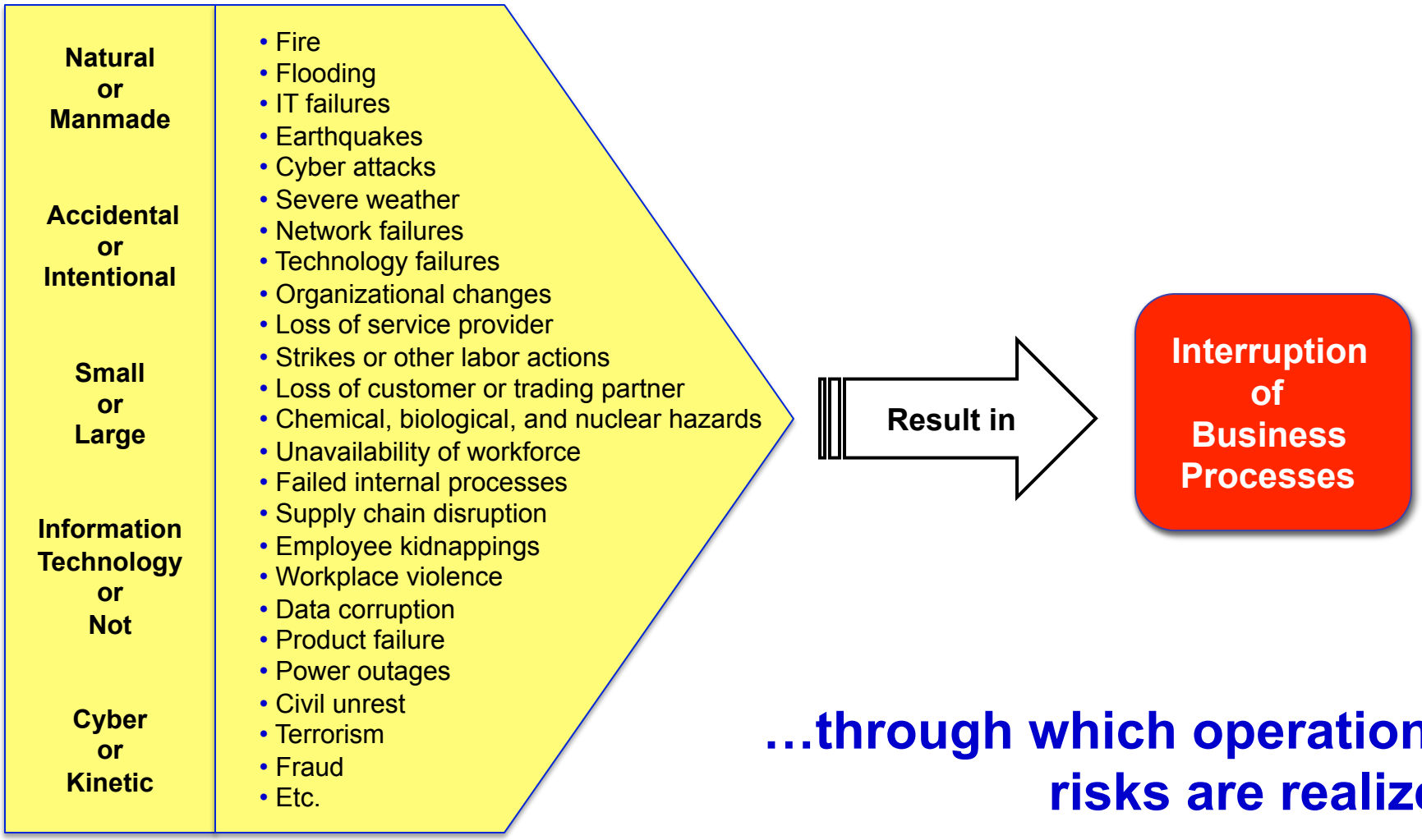
Operational mission of organizations is under stress on a minute-by-minute basis.

The stress comes from

- pervasive use of technology
- globalization
- complexity of business processes
- operational complexity
- movement toward intangible assets
- global economic pressures
- open borders
- geo-political pressures
- regulatory and legal boundaries
- intertwining of cyber and physical domains

…and is exasperated by increased intertwining of cyber and physical domains.

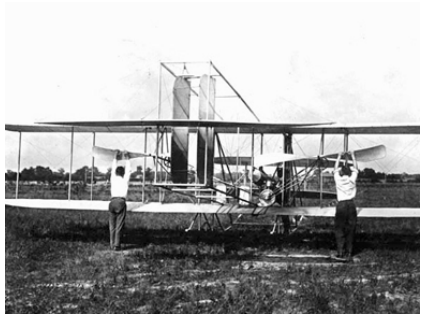
Disruptive Events



…through which operational risks are realized

Yesterday vs. Today

Ever-Increasing Capability & Complexity



Biplane

0 SLOC

Apollo Lunar Module

2K SLOC

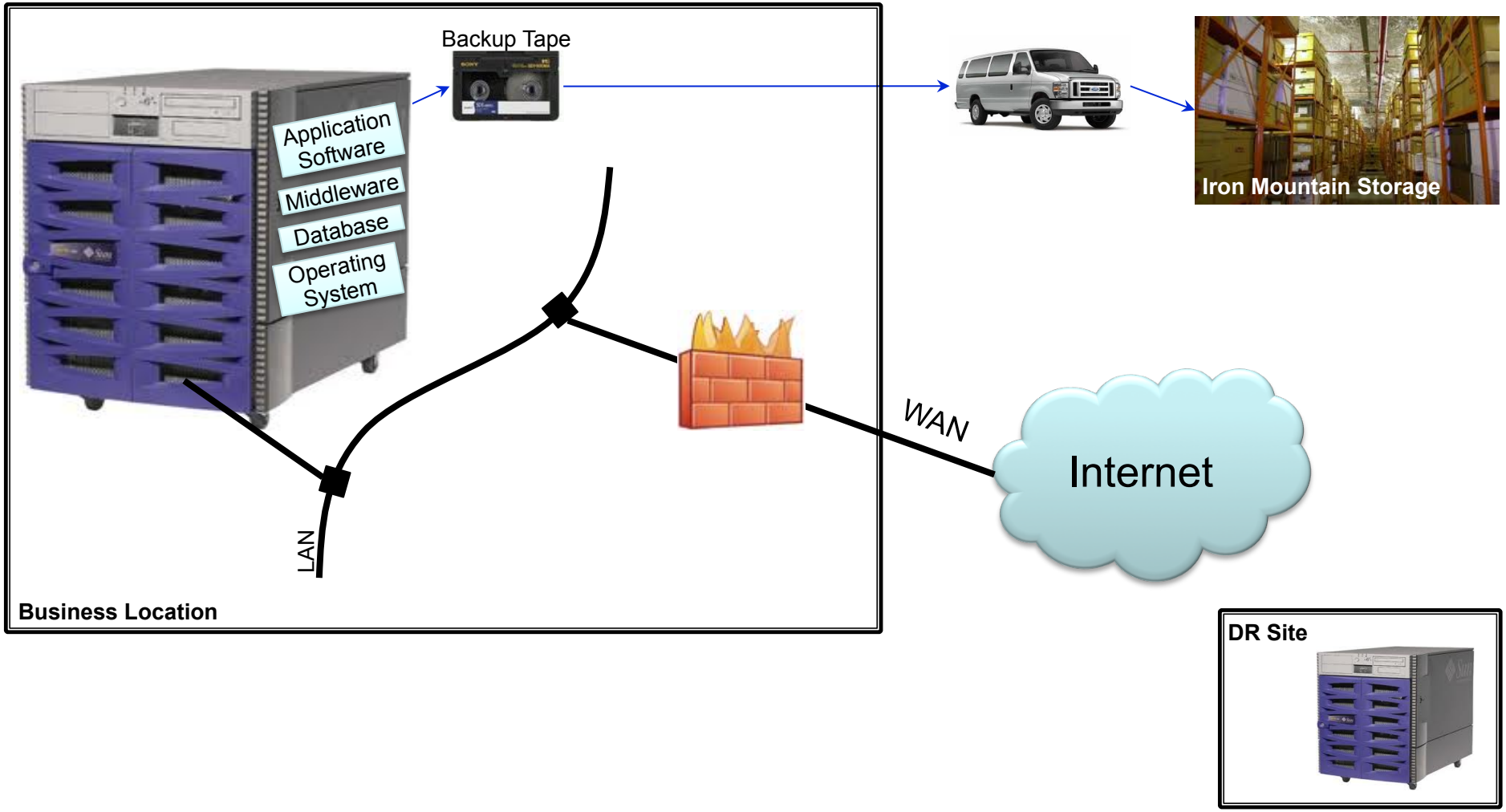
SR-71

500K SLOC

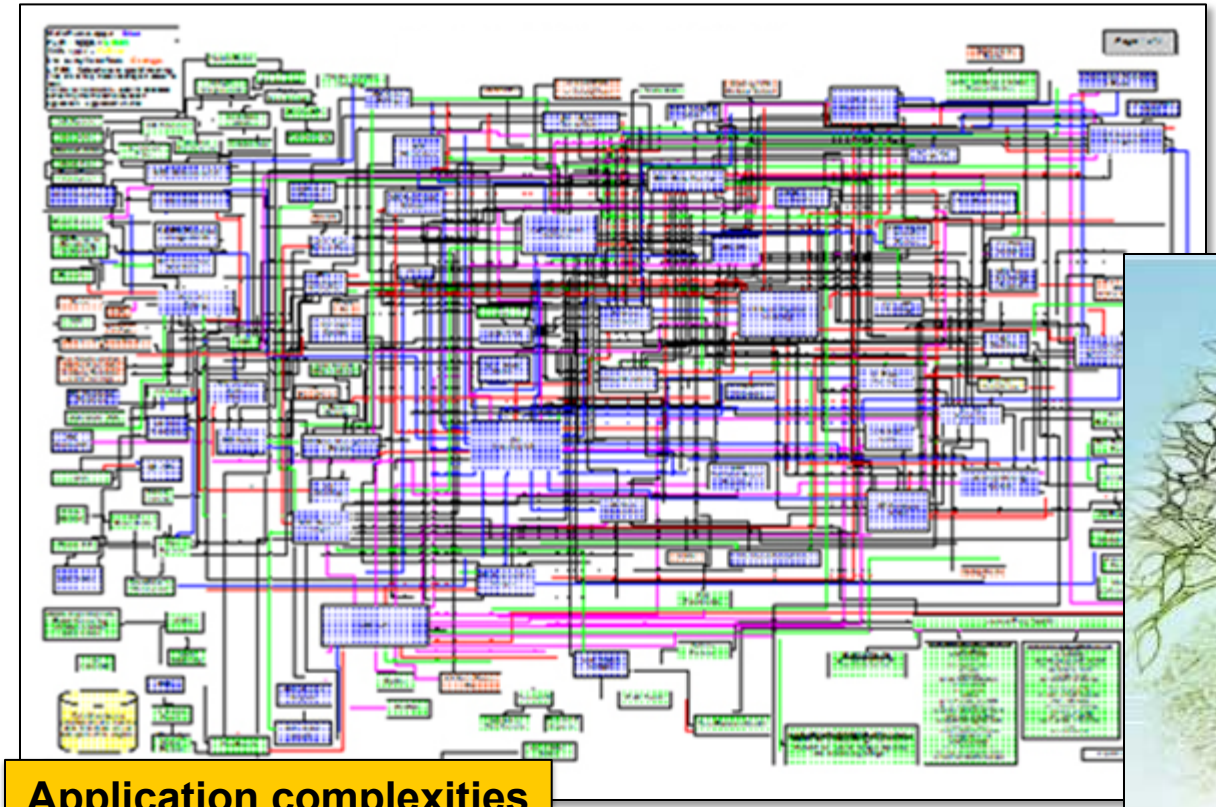
F-35

9.9M SLOC

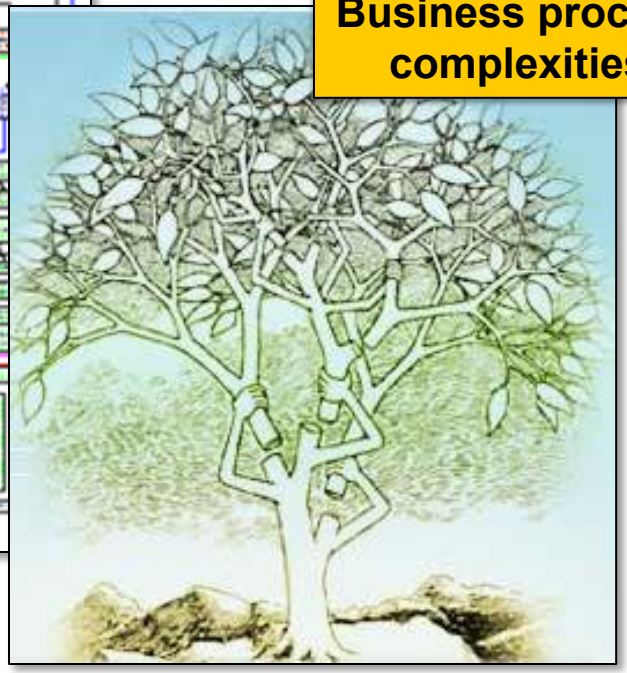
Yesterday's mission success would have been…



