

Managing Cybersecurity Risk Through Operational Resilience: Lessons from the Department of Defense

Katie Stewart

kcstewart@cert.org

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0327

CERT defines Operational Resilience as:

The emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its operational limit.

Iran-U.S. RQ-170 incident has defense industry saying 'never again' to unmanned vehicle hacking

May 3, 2016
By John Keller
Editor

THE MIL & AERO COMMENTARY, 3 May 2016. If there's anything that continues to haunt U.S. military unmanned vehicle development, it's the December 2011 Iran-U.S. RQ-170 incident in which Iranian military cyber warfare experts commandeered a U.S. Lockheed Martin RQ-170 Sentinel stealth drone operating near the Iranian city of city of Kashmar.

U.S. military authorities initially denied that the stealth had war

THE WALL STREET JOURNAL.

U.S. Edition | March 21, 2019 | Print Edition | Video

Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts

Hacking threatens U.S.'s standing as world's leading military power, study says

By Gordon Lubold and Dustin Volz
March 12, 2019 2:32 p.m. ET

WASHINGTON—The Navy and its industry partners are "under cyber siege" by Chinese hackers and others who have stolen national security critical weaknesses that threaten the U.S.'s standing as a global superpower, an internal Navy review concluded.

The New York Times

Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say



Carnegie Mellon University
Software Engineering Institute

China proudly debuts its new stealth jet it built 'by hacking into US computers and stealing plans'

- Two of the stealth planes carried out a flyby demonstration at an air show
- Analysts said the brief and cautious J-20 routine answered few questions
- Previous reports claimed the design was similar to US fighter planes
- Earlier this year Chinese national, Su Bin, 51, was sent to prison for his part in the 2013 and F-22 fighter jets

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

CYBER TRAINING OBVIOUSLY WORKING—

Year-old router bug exploited to steal sensitive DOD drone, tank documents

Hacker who offered Air Force, Army docs claimed to have exploited known Netgear FTP flaw.

SEAN GALLAGHER - 7/11/2018, 6:18 PM



NEWS

U.S. Navy considers possibility of cyber attack after another ship collision

U.S. Navy officials have gone on record to say hacking will be looked at as a possibility as the cause of the USS John S. McCain collision.



China's newest warplane, the J-20 stealth fighter, made its first public flight at an airshow in the southern city of Zhuhai. It bears an uncanny resemblance to US military's F-22 Raptor



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

With Cyber Risk, Who Is The Enemy?



Third Party Risk:

- 57% of companies believe they do not have adequate visibility into their subcontractors, and 21% are unsure.
- Within the FS industry, 81% believe they do not have adequate visibility.

(Deloitte Extended Enterprise Risk Management Survey 2018)

But what about...



Insider Threat:

- 25% of cyber attacks are originated by an insider, and 36% of those are unintentional/accidental
- 95% of organizations provide security awareness training to their employees at least once per year
- 55% of security decision-makers reported that their C-level executives were in most need of awareness training

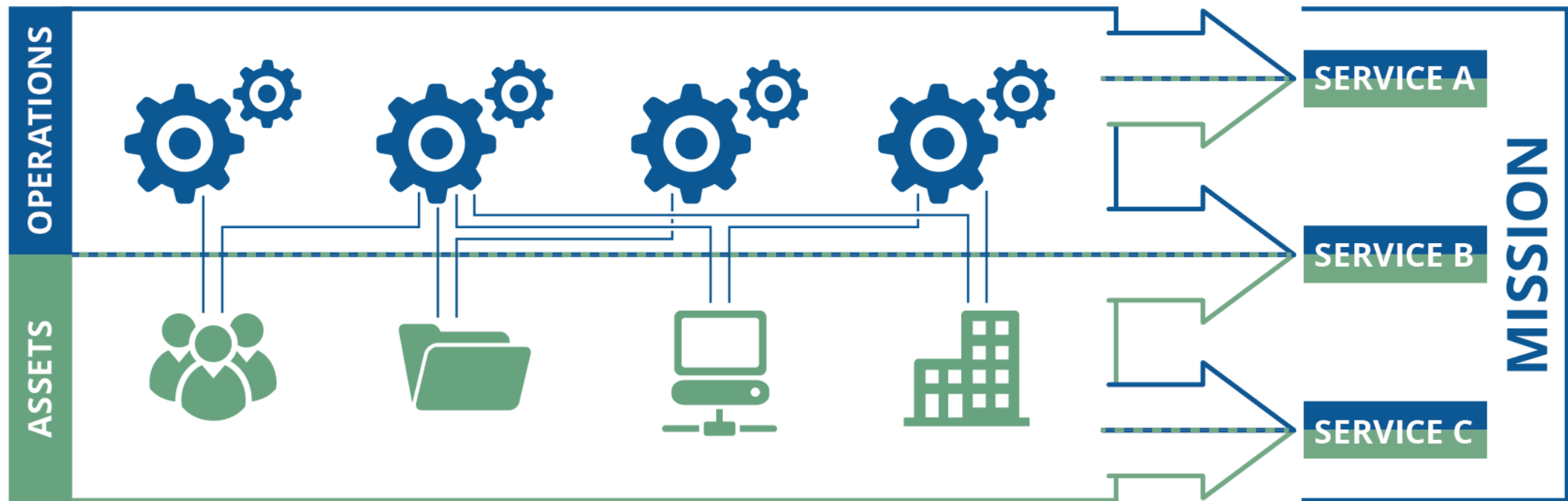
(2018 State of Cybercrime Survey, CERT and CSO)

