MTR150264

MITRE

Cyber Prep 2.0

Motivating Organizational Cyber Strategies in Terms of Preparedness

Deborah Bodeau
Richard Graubart
May 2017

Dept. No.: J83C
Project No.: 01ADM105-CP

Bedford, MA

Approved By

//signed//	May 2017
Roberta Stempfley	

Abstract

As cyber threats evolve, organizations increasingly need to define their strategies for cyber security, defense, and resilience. Cyber Prep is a threat-oriented approach that allows an organization to define and articulate its threat assumptions, and to develop organization-appropriate, tailored aspects of a preparedness strategy. Cyber Prep focuses on advanced threats, but also includes material related to conventional cyber threats. Cyber Prep can be used in standalone fashion, or it can be used to complement and extend the use of other, more detailed frameworks (e.g., the NIST Cybersecurity Framework) and threat models. This paper provides detailed background on the Cyber Prep methodology, to help systems engineers and other analysts who are applying that methodology to understand its nuances and to situate it in the larger landscape of cyber strategic planning and risk management frameworks and methodologies.

This page intentionally left blank.

Executive Summary

Over the past several years, the cyber threat ecosystem has grown in size and complexity. Reports of major data breaches, concerted campaigns by persistent advanced actors, and marketplaces offering malware and unpublished vulnerabilities have raised the awareness of Government and business leaders that cybersecurity risks and resilience in the face of cyber attacks must be considered as part of enterprise risk management. Cyber preparedness – preparedness to handle cyber attacks as well as stealthy malicious cyber activities over extended periods – has become an integral part of the aspects of enterprise risk management related to dependence on cyberspace.

The landscape of resources – frameworks, guidelines, information sharing efforts, and commercial services – related to cyber risk management continues to increase in size and complexity. These frameworks and guidance vary in their underlying assumptions about the nature of the cyber threat. Some explicitly assume conventional threats. Others, while mentioning advanced adversarial threats, do not consider the need for resilience in the face of ongoing, stealthy campaigns. Some focus on technical solutions, while others emphasize operations. This diversity makes it very challenging for an organization to determine which resources to use to define its cyber preparedness strategy.

The Cyber Prep methodology addresses this problem by providing a general approach to articulating an organization's "risk frame" – i.e., how it thinks about risk, particularly its assumptions about threats and its concerns about consequences – and its overall strategy for addressing the cyber threats it faces. In particular, Cyber Prep helps mature understanding of aspects of the advanced persistent threat (APT), providing motivation for technical investments and organizational evolution. Systems engineers and organizational change management analysts use a small set of instruments (questionnaires, analysis guidance, automated tools) to apply the Cyber Prep methodology. Those instruments are supported by frameworks for characterizing threat and preparedness as described in this paper.

Distinguishing characteristics of Cyber Prep include the ways that it:

- Looks at both the *threat* that organizations face and the *measures* that organizations may take to defend themselves, making explicit the *relationship* between these two components. Cyber Prep enables an organization to articulate why it might be a target of advanced cyber adversaries, to develop profiles of its anticipated adversaries and characterize the attack scenarios and consequences of greatest concern, and thus to motivate specific aspects of its cyber preparedness strategy.
- Uses multiple dimensions to characterize both the attacker and defender:
    - For the Attacker, Cyber Prep considers Intent (e.g., goals such as financial gain or geopolitical advantage), Scope (or targeting), Timeframe, and Capabilities. These are driven by representative attack scenarios, which in turn are driven by organizational characteristics (e.g., assets, missions, role in the cyber ecosystem).
    - For the Defender, Cyber Prep considers Governance (e.g., organizational roles), Operations (e.g., proactive vs. reactive posture, stages of the cyber attack lifecycle or cyber kill chain addressed), and Architecture & Engineering (e.g., how well-defined the security architecture is, how the organization approaches security engineering).
- Facilitates definition and articulation of threat assumptions and concerns, and identification of tailored mitigations, appropriate for the organization based on the threat. *It is emphatically not intended to serve as either a compliance vehicle, or a maturity model.* Thus, while the Governance, Operations, and Architecture & Engineering areas are described in an incremental manner for the five preparedness strategies, Cyber Prep assumes that the organization will pick and choose strategic goals based on such considerations as (i) size, culture, and legal, regulatory, and contractual constraints and (ii) the threats of greatest concern to the organization. This contrasts with the all-or-nothing approach typical of compliance or maturity models.

- Can be used in standalone fashion and/or it can be used to complement, link and extend the use of other frameworks. Examples include the NIST Cybersecurity Framework (CSF) and sector-specific approaches such as the FFIEC Cybersecurity Assessment Tool; the CERT Resilience Management Model and the DHS Cyber Resilience Review; and a variety of proprietary capability maturity models and frameworks.

Cyber Prep provides a toolset in the form of questionnaires, analysis guidance, tables, descriptions, and pointers to other resources to help an organization identify the threat it faces, the consequences it seeks to deal with, and the frameworks, guidelines, and cyber threat information sharing efforts it can use.

Questions an organization should consider to orient to the threat include:

- What goals does a cyber adversary have (e.g., personal enrichment, geopolitical advantage)?
- At what scope or in what arena does the adversary operate?
- What are the likely capabilities and resources of the adversary (e.g., simply reuses freeware malware, develops customized malware targeted at the organization)?
- In what timeframe does the adversary operate (e.g., episodic, long term strategic campaigns)?

After characterizing its threat, an organization can determine the types and degrees of consequences that would result if an adversary successfully achieves its goals.

Understanding adversaries and potential impacts helps an organization define its strategy. An organization can use the characterizations of aspects of Governance, Operations, and Architecture & Engineering to assess its current preparedness and to define its cyber preparedness strategy. An organization that seeks to improve its overall cybersecurity posture often starts by acquiring cybersecurity products and tools, and then abandoning them because it lacks the expertise or sufficient staff to use them effectively, or because it failed to clearly plan or resource the products and tools to make them operational. Cyber Prep helps an organization consider such interdependent aspects of preparedness as:

- Governance: What is the organization's overall approach to defending against cyber threats? How strongly integrated is cyber risk management with other aspects of organizational risk management? Is the focus on compliance or pushing the state of the art to better engage the APT?
- Operations: Is the organization simply reacting to incidents as they become evident, or are cyber defenders proactively engaging early and across the cyber attack life cycle? How much does the organization use threat intelligence in its