Today mission success is about …



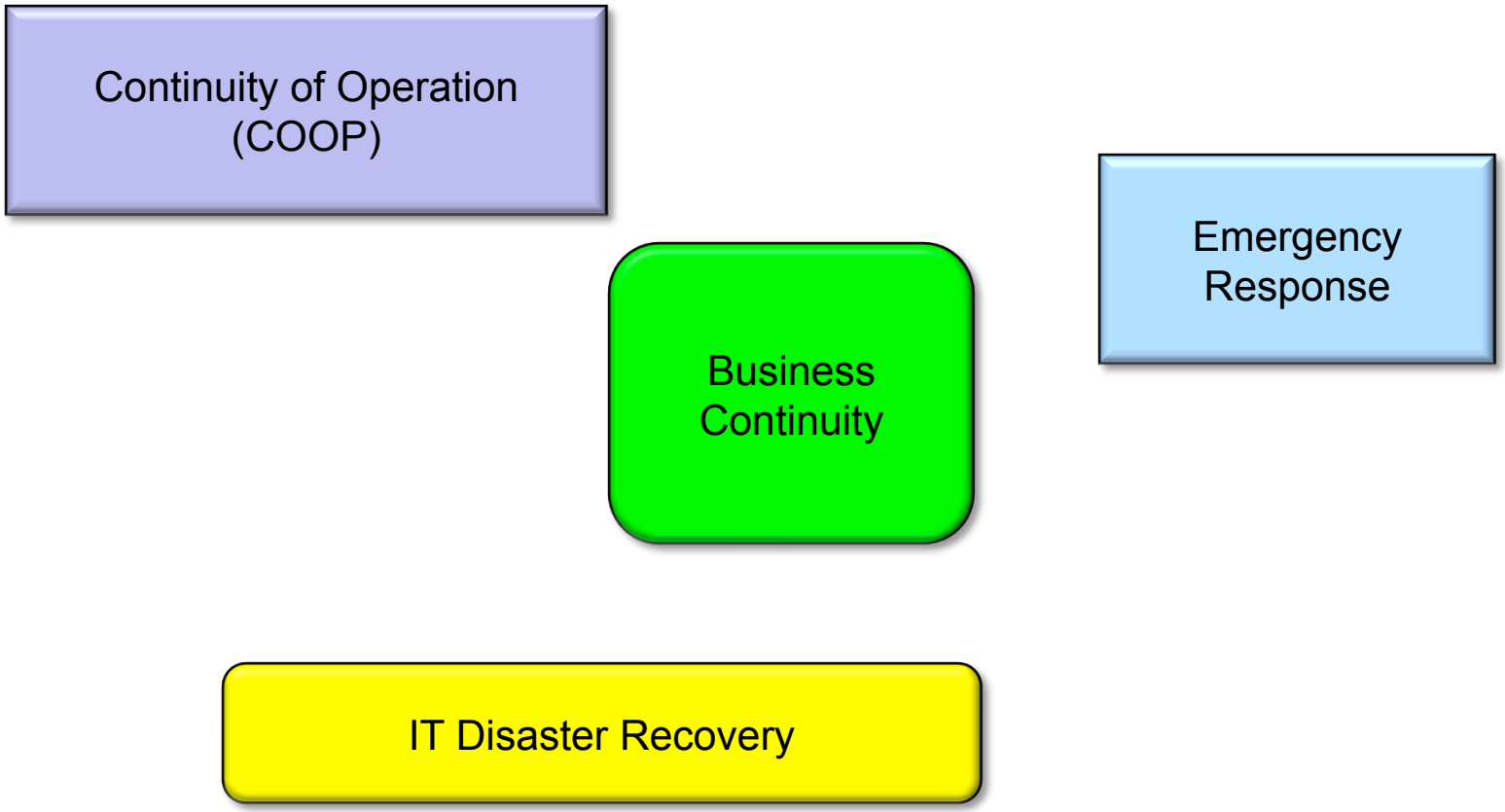
Application complexities



Business process complexities

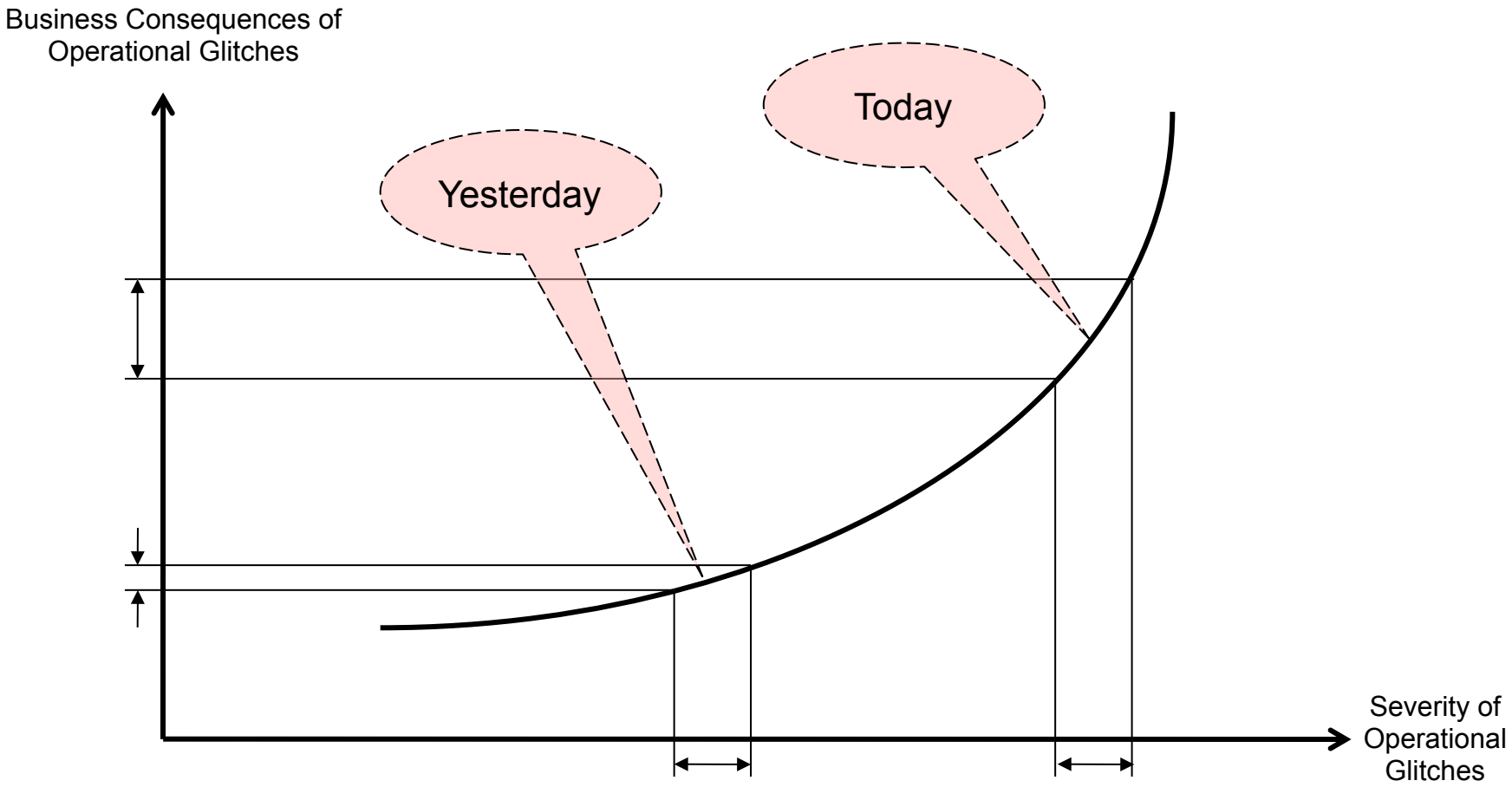
and more…

Yesterday's Mission Protection



Today's Mission Protection

Today's Business Environment



Today's Business Environment Is Much Less Forgiving

Operational Resilience

Operational Risk

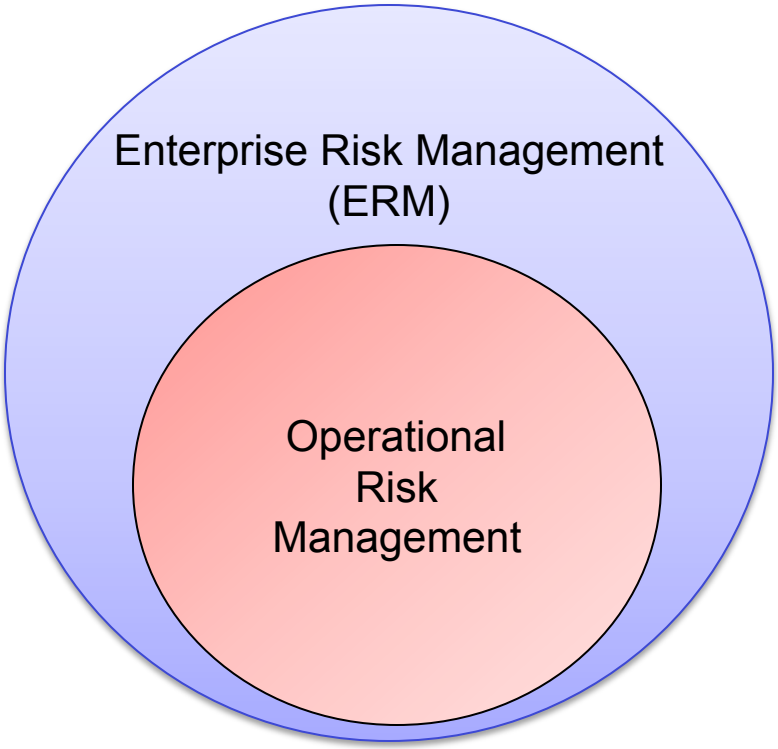
A form of risk affecting day-to-day business operations

A very broad risk category

- from high-frequency low-impact to low-frequency high-impact

Exacerbated by

- actions of people
- systems and technology failures
- failed internal processes
- external events
- bad decisions



Why do operational risks matter?