In Texas, Nigerian awaits trial for 'extremely sophisticated' email fraud scheme

By **Dylan Baddour** Published 11:40 am CST, Monday, January 4, 2016



<https://www.chron.com/news/houston-texas/texas/article/In-Texas-Nigerian-awaits-trial-for-extremely-6735414.php#photo-9199759>



US Telco Fined \$3 Million in Domain Renewal Blunder

By [Catalin Cimpanu](#)

October 2, 2017 10:50 AM 0

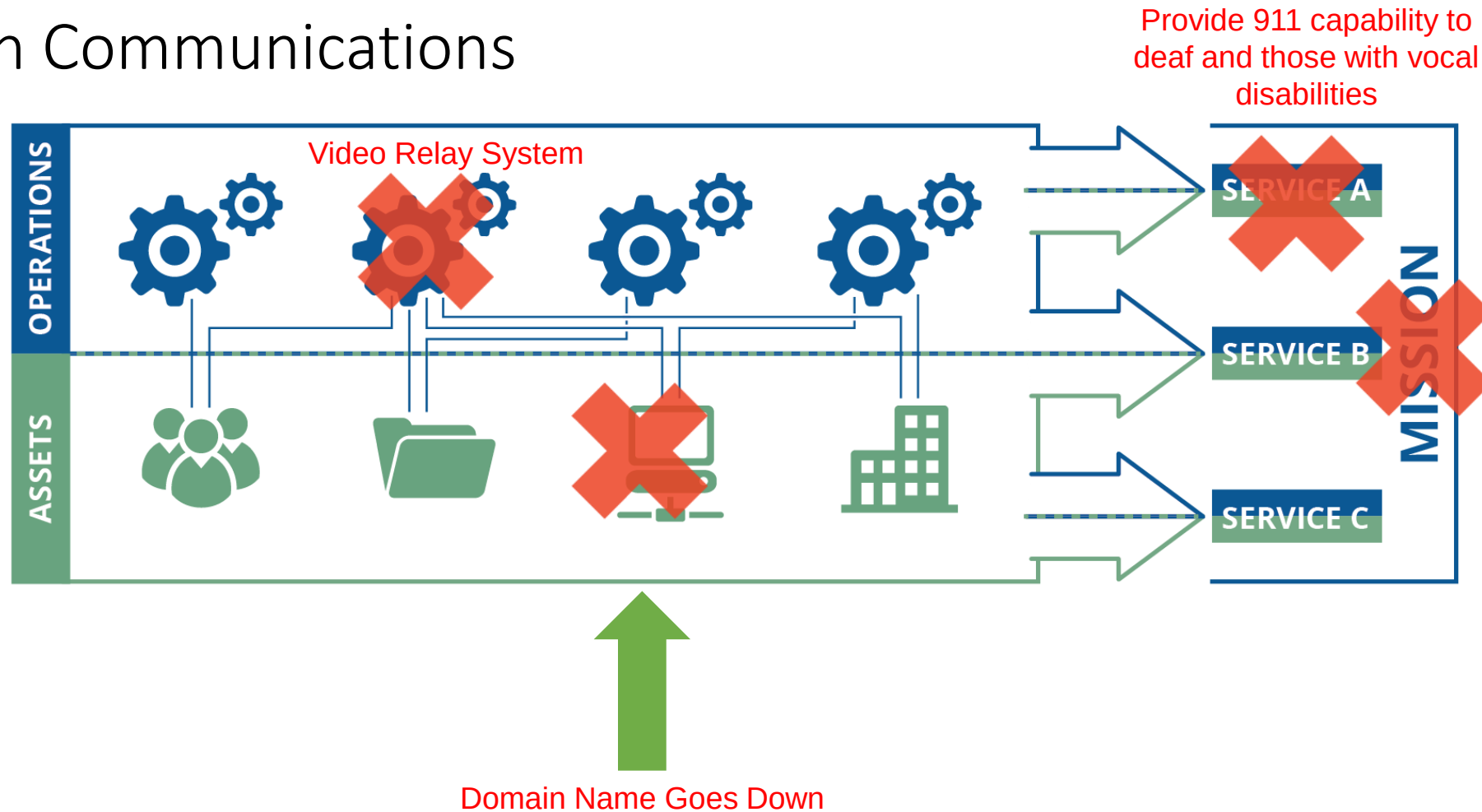


Sorenson Communications, a Utah-based telecommunications provider, received a whopping \$3 million fine from the Federal Communications Commission (FCC) on Friday for failing to renew a crucial domain name used by a part of the local 911 emergency service.

