CISQ Cyber Resilience Summit

Risk Management Standards in Practice

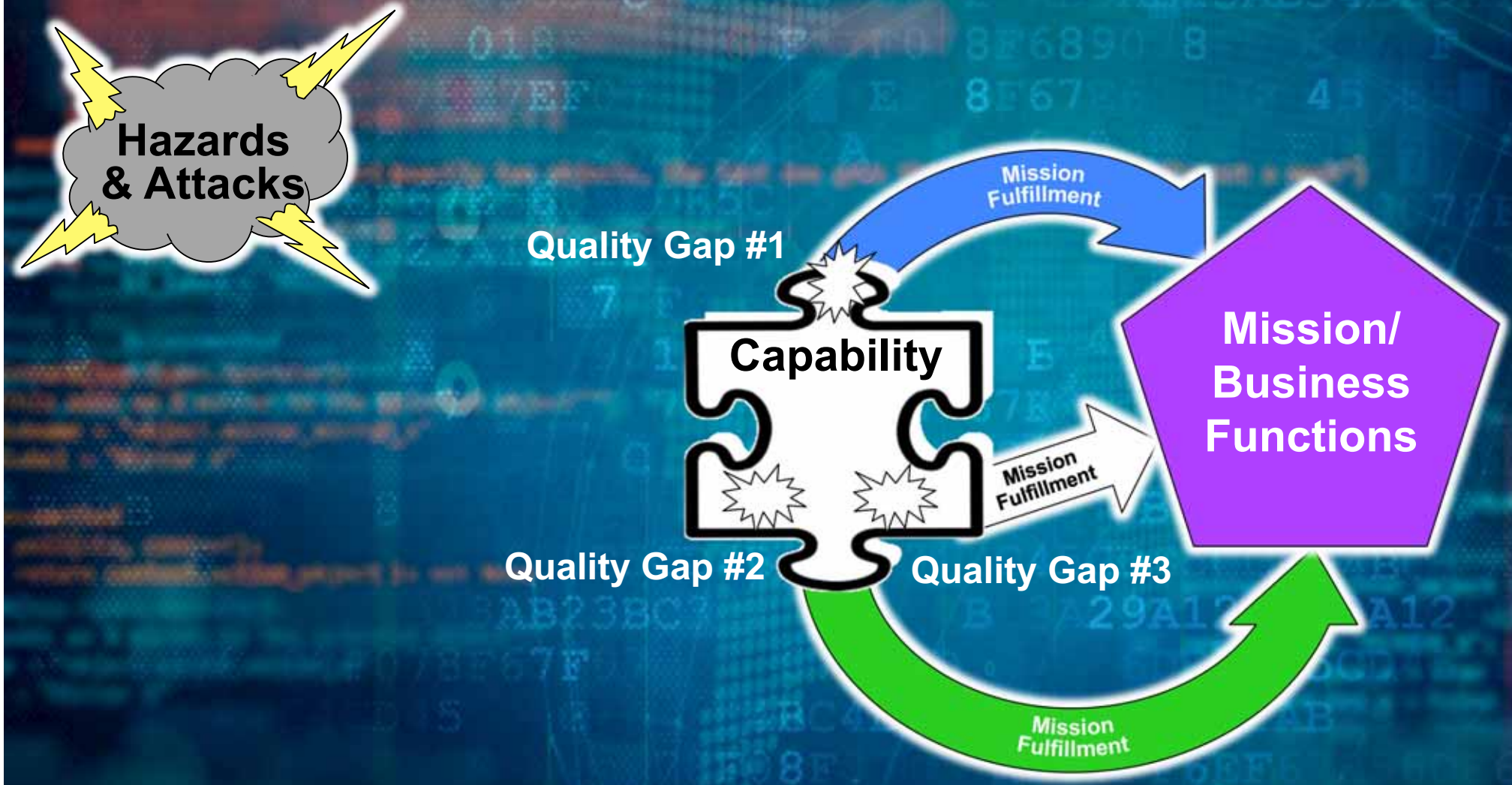
Robert A. Martin
20 March 2018

MITRE

MITRE

MITRE