Trust and confidence of employees and customers

Reputation and image

Regulatory compliance, fines, and legal penalties

Customer retention and growth

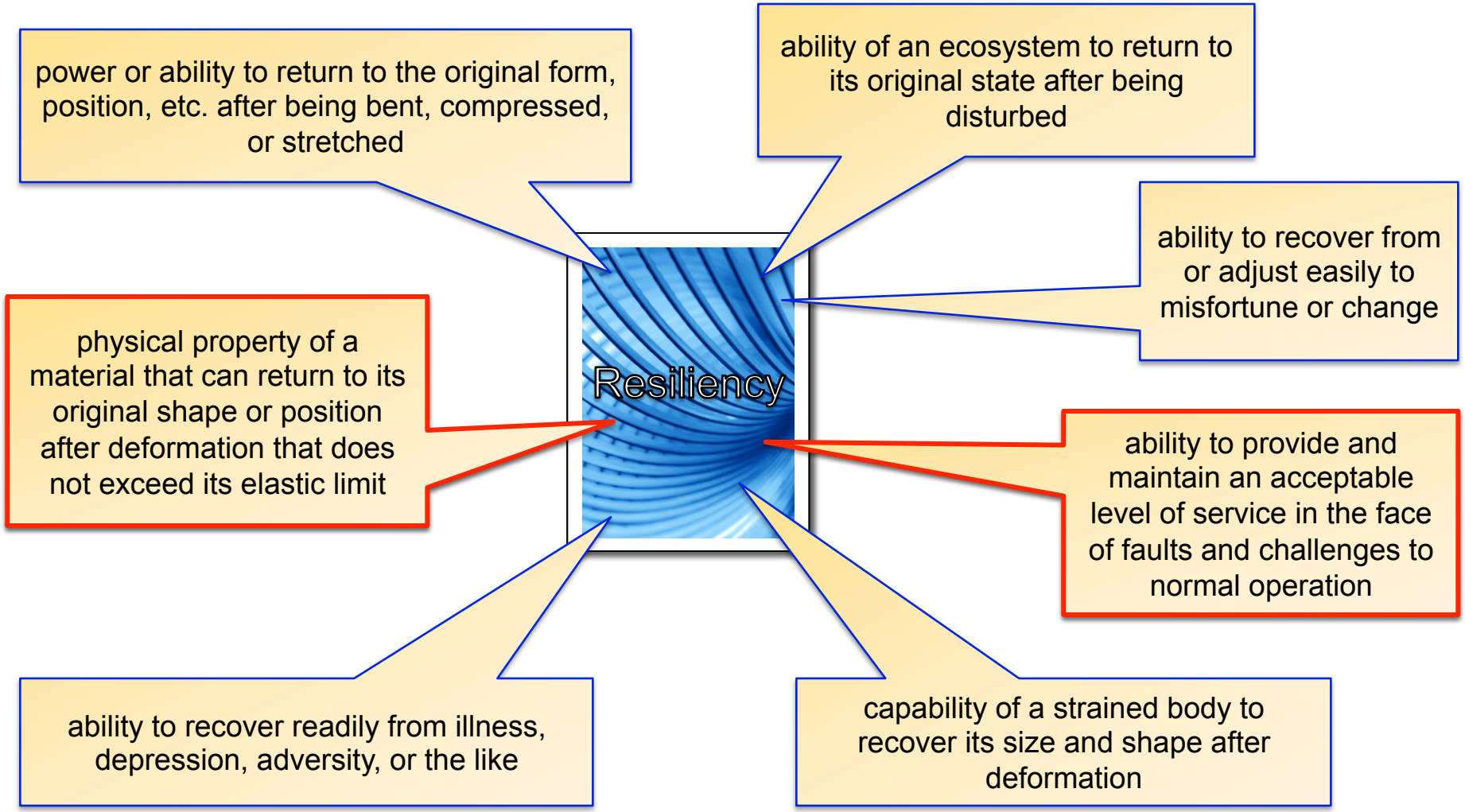
Life, safety, and health of customers and employees

Productivity and profitability

Organizational survival

… because they have explicit and direct IMPACT

re·sil·ience *noun* [ri-ˈzil-yəns]



Operational Resilience

The ***emergent*** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

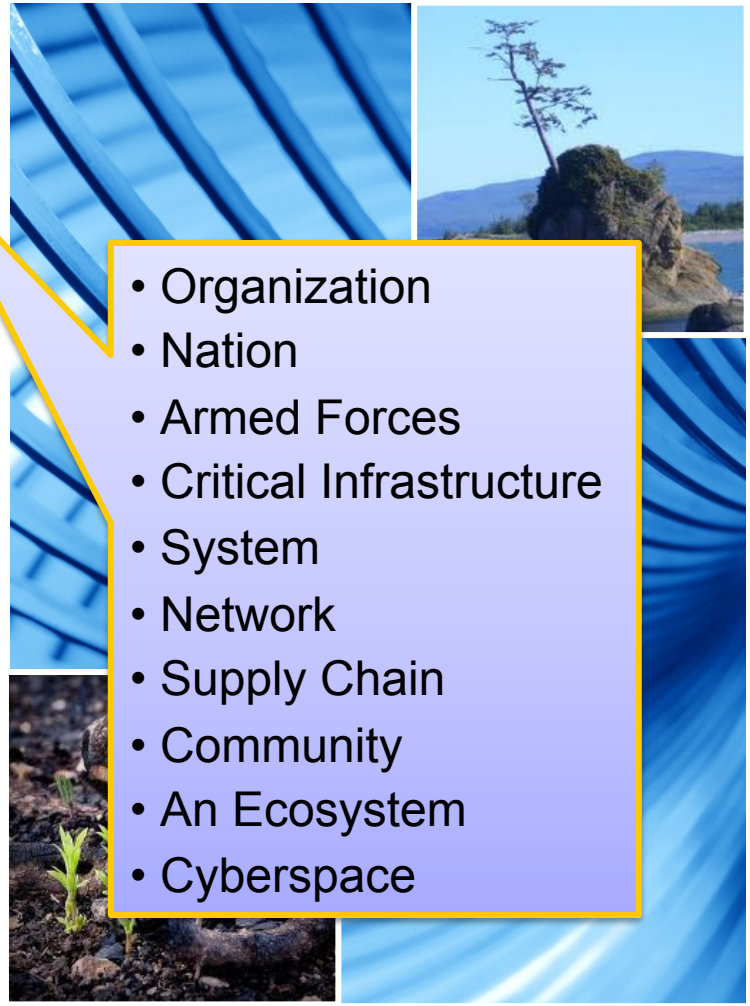
- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated

Operational Resilience

The ***emergent*** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated



An Analogy: Health

Is there a place that you can purchase health?

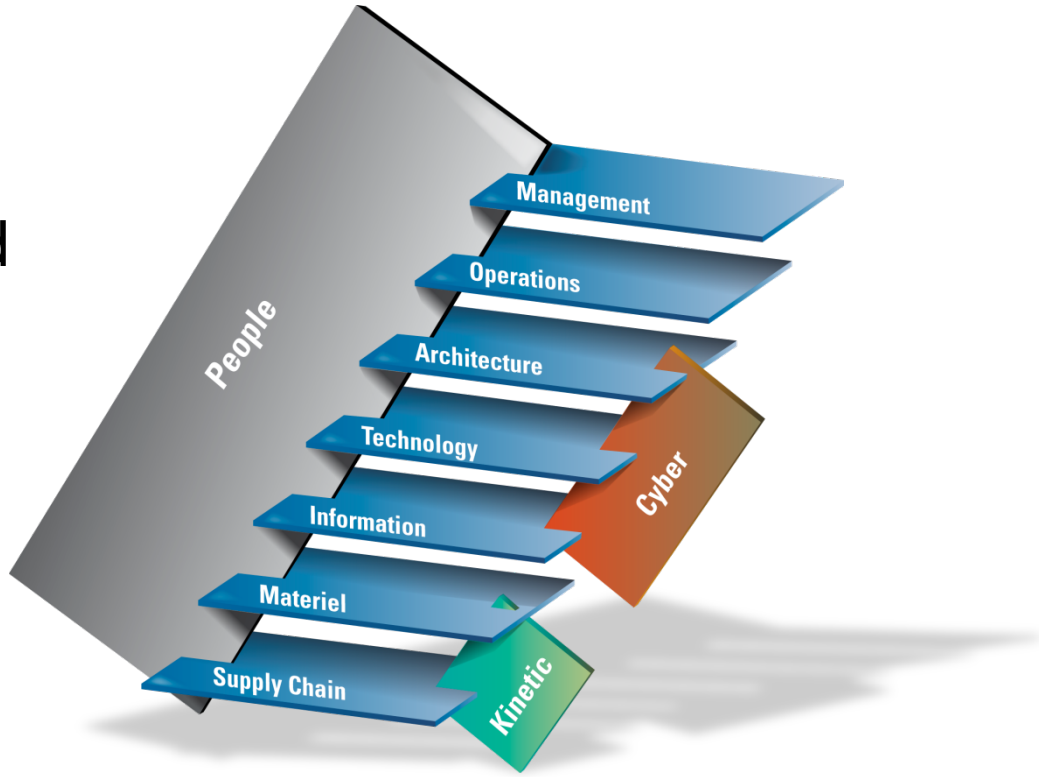
Is there a place where health is manufactured?

How do you become healthy?

Health & Resilience: They are both emergent properties.

Operational Resilience & Mission Success

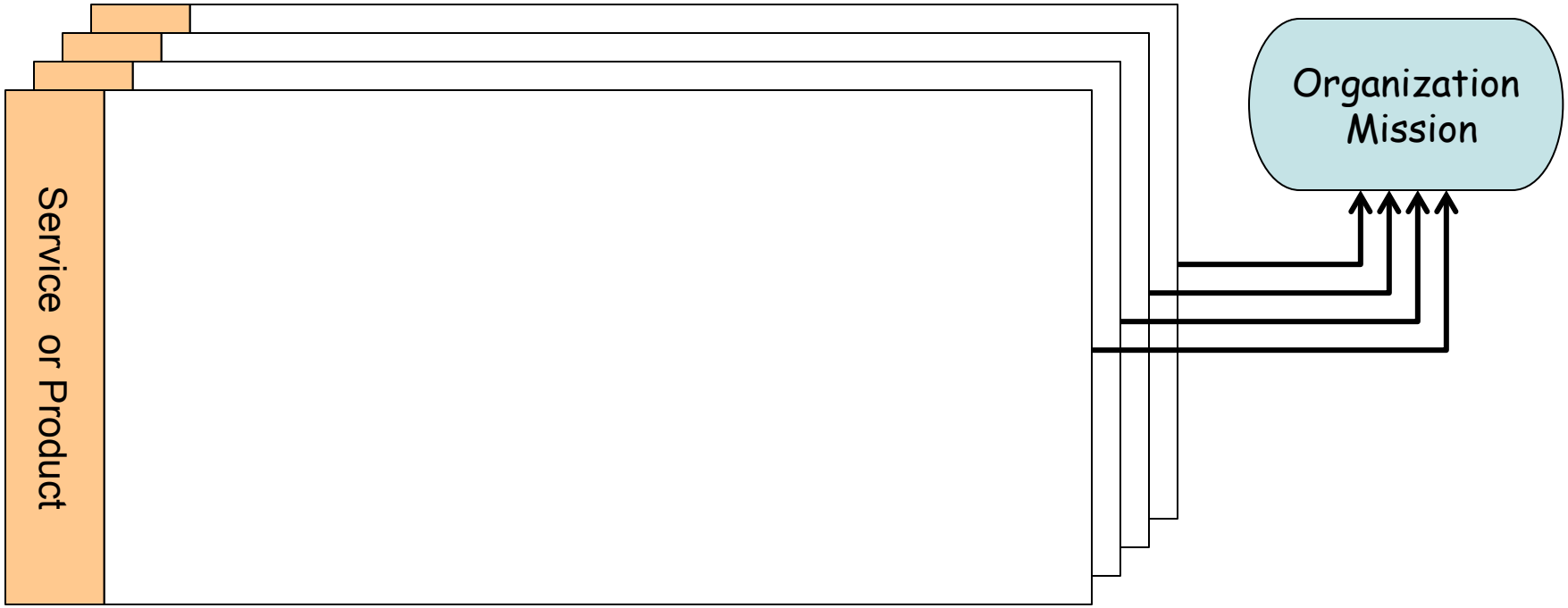
To be operationally resilient, cyber- and/or kinetic-enabled missions must address operational risk on a number of “planes.”