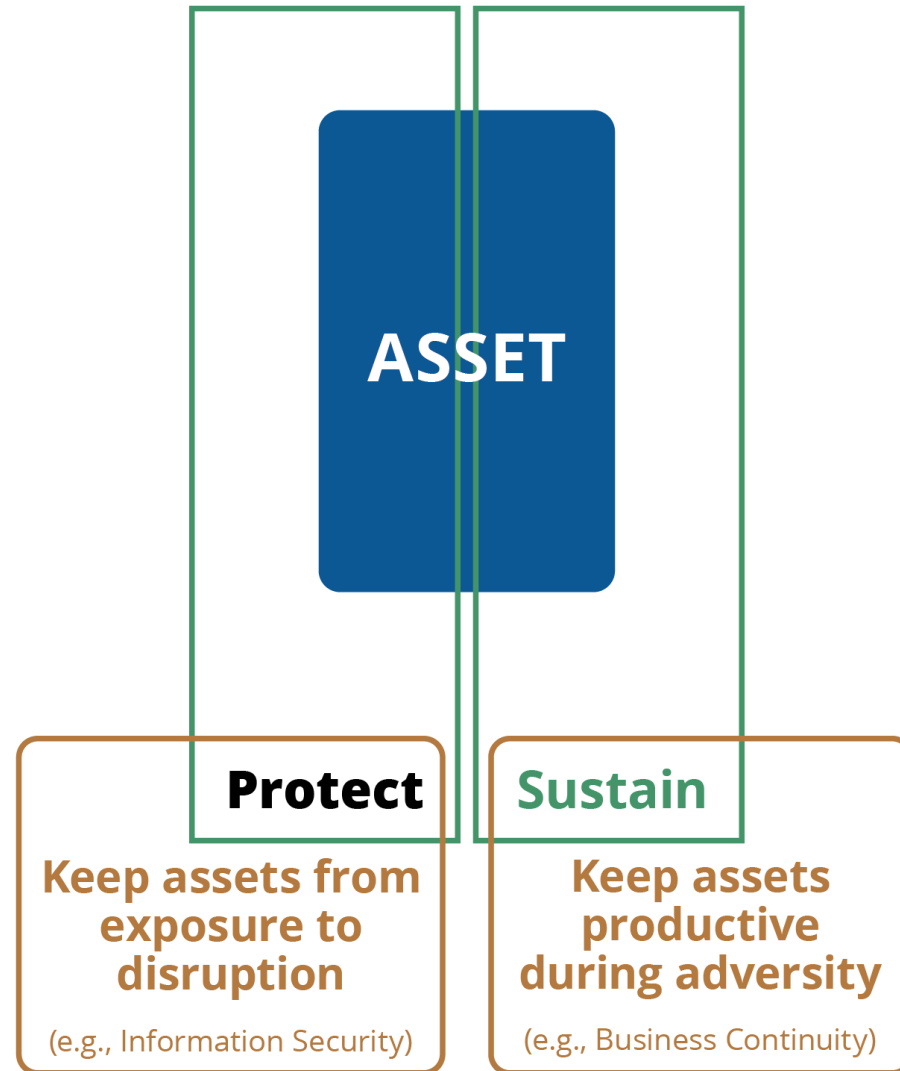
The affected service was the Video Relay System (VRS), a video calling service that telecommunication firms must provide to deaf people and others people with vocal disabilities so they can make video calls to 911 services and use sign language to notify operators of an emergency or crime.

<https://www.bleepingcomputer.com/news/technology/us-telco-fined-3-million-in-domain-renewal-blunder/>