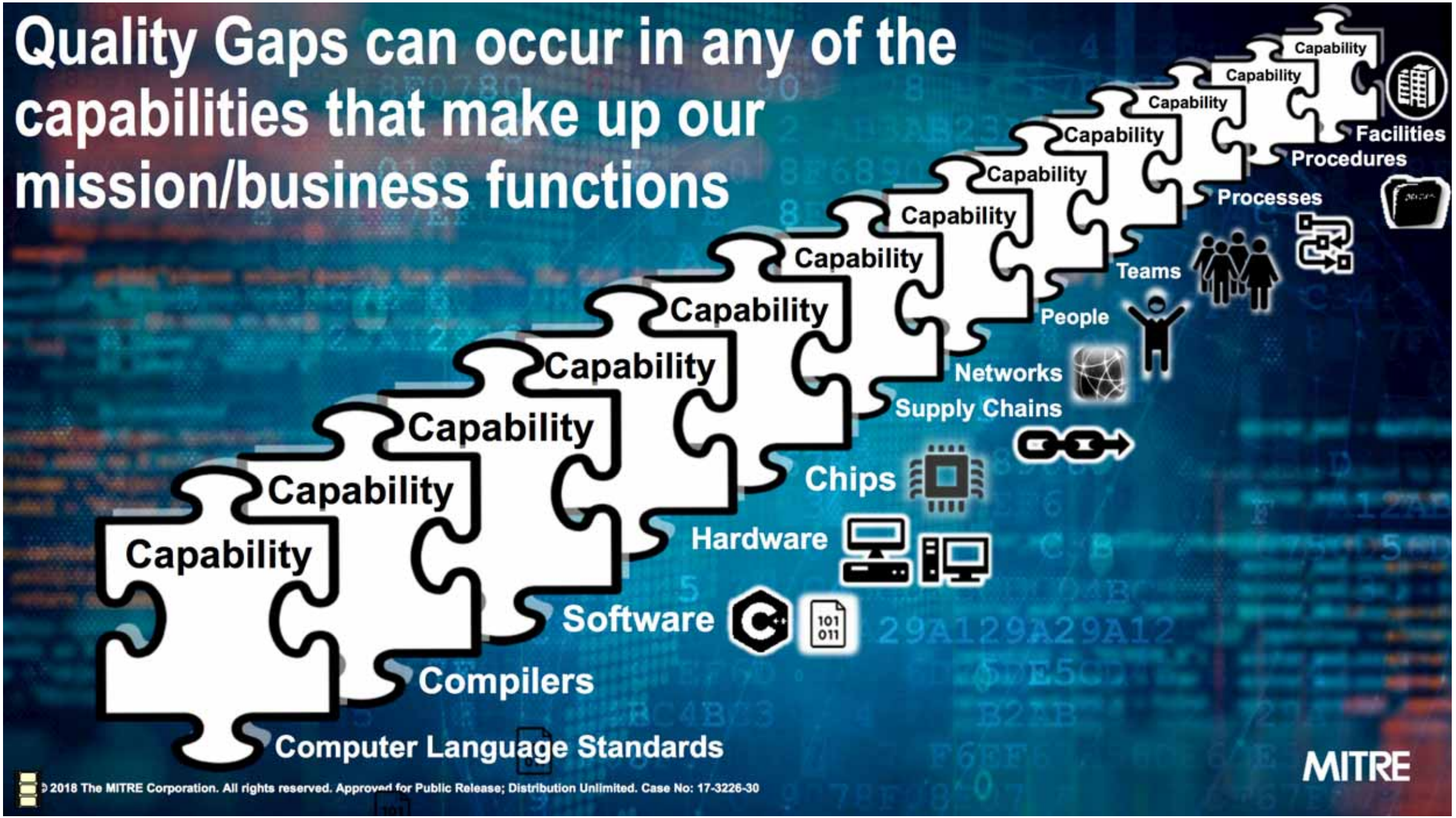
One element of Risk Management is Identifying Quality Gaps in Capabilities Critical to Mission/Business Functions