Operational Efforts Must Consider and Enable Such Multidimensionality

Organizational Mission - Revisited

Services and Products

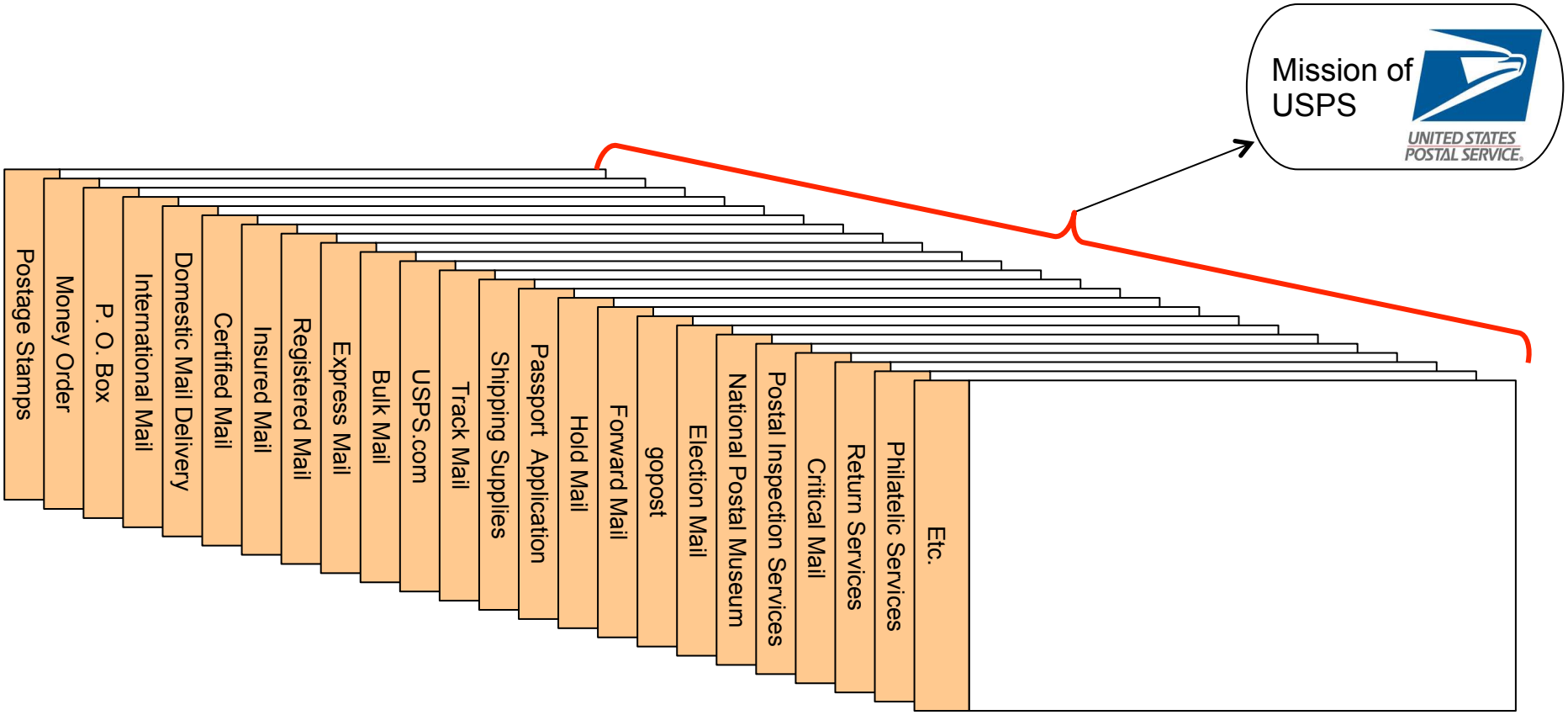


Outputs of an organization

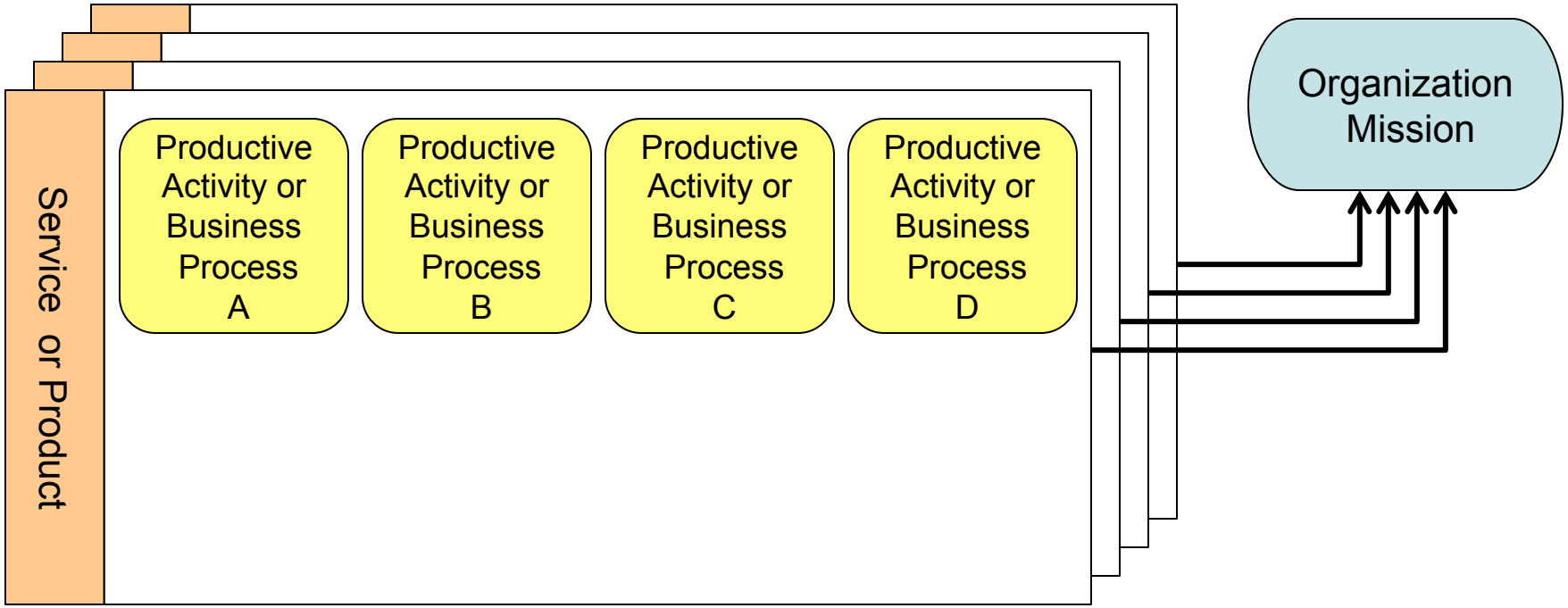
can be internally or externally focused.

Collectively they enable an organization's mission.

Example: U.S. Postal Service



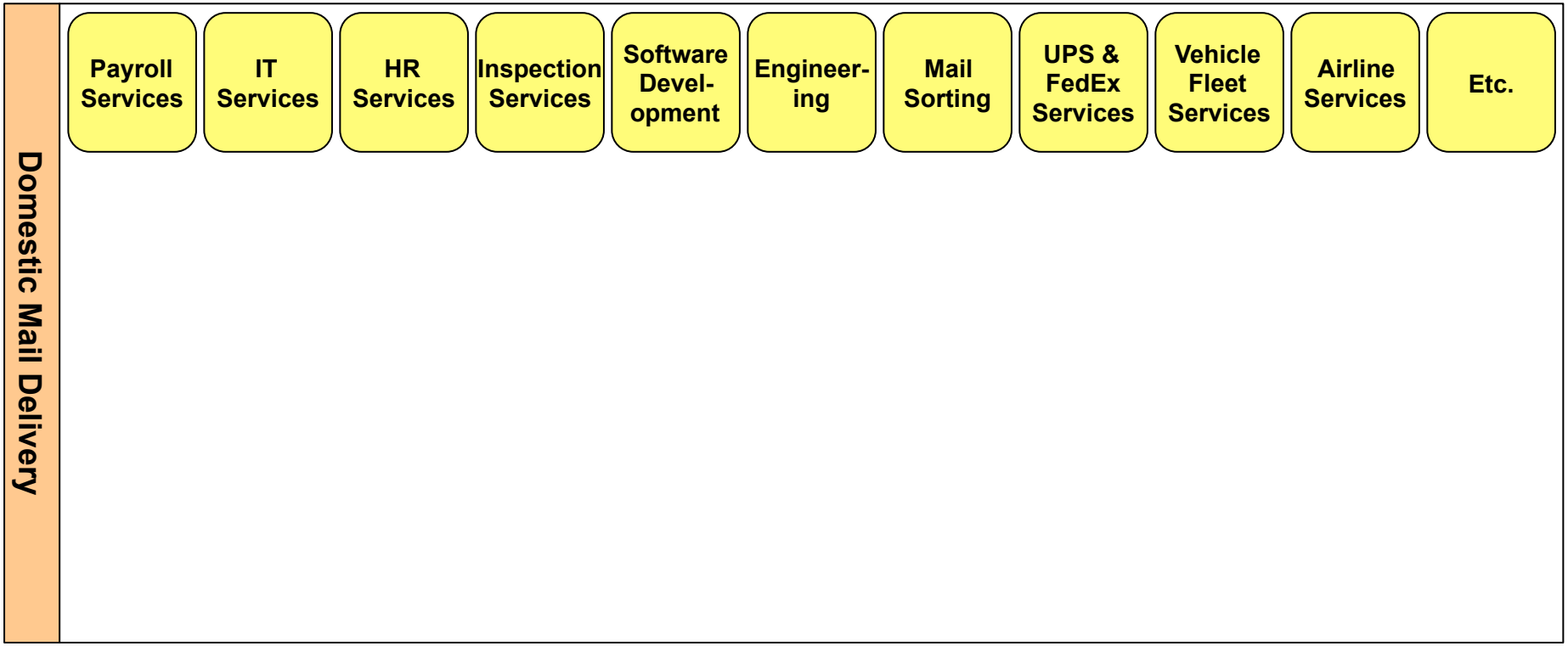
Productive Activities or Business Processes



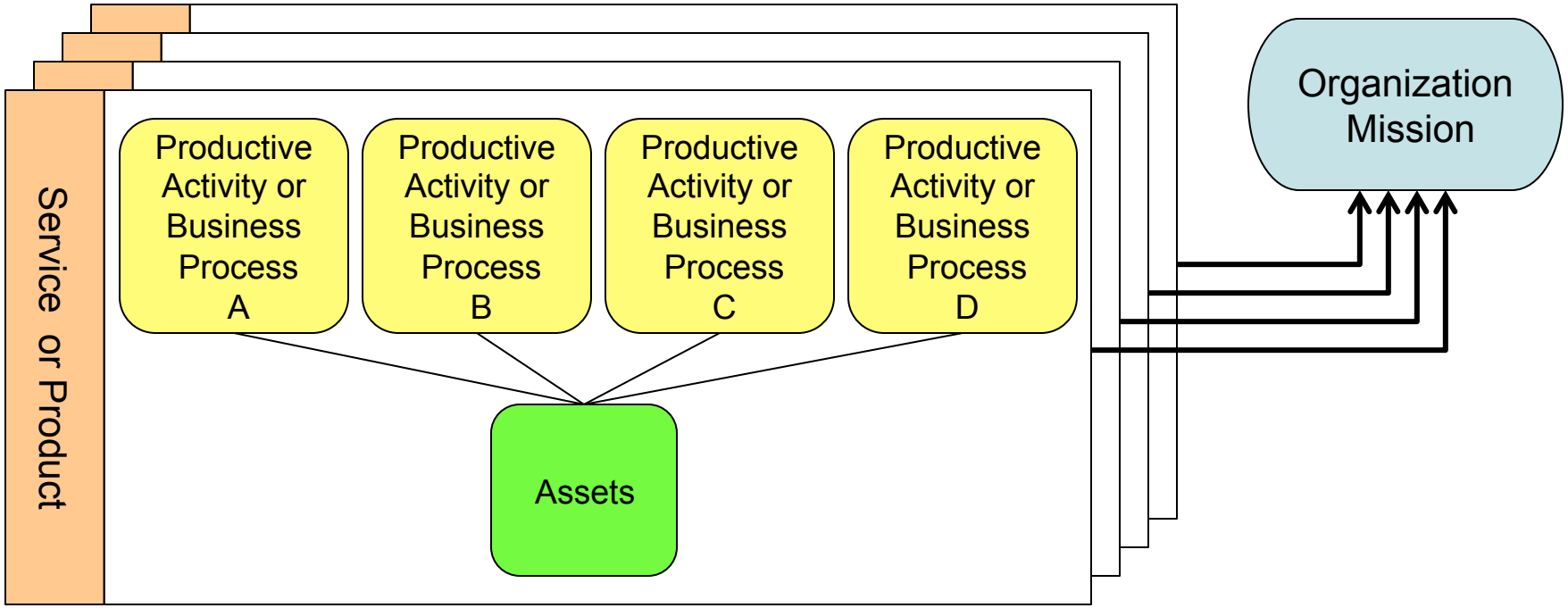
Activities that the organization (and/or its suppliers) perform to ensure that services and products are generated

A service or product is made up of one or more business processes.

