COLUMBIA | ENGINEERING
The Fu Foundation School of Engineering and Applied Science

Cybersecurity for Infrastructure

Center for Buildings, Infrastructure and Public Space

Shamir G. Pérez Sarraff
Lizzie Song
Dante Wu
Qiong Wu

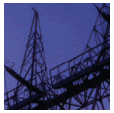
INTRODUCTION:

Critical infrastructure systems support the nation's economy, society and security but they are susceptible to cyber attacks. Advances in networking, computing, sensing and control systems have enabled a broad range of new devices. However, security often is left for later. Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. The industry needs enhanced awareness of potential cyber attacks and the ability to design in flexibility and resilience to mitigate the effects of such attacks in the critical manufacturing, dams, energy, transportation, water and wastewater system, nuclear reactors, materials and waste, and other sectors.

CRITICAL PHYSICAL INFRASTRUCTURE SECTORS:

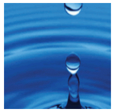
Critical Manufacturing
Unauthorized intrusion into control systems and data acquisition systems could disrupt supply chain

Dams
The cyber risks challenge outdated dam control systems of water storage, irrigation, electricity generation and flood control



Energy
Unstable energy supply or even blackout could cause public panic and cease many economic activities and across multiple sectors

Transportation
Disruption on traffic control system would interrupt movements of passengers and assets in the use of aviation, ships, rail, pipelines, highways, trucks and buses



Water and Wastewater Systems
Attacks could be large numbers of illnesses or casualties and/or a denial of service that would also impact public health and economic vitality

Nuclear Reactors, Materials, and Waste
Cyberattacks on nuclear power plants and isotopes used for medical procedures allow malicious actors to manipulate or exploit facility operations

Image Source: U.S. DHS Critical Infrastructure Sectors: https://www.dhs.gov/cisa/critical-infrastructure-sectors

RISKS IN DIFFERENT PHASES:

Design

- Exposing business plans and acquisition strategies
- Ransomware attack and computer crashing may destroy information then cause productivity loss and business delay

Construction

- Customer, contractor, and supplier lists and pricing disclosing
- Construction plans leak

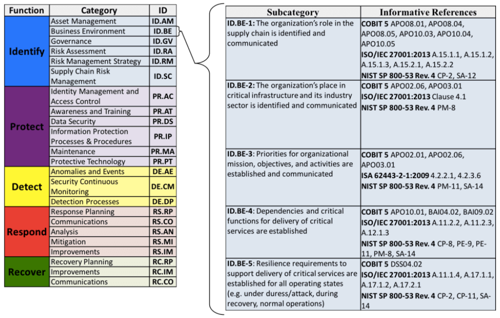
Operation

- Revealing personally identifiable information of employees
- Property damage and personal injury due to cybersecurity incidents

NIST FRAMEWORK:

Framework Components :

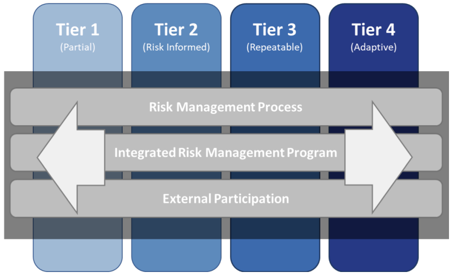
1. Framework Core



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

2. Framework Implementation Tiers



3. Framework Profiles

Profiles are an organization's unique alignment of requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile with a "Target" Profile. Below is an example:

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

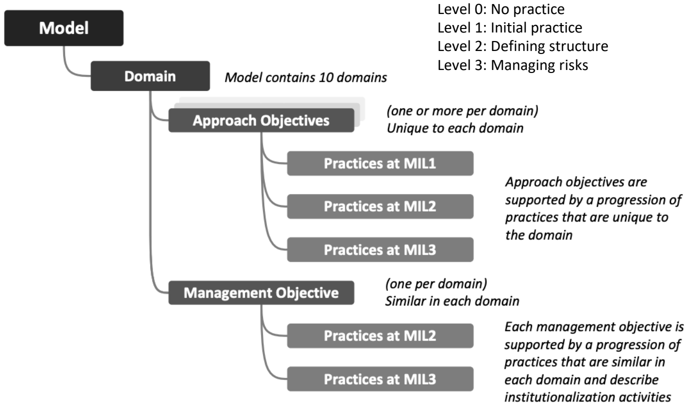
Target Profile

An Introduction to the Components of the Framework. Retrieved from NIST May 1st 2019

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2):

Model and Domain Elements:

*MIL = Maturity Indicator Level (0–3)
Level 0: No practice
Level 1: Initial practice
Level 2: Defining structure
Level 3: Managing risks



Model
Domain
Model contains 10 domains
Approach Objectives
(one or more per domain)
Unique to each domain
Practices at MIL1
Practices at MIL2
Practices at MIL3
Approach objectives are supported by a progression of practices that are unique to the domain
Management Objective
(one per domain)
Similar in each domain
Practices at MIL2
Practices at MIL3
Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities

10 Domains:
Risk Management, Asset, Change, and Configuration Management, Identity and Access Management, Threat and Vulnerability Management, Situational Awareness, Information Sharing and Communications, Event and Incident Response, Continuity of Operations, Supply Chain and External Dependencies Management, Workforce Management, Cybersecurity Program Management

Recommended Process for Using Evaluation Results:

	Inputs ➡	Activities ➡	Outputs
Perform Evaluation ⬇	1. C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct C2M2 Self-Evaluation Workshop with appropriate attendees	C2M2 Self-Evaluation Report
Analyze Identified Gaps ⬇	1. C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan ⬇	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2), Version 1-1, Feb 2014

CONCLUSION:

Cyberspace and its underlying infrastructure are vulnerable to a wide range of cyber risks. Protecting the cybersecurity of our critical infrastructure is a top priority for the nation. The NIST Framework is a strategic guidance for critical infrastructure sectors and organizations to reduce and manage their cyber risks regardless of their sizes or cybersecurity sophistication. Additionally, the industry should put efforts into aligning critical infrastructure owners and operators with existing resources to assist in using the Framework to manage their cyber risks.