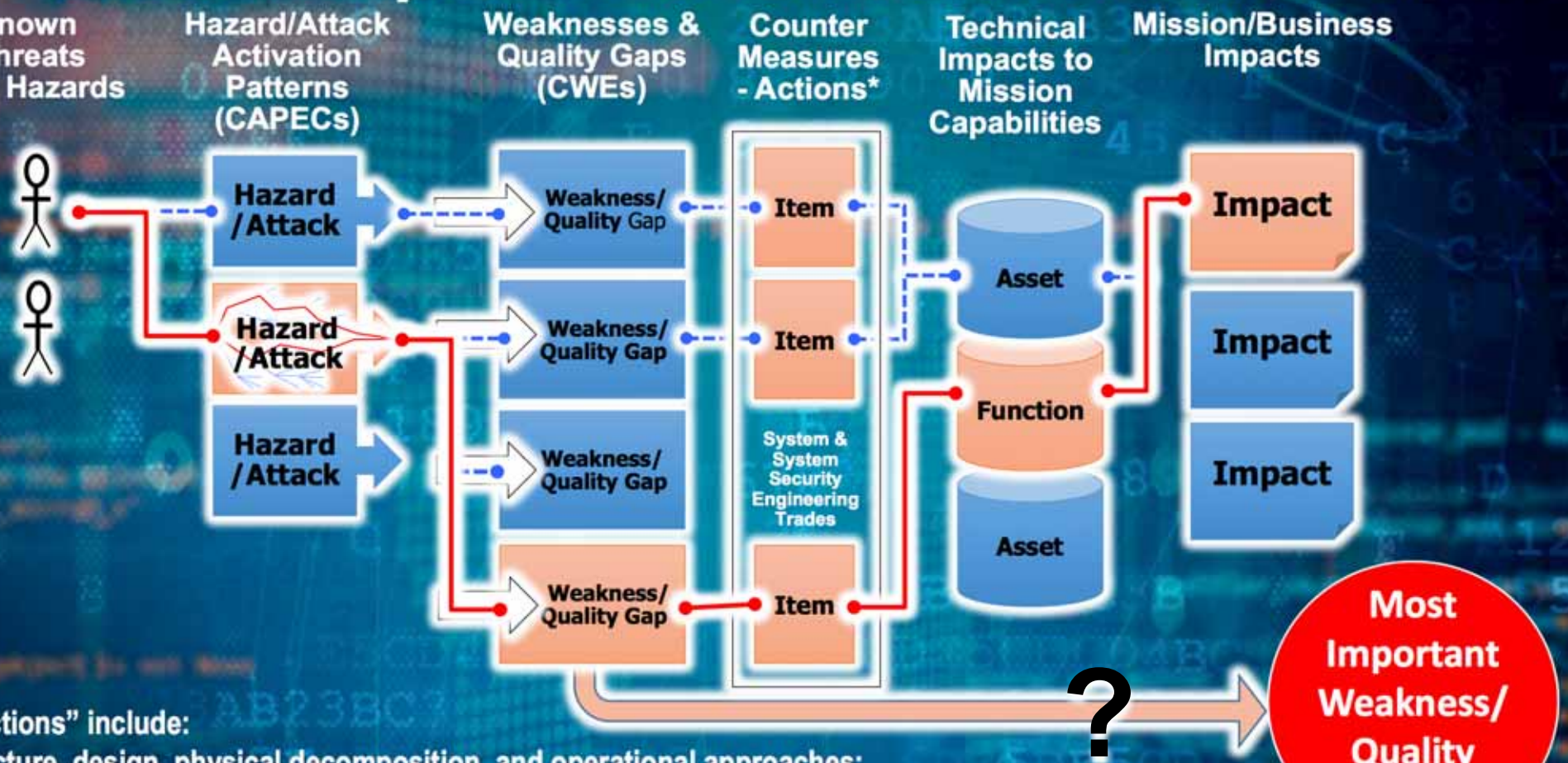
MITRE

One element of Risk Management is Identifying Quality Gaps in Capabilities Critical to Mission/Business Functions