Example: U.S. Postal Service



Assets



Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.

Asset Types of Importance to Operational Resilience

People

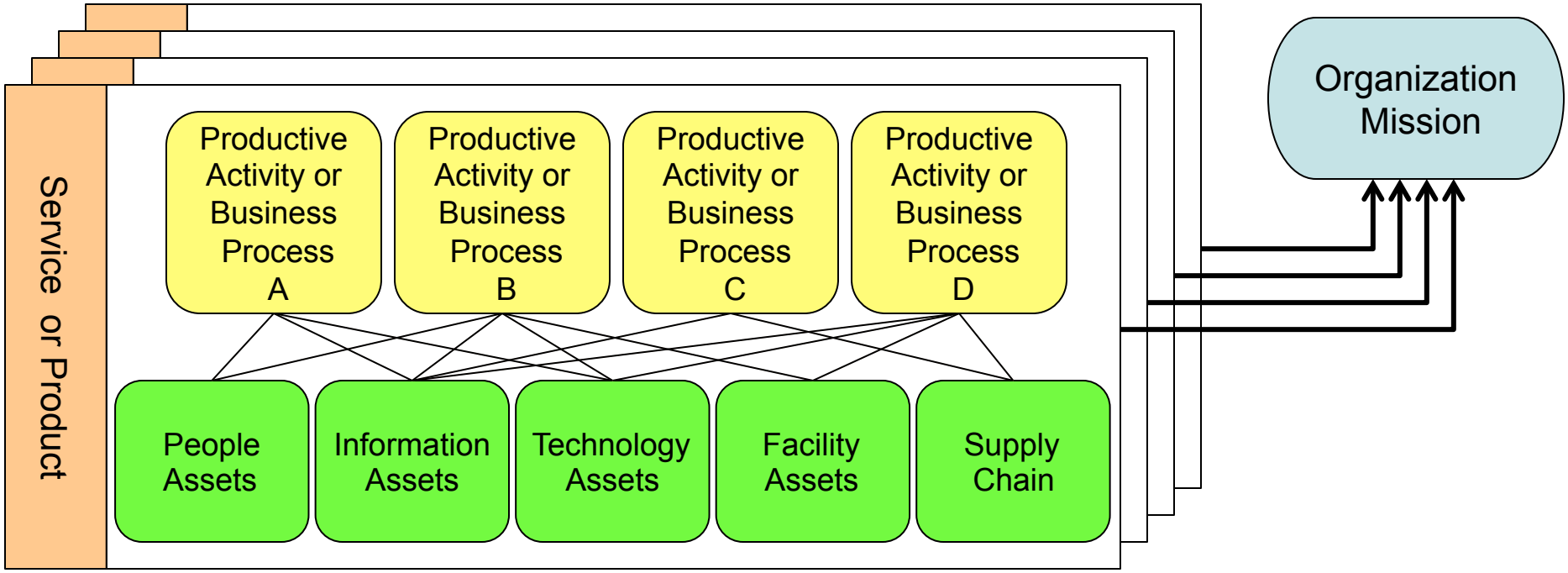
Information

Facilities

Technology

Supply Chain / Raw Material

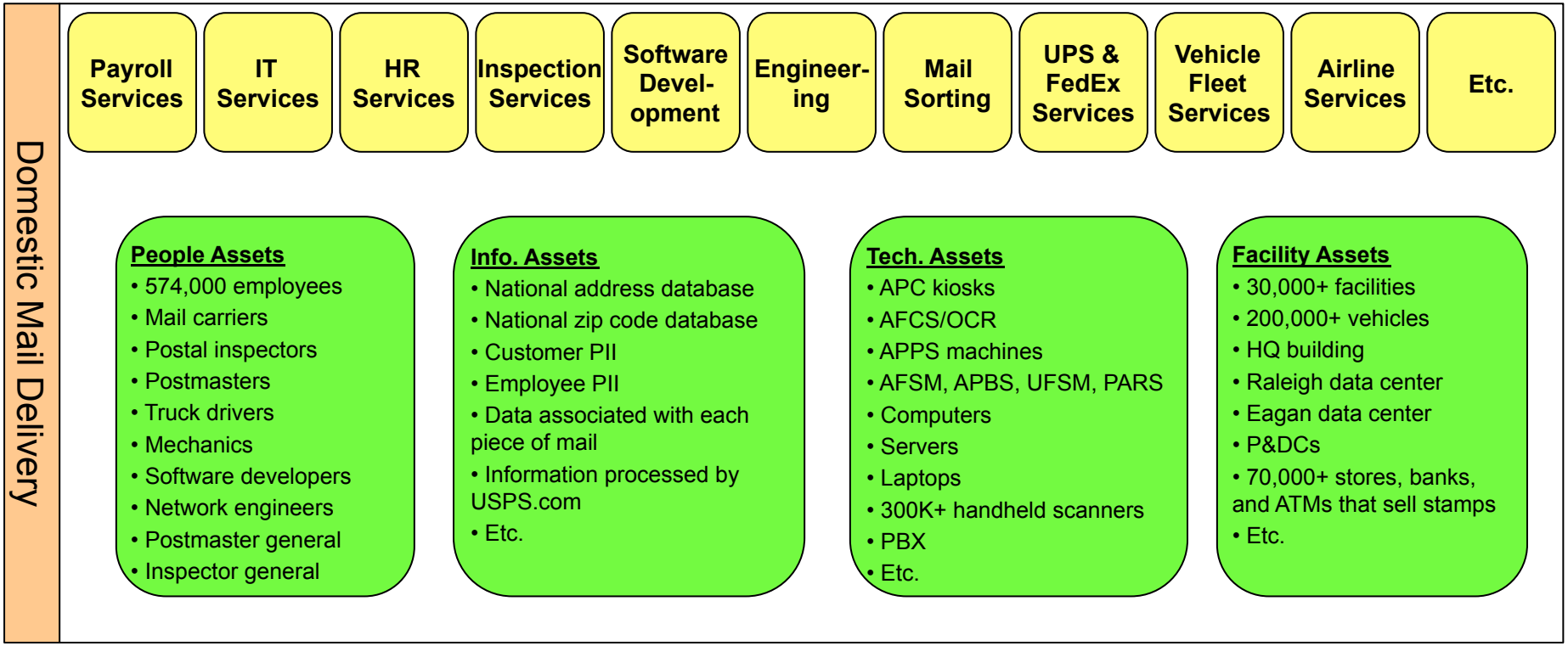
Asset Types



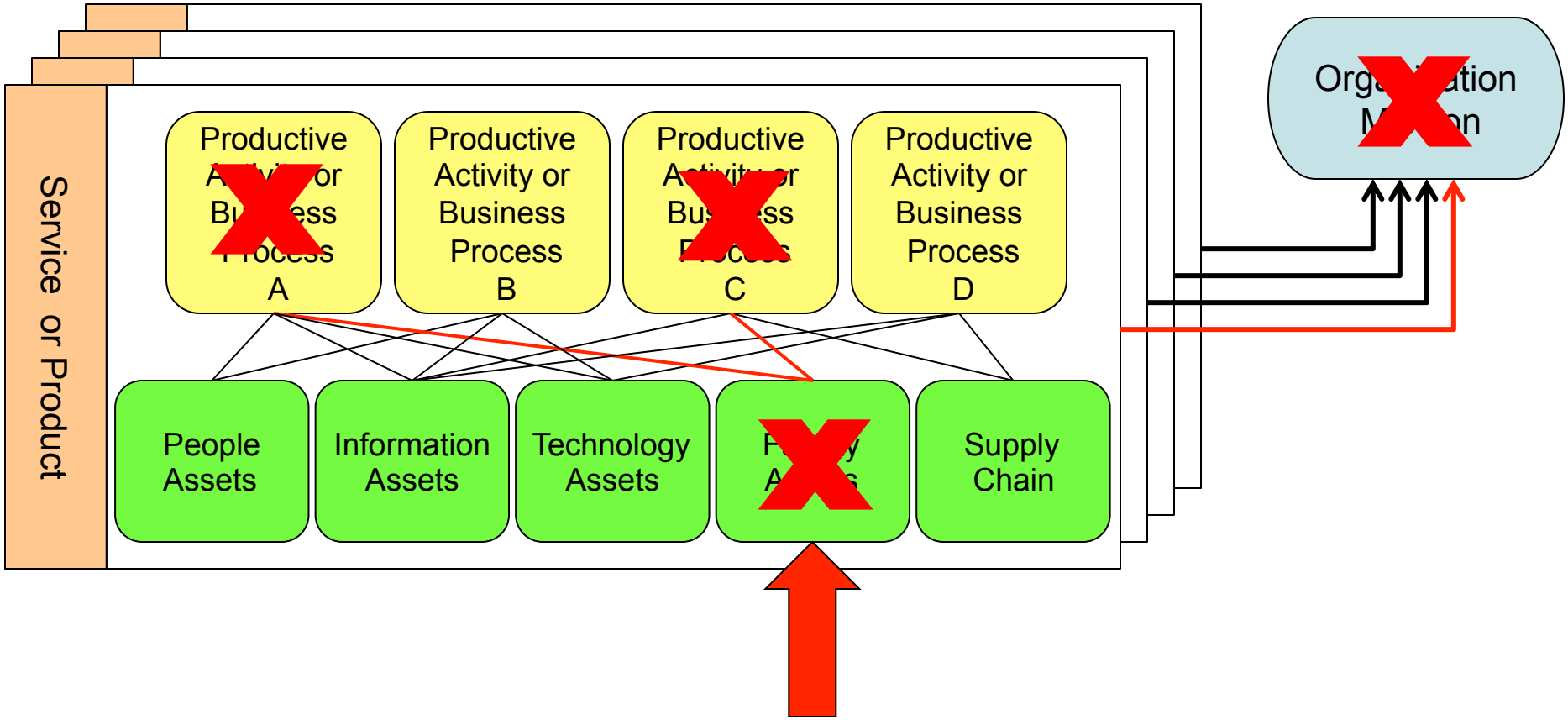
Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.