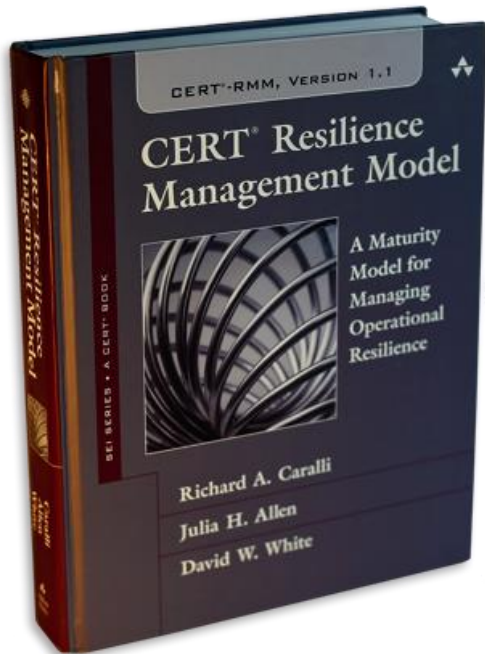
Sorenson Communications



Operational Resilience Starts at the Asset Level



CERT Resilience Management Model



Engineering

ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management

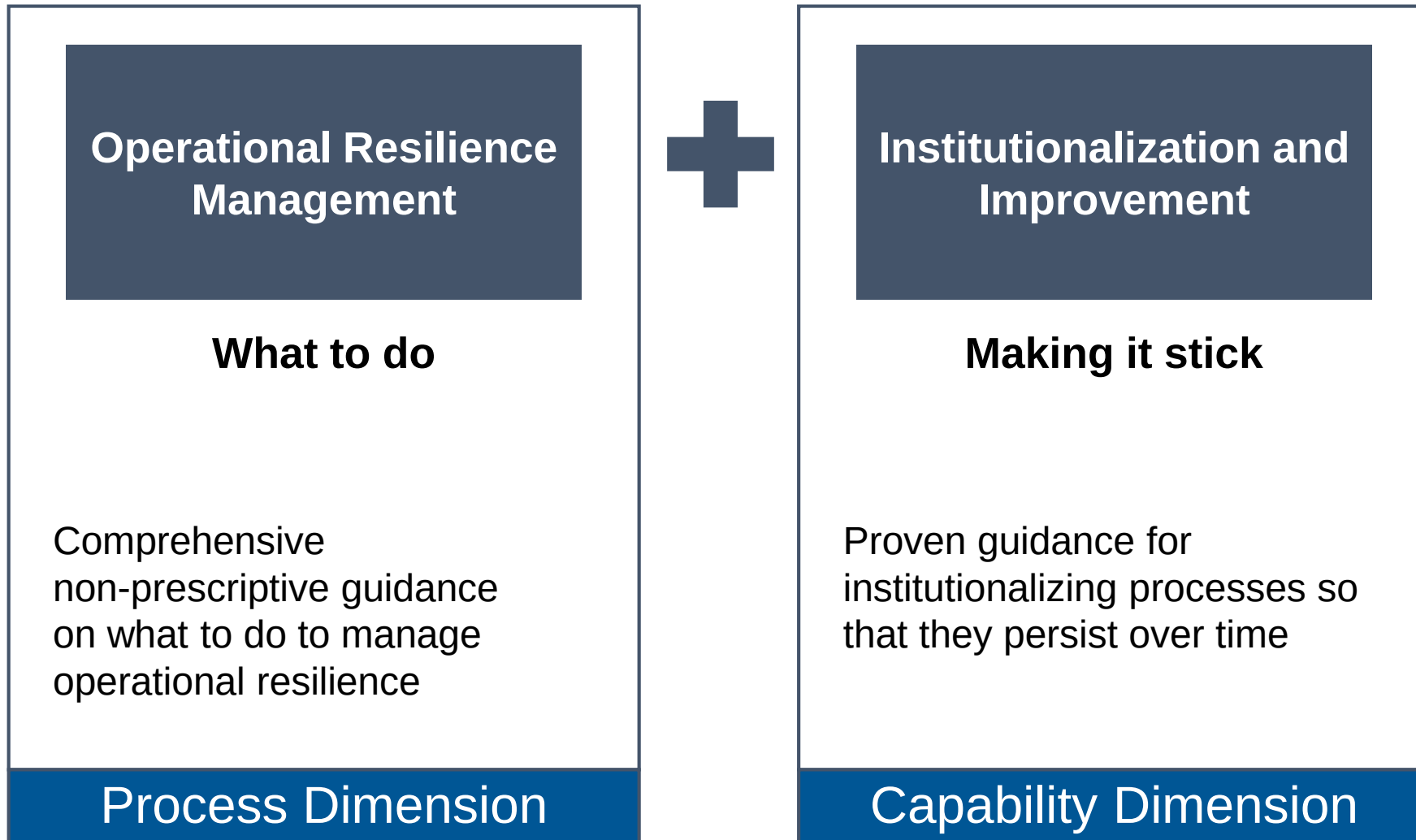
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

Operations

AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management

MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus



Want to know more?

- www.cert.org
- Research Areas Include:
 - Cyber Intelligence
 - Digital Forensics
 - Enterprise Risk Management
 - Insider Threat
 - Measurement and Analysis
 - Network Situational Awareness
 - Secure Development
 - System and Platform Evaluation