MITRE


Quality Gaps can occur in any of the capabilities that make up our mission/business functions
Capability
Capability
Capability
Capability
Capability
Capability
Capability
Capability
Capability
Capability
Capability
Facilities
Procedures
Processes
Teams
People
Networks
Supply Chains
Chips
Hardware
Software
Compilers
Computer Language Standards
MITRE
© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 17-3226-30

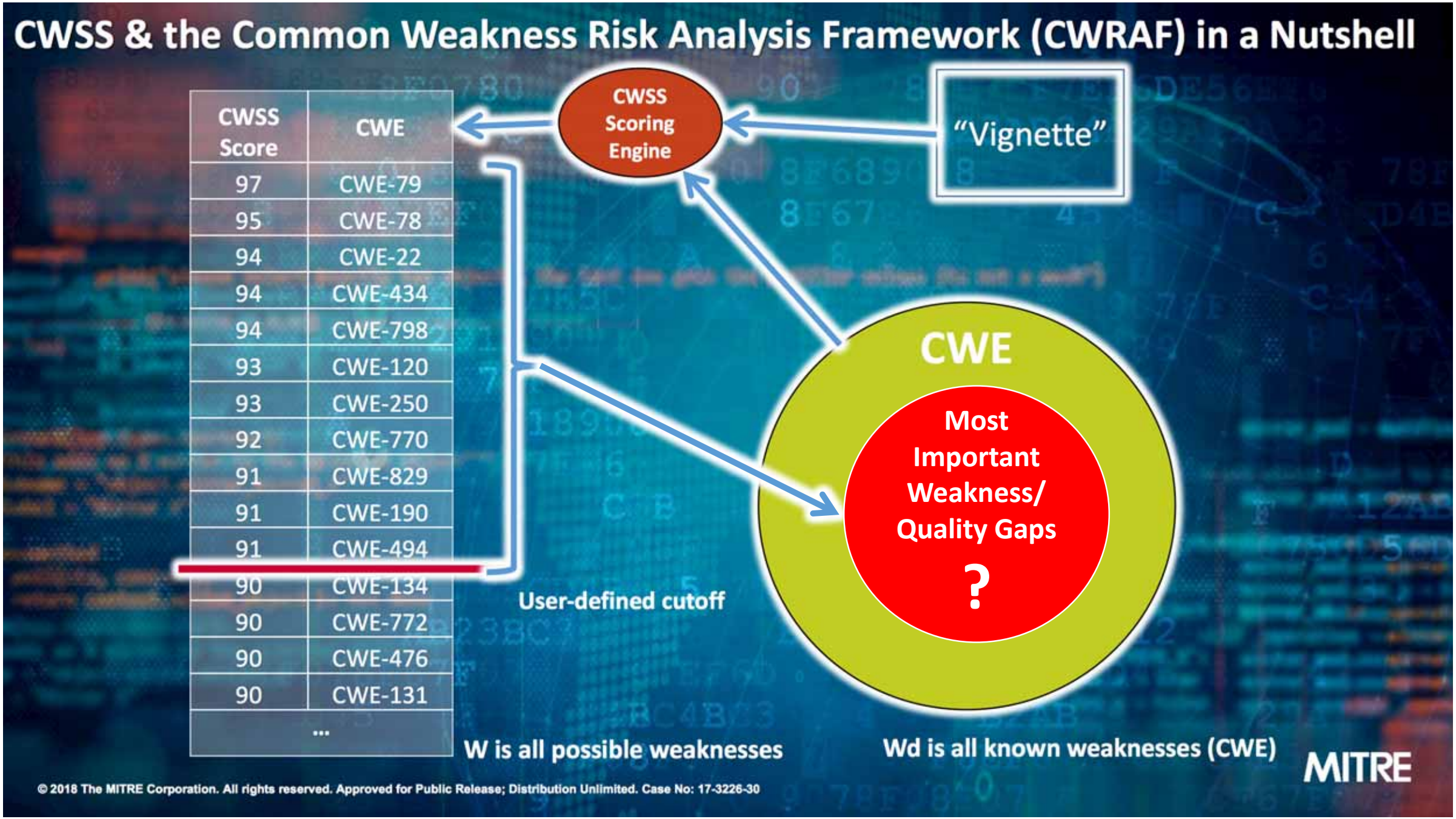
Risk Management is about addressing the Hazards & Attacks that can impact Mission/Business Functions