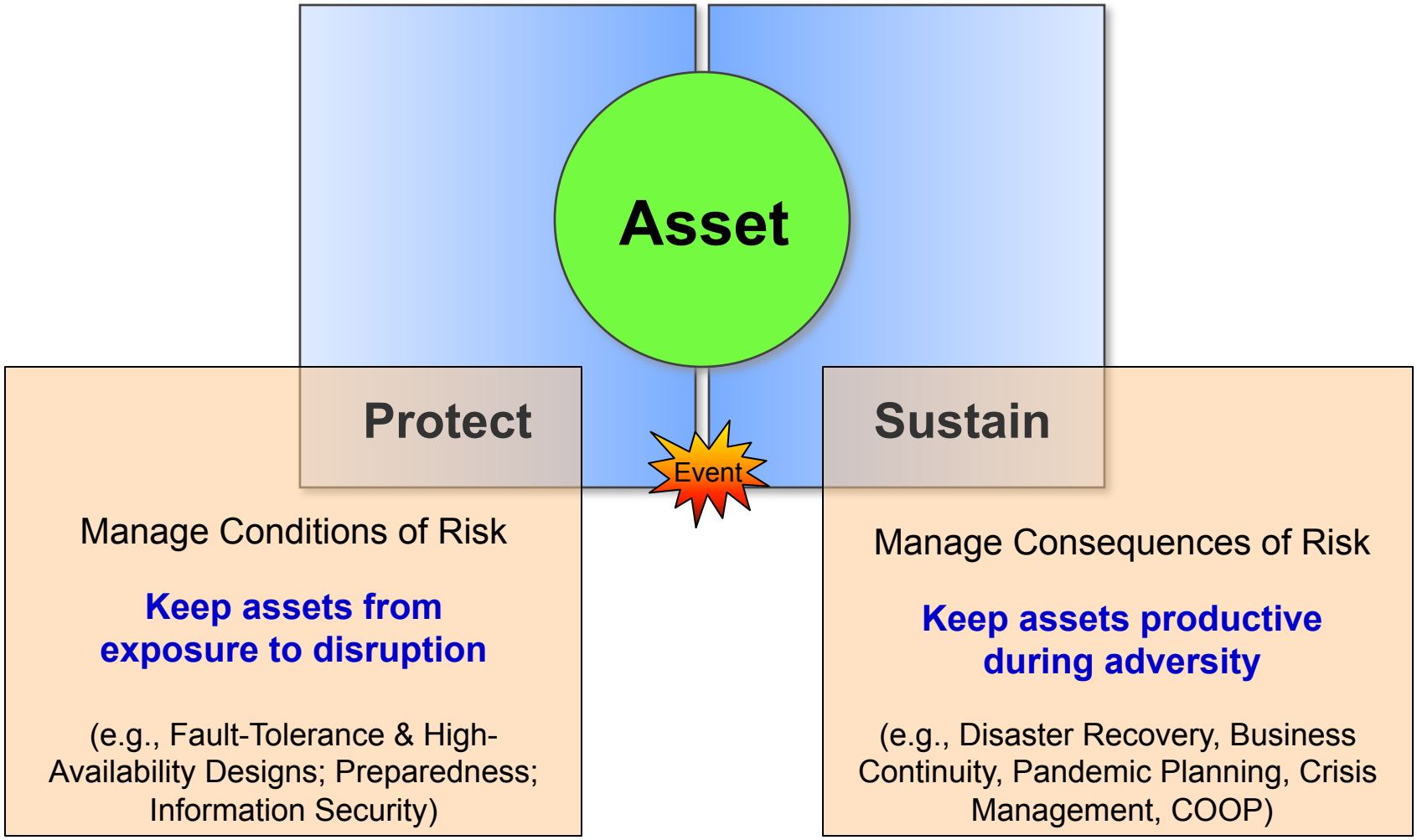
Example: U.S. Postal Service



Operational Resilience Starts at Asset Level



Operational Resilience Starts at Asset Level



Analogy - Protection and Sustainment Strategies

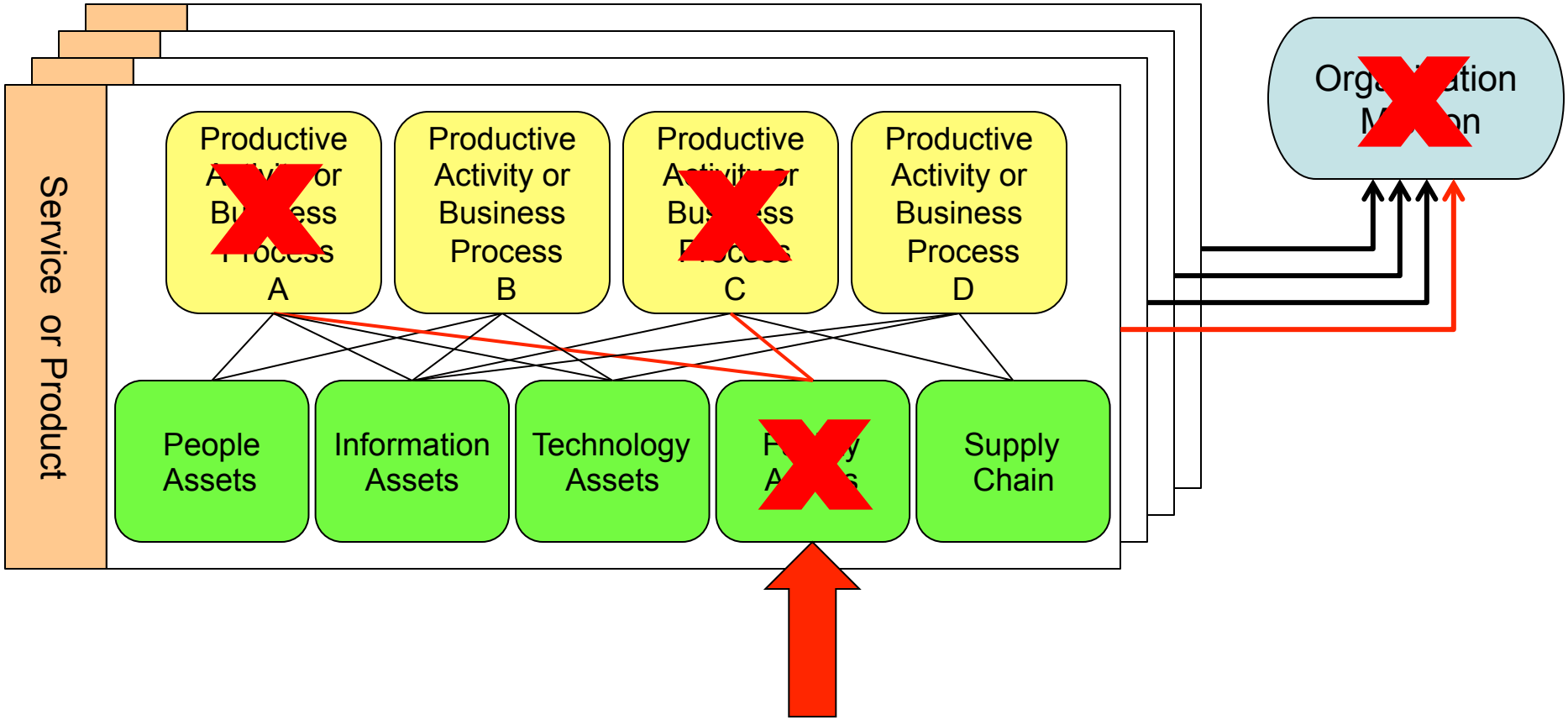
Protection Activities

- Translate into activities designed to keep assets from exposure to disruption
- Example: “security” activities, but may also be embedded in IT operations activities

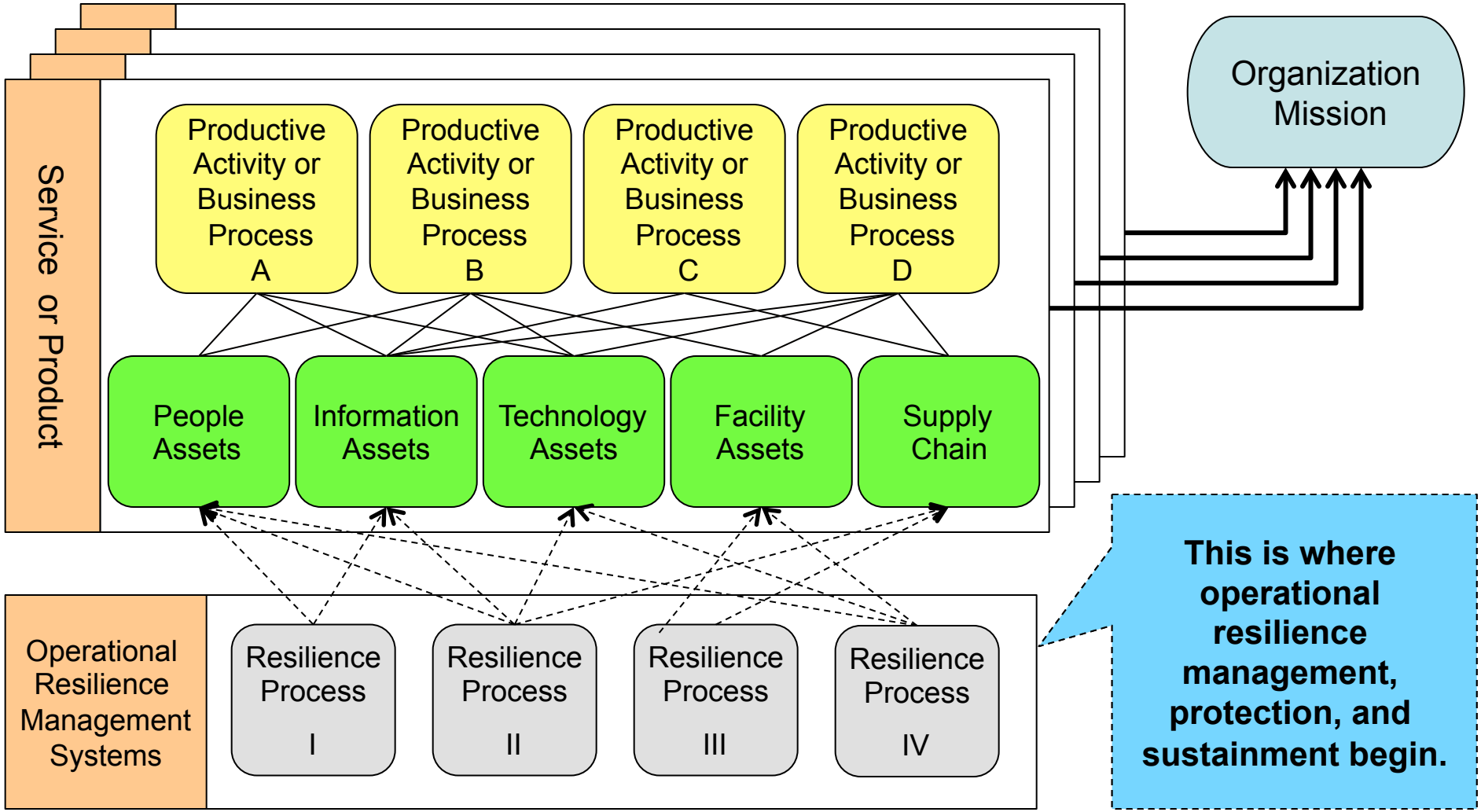
Sustainability Activities

- Translate into activities designed to keep assets productive during adversity
- Example: “business continuity” activities

Asset Disruption

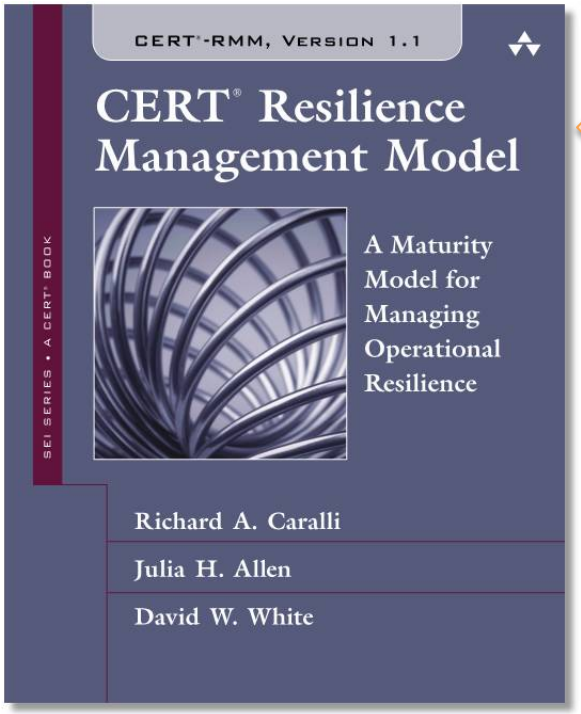


Organizational Context for Resilience Activities



Is there one place that I can go to see what are all the right things that an organization should do in order to improve and manage its operational resilience in a systematic, practical, and proven manner?