"Counter Measures - Actions" include:
choices about architecture, design, physical decomposition, and operational approaches;
adding/changing security/safety functions, protection schemes, activities & processes;
use of static & dynamic code assessments, dynamic testing, physical testing, and pen testing;
attack surface & fault-tree analysis, architecture and design reviews

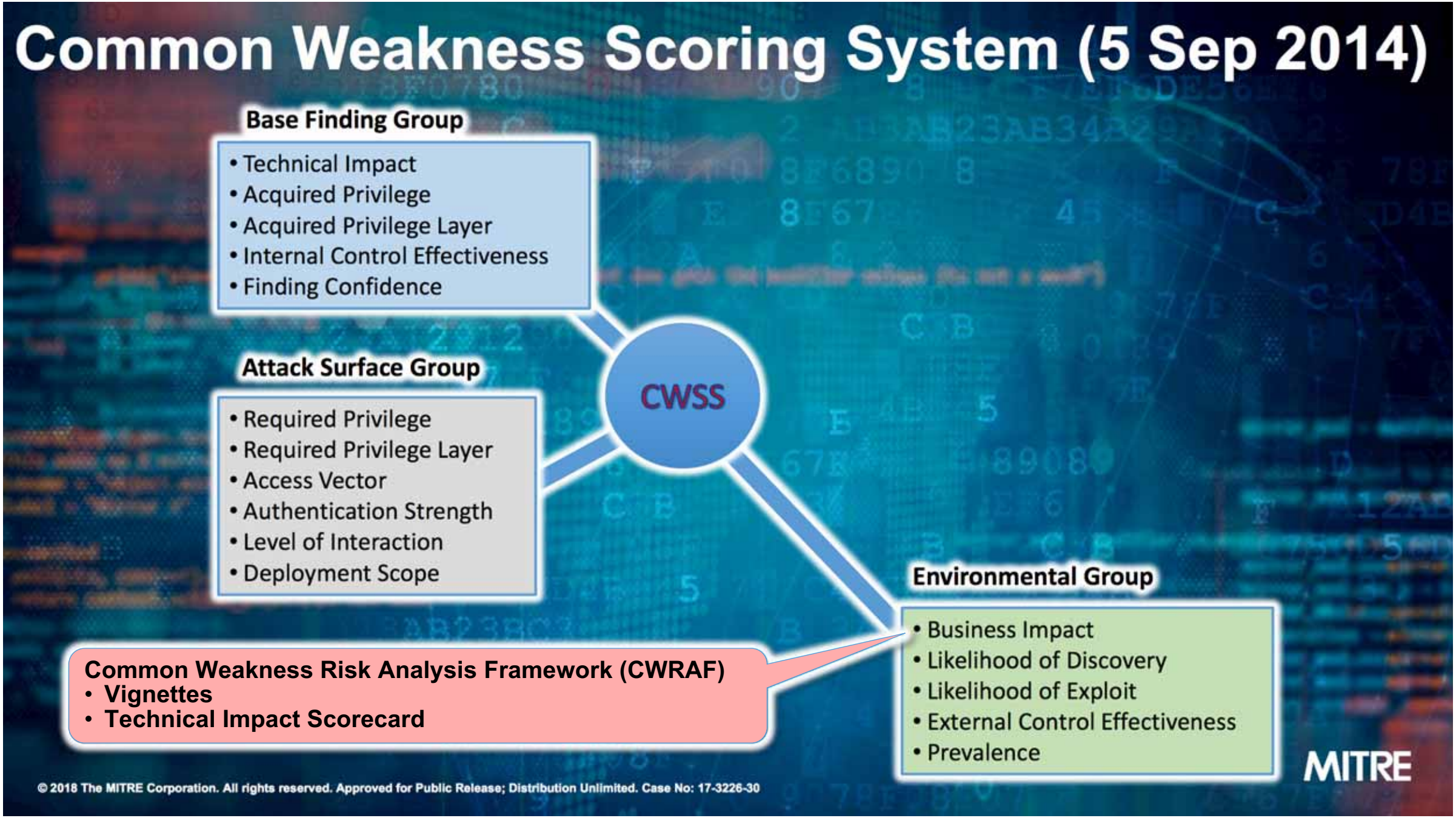
MITRE

CWSS & the Common Weakness Risk Analysis Framework (CWRAF) in a Nutshell



MITRE

Common Weakness Scoring System (5 Sep 2014)