CERT Resilience Management Model (CERT-RMM)



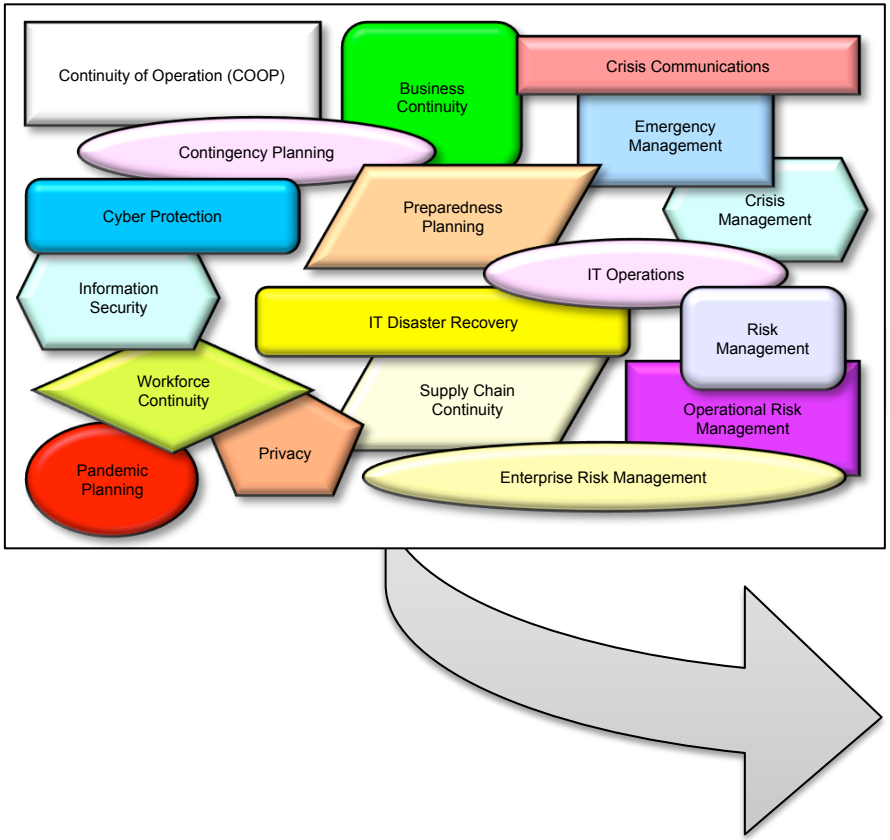
http://www.cert.org/resilience/

Framework for managing and improving operational resilience

"…an extensive super-set of the things an organization could do to be more resilient."

—CERT-RMM adopter

Desired Integrated Approach



Pull for Integrated Cyber Resilience

Research on new approaches to achieving security and resiliency in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements.

CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Federal Computer WEEK

Strategy and business management for government leaders

Updated homeland security strategy emphasizes resilience

Blueprint for a Secure Cyber Future

The C
Home
Novemt

The Blueprint lists four goals for protecting critical information infrastructure:

- Reduce Exposure to Cyber Risk
- Ensure Priority Response and Recovery
- Maintain Shared Situational Awareness
- Increase Resilience

Department of Defense

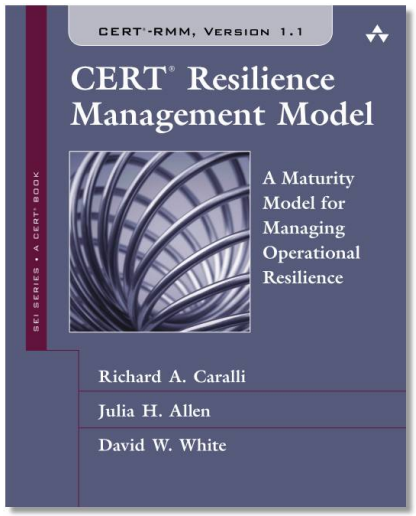
S&T Emphasis Areas

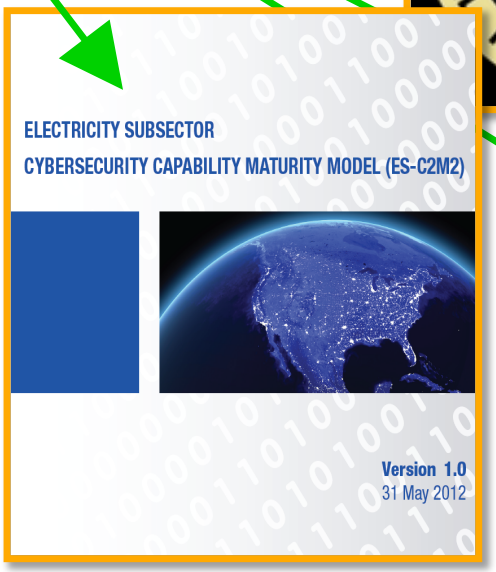
The Department has identified seven priorities:

- Defense Strategic Guidance
- Autonomy
- Counter Weapons of Mass Destruction
- Cyber Sciences
- Data-to-Decisions
- Electronic Warfare
- Engineered Resilient Systems
- Human Systems

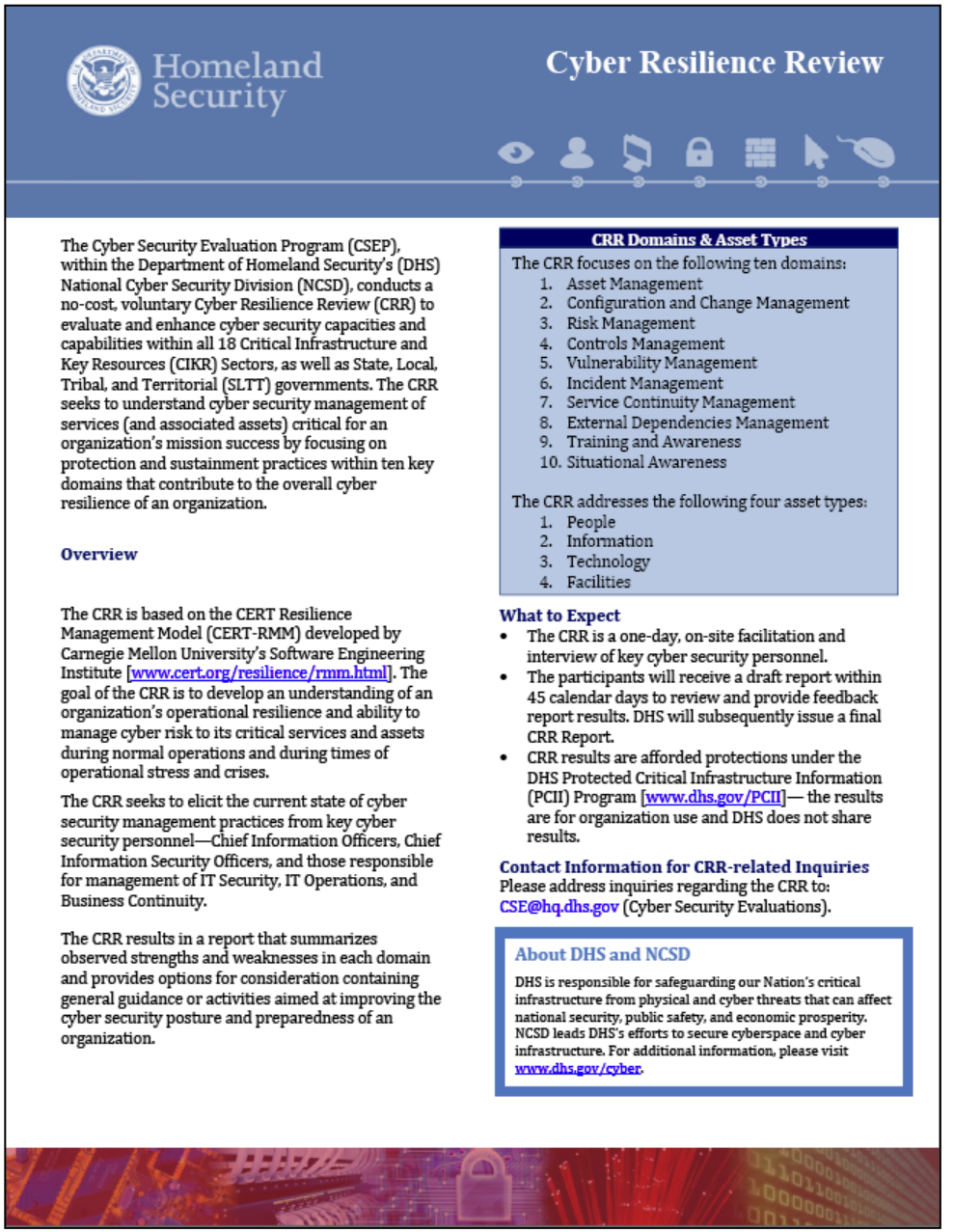
Success Stories

A Sampling of CERT-RMM Applications and Derivatives





Department of Homeland Security



Homeland Security

Cyber Resilience Review

The Cyber Security Evaluation Program (CSEP), within the Department of Homeland Security's (DHS) National Cyber Security Division (NCSD), conducts a no-cost, voluntary Cyber Resilience Review (CRR) to evaluate and enhance cyber security capacities and capabilities within all 18 Critical Infrastructure and Key Resources (CIKR) Sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments. The CRR seeks to understand cyber security management of services (and associated assets) critical for an organization's mission success by focusing on protection and sustainment practices within ten key domains that contribute to the overall cyber resilience of an organization.

Overview

The CRR is based on the CERT Resilience Management Model (CERT-RMM) developed by Carnegie Mellon University's Software Engineering Institute [www.cert.org/resilience/rmm.html]. The goal of the CRR is to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services and assets during normal operations and during times of operational stress and crises.

The CRR seeks to elicit the current state of cyber security management practices from key cyber security personnel—Chief Information Officers, Chief Information Security Officers, and those responsible for management of IT Security, IT Operations, and Business Continuity.

The CRR results in a report that summarizes observed strengths and weaknesses in each domain and provides options for consideration containing general guidance or activities aimed at improving the cyber security posture and preparedness of an organization.

CRR Domains & Asset Types

The CRR focuses on the following ten domains:

1. Asset Management
2. Configuration and Change Management
3. Risk Management
4. Controls Management
5. Vulnerability Management
6. Incident Management
7. Service Continuity Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The CRR addresses the following four asset types:

1. People
2. Information
3. Technology
4. Facilities

What to Expect

- The CRR is a one-day, on-site facilitation and interview of key cyber security personnel.
- The participants will receive a draft report within 45 calendar days to review and provide feedback report results. DHS will subsequently issue a final CRR Report.
- CRR results are afforded protections under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/PCII]— the results are for organization use and DHS does not share results.

Contact Information for CRR-related Inquiries

Please address inquiries regarding the CRR to: CSE@hq.dhs.gov (Cyber Security Evaluations).

About DHS and NCSD

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. NCSD leads DHS's efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber.