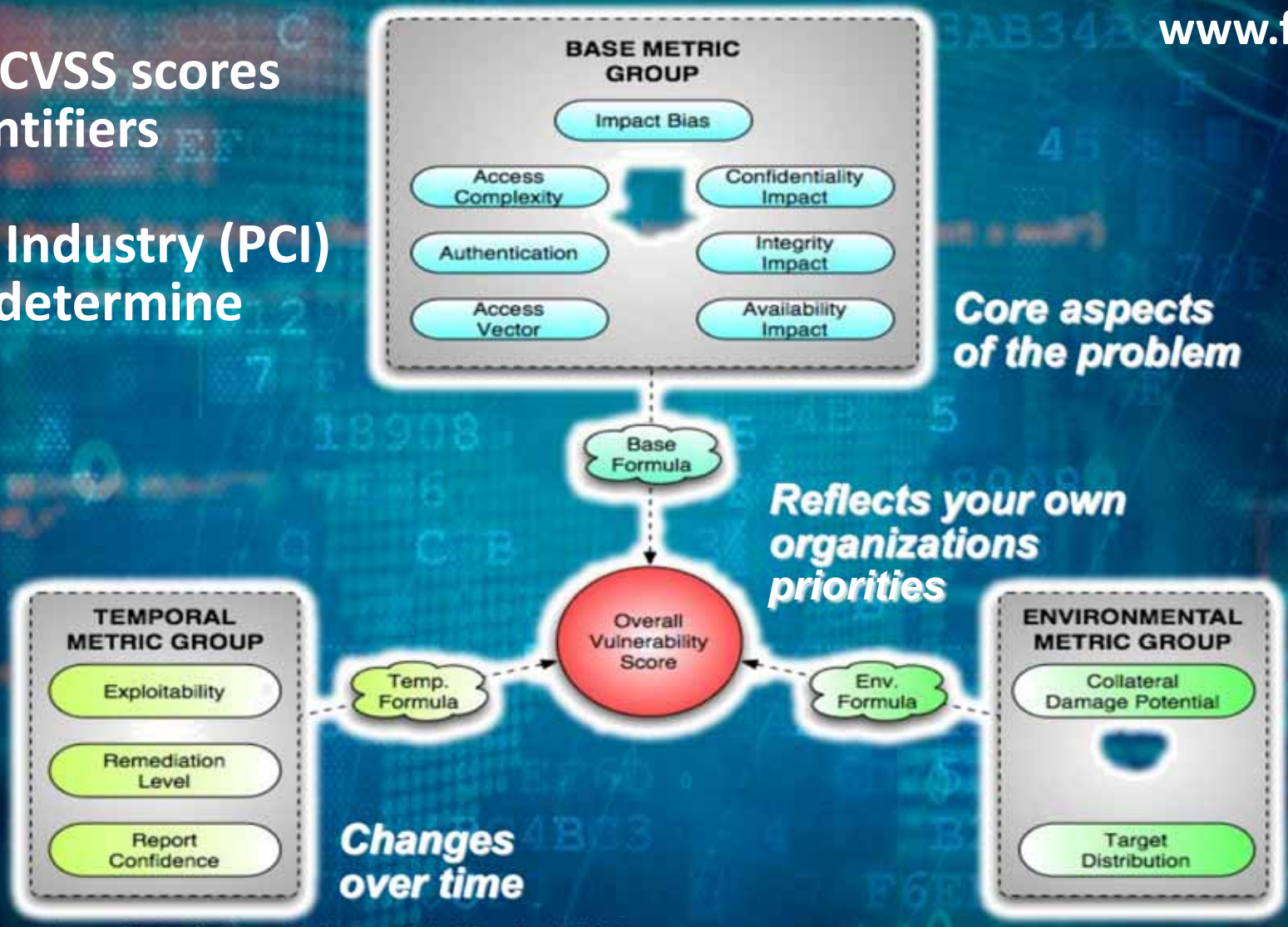


MITRE

Common Vulnerability Scoring System

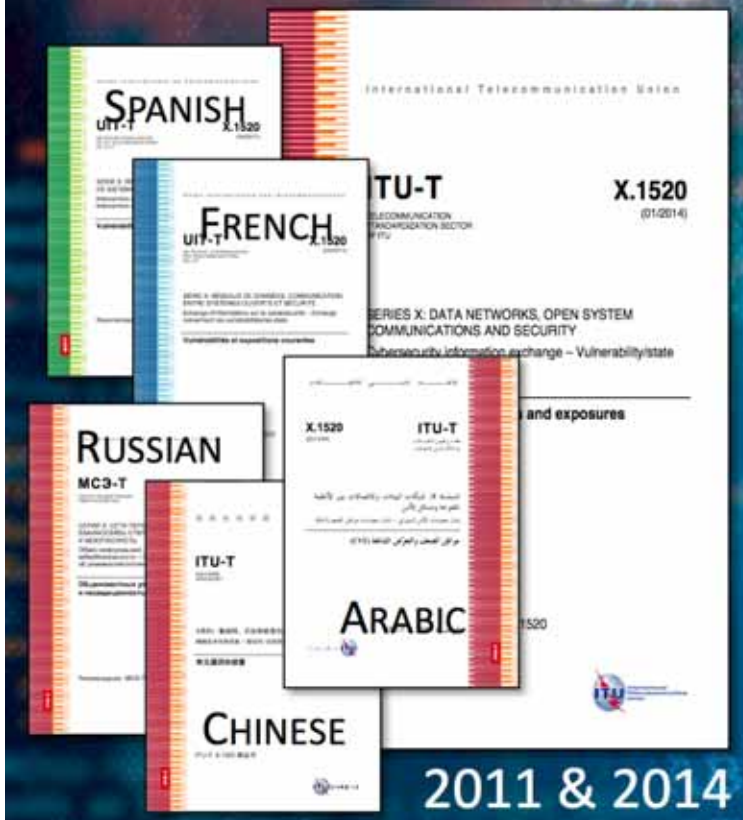
- NVD provides CVSS scores for all CVE identifiers
- Payment Card Industry (PCI) using CVSS to determine compliance