ES-C2M2

ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0
31 May 2012

U.S. Postal Inspection Service (USPIS)

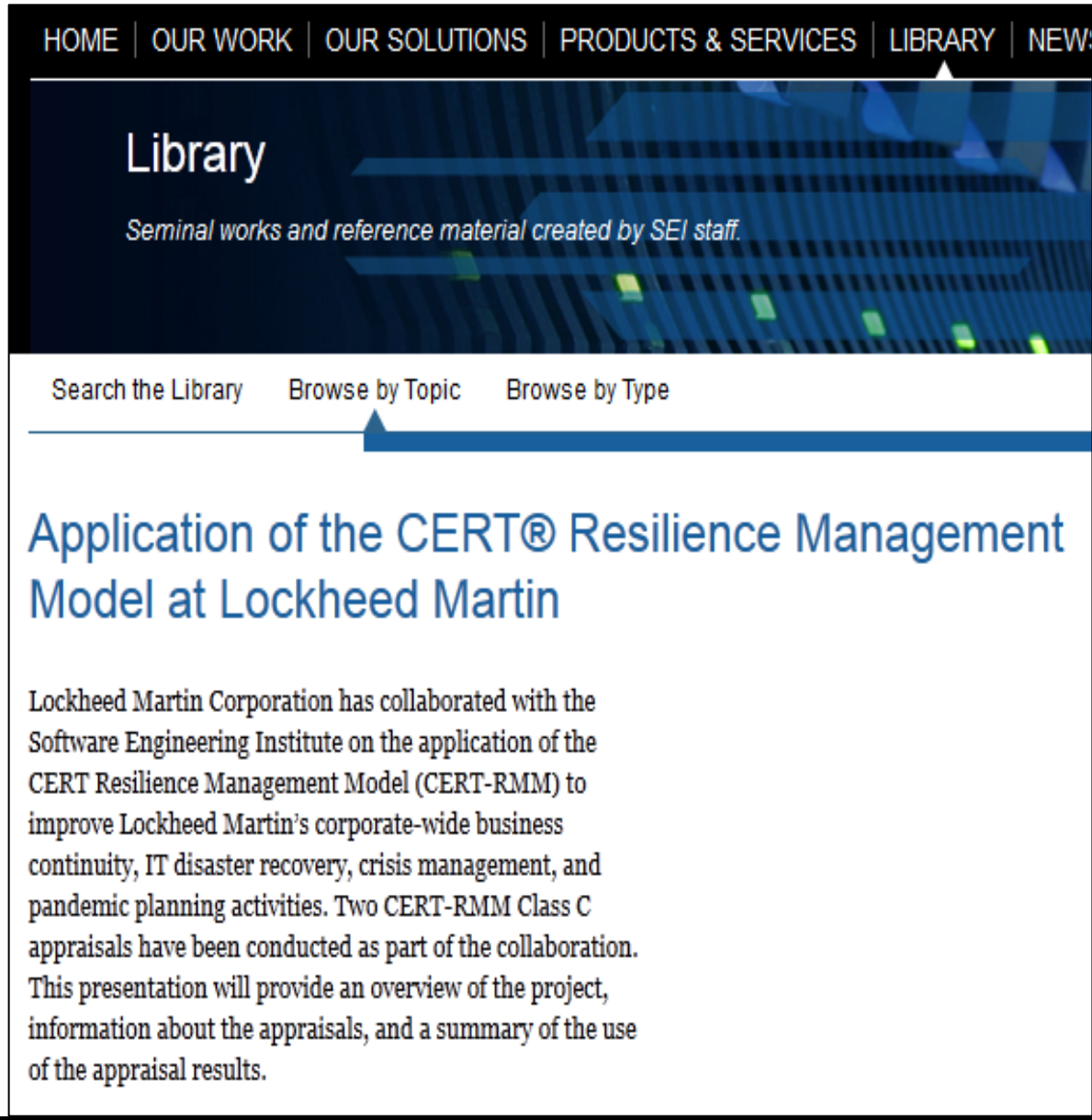
The law enforcement arm of the U.S. Postal Service

The USPIS has used CERT-RMM to address such operational risks as

- export screening
- new product security
- measuring and monitoring risks associated with fraud
- physical security and aviation screening for international mail
- improved processes for investigative response to network security incidents

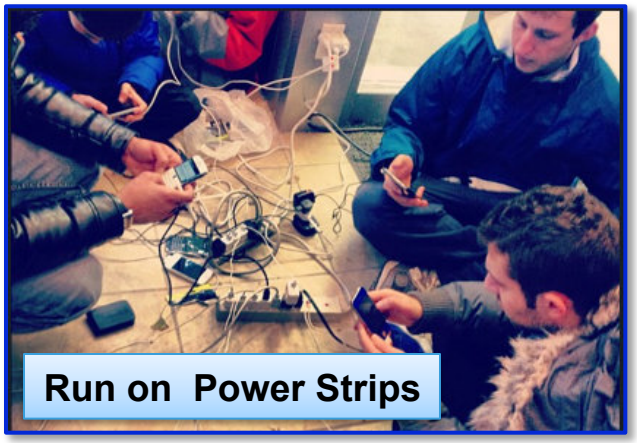
Lockheed Martin

LOCKHEED MARTIN



In Closing

Hurricane Sandy Surprised Us in Many Ways



Most Talked-About Subject Afterward…

Cornell University

CHRONICLE ONLINE

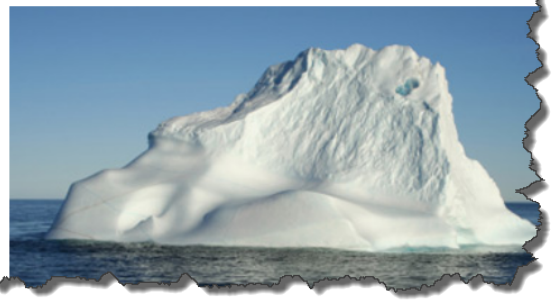
March 4, 2013

Arctic ice loss amplified Superstorm Sandy violence

By Blaine Friedlander

If you believe that last October's Superstorm Sandy was a freak of nature -- the confluence of unusual meteorological, atmospheric and celestial events -- think again.

Cornell and Rutgers researchers report in the



Bloomberg Businessweek
Politics & Policy

Like 113k

Global Economics | Companies & Industries | Politics & Policy | Technology | Markets & Finance | Innovation & Design | Life

It's Global Warming, Stupid

By Paul M. Barrett on November 01, 2012 | 1282 Comments

Yes, yes, it's unsophisticated to blame any given storm on climate change. Men and women in white lab coats tell us—and they're right—that many factors contribute to each severe weather episode. Climate deniers exploit scientific

CLIMATEPROGRESS

Like

How Does Climate Change Make Superstorms Like Sandy More Destructive?

By Joe Romm on Oct 31, 2012 at 5:03 pm

The New York Times
Tuesday, March 19, 2013

Environment

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SP

A Blog About Energy and the Environment

SCIENCE | October 30, 2012, 5:46 pm | 178 Comments

Did Global Warming Contribute to Hurricane Sandy's Devastation?

By JUSTIN GILLIS

Hurricane Sandy Damage Partly Caused By Climate Change, Scientists Say

Posted: 11/06/2012 10:06 am EST Updated: 11/06/2012 10:06 am EST

Most Talked-About Subject Afterward…

Cornell University

CHRONICLEONLINE

March 4, 2013

Arctic ice loss amplified Superstorm Sand

By Blaine Friedlander

If you believe that last October's Superstorm Sandy was a freak of nature -- the confluence of unusual meteorological, atmospheric and celestial events -- think again.

Cornell and Rutgers researchers report in the

Bloomberg Businessweek

Politics & Policy

Like 113k

Global Economics | Companies & Industries | Politics & Policy | Technology | Markets & Finance | Innovation & Design | Lifes

It's Global Warming, Stupid

on November 01, 2012 | 1282 Comments

Yes, yes, it's unsophisticated to blame any given storm on te change. Men and women in white lab coats tell ey're right—that many factors contribute to each episode. Climate deniers exploit scientific

Is this the most important question to ask?

ress

Like

e Superstorms Like Sandy More

The New York Times

Tuesday, March 19, 2013

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH

A Blog About Energy and the Environment

SCIENCE | October 30, 2012, 5:46 pm | 178 Comments

Did Global Warming Contribute to Hurricane Sandy's Devastation?

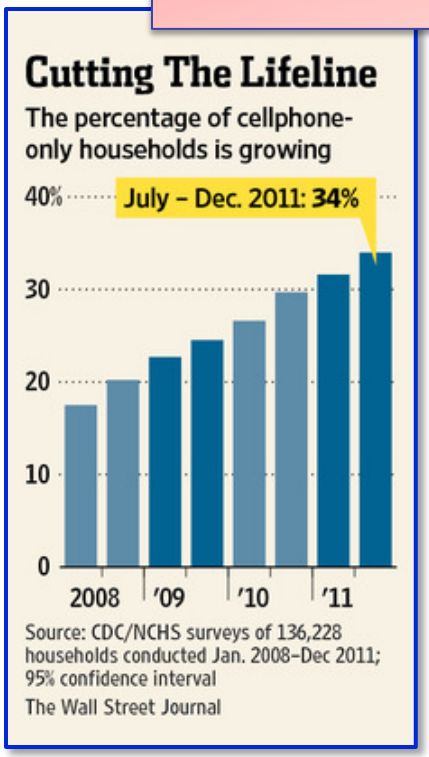
By JUSTIN GILLIS

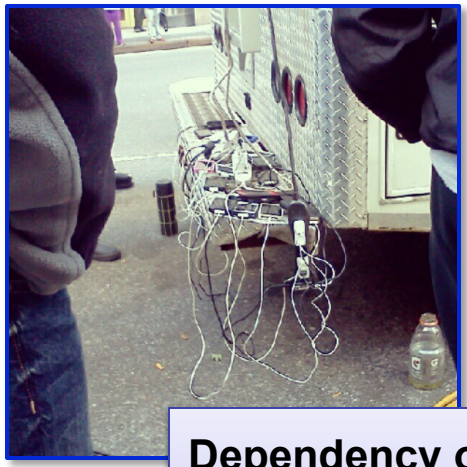
Hurricane Sandy Damage Partly Caused By Climate Change, Scientists Say

Posted: 11/06/2012 10:06 am EST Updated: 11/06/2012 10:06 am EST

A better question to ask: *How has the national risk environment changed?*

Movement from traditional wireline telephony to cell phones and broadband cable telephony





Dependency on large number of mobile devices needing frequent recharging

"… As of 2003, 153 million Americans lived in coastal counties – an increase of 33 million since 1980 – and 3.7 million lived within a few feet of high tide…"

—Bryan Walsh, Time Magazine, November 12, 2012

… and there are many more.

Expansion of National Risk Environment

- Globalization
- Operational complexity
- Pervasive use of technology
- Intertwining of cyber and physical domains
- Increased role of cybersecurity in securing physical assets
- Movement toward intangible assets
- Global economic pressures
- Regulatory and legal boundaries
- Geo-political pressures

Successful management of operational risk may require a (significant) shift in thinking and approach.

Protecting the enterprise remains a complex and multifaceted challenge.

Disruptive events, through which risks are realized, will continue to surprise us.

Traditional tools, techniques, and methods may not work as well in this environment.

How should an enterprise deal with (and plan for) such surprises?

How should an enterprise operate in such an environment?

Promising Approaches

Next generation of integrated cyber-resilience management frameworks?

MODELS

Resilience Engineering – A new engineering discipline?

EDUCATION

RISK MGMT

Re-shaping (not fighting with) the risk landscape?

Should organizations be legally allowed to fight back when under cyber attack?

POLICY

Mechanisms to compose resilient systems from brittle components?

TECHNOLOGY

"The oak fought the wind and was broken,
the willow bent when it must and survived."

Robert Jordan, The Fires of Heaven

Thank you for your attention…

SEI Training

Introduction to the CERT Resilience Management Model

February 18 - 20, 2014 (SEI, Arlington, VA)

June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document