www.first.org/cvss/



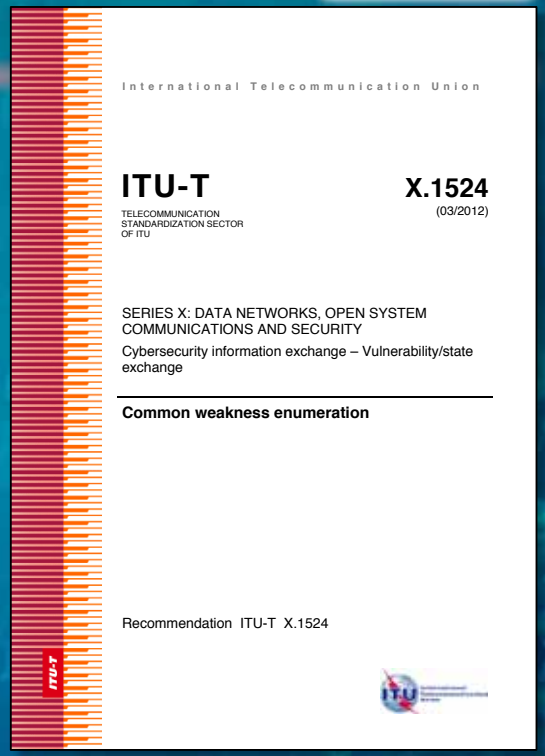
MITRE

Standards for Inputs and Calculating Risks…



2011 & 2014

2011 & 2016

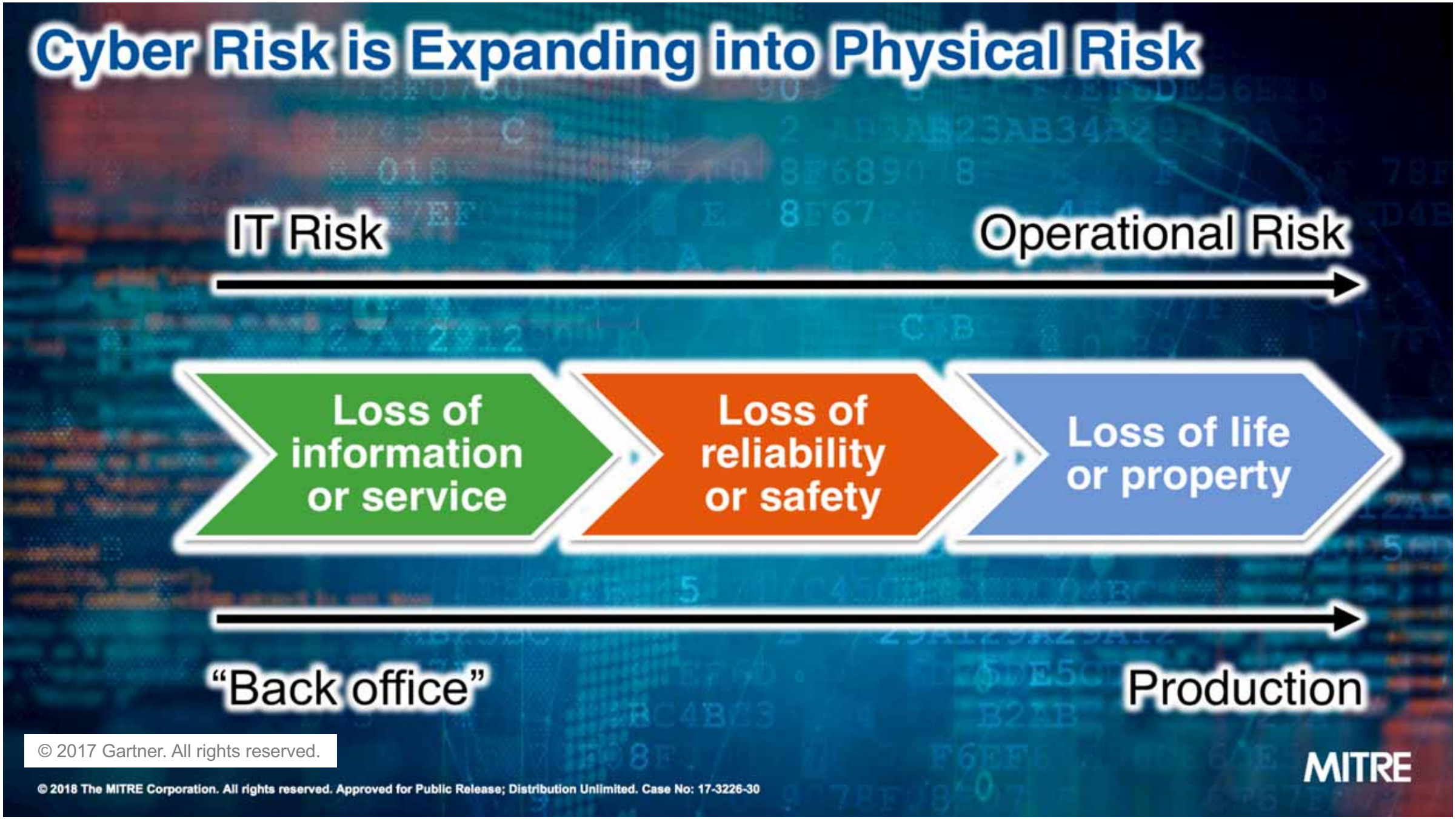


2012

2015

MITRE

Cyber Risk is Expanding into Physical Risk



MITRE

Who's risk is being managed?

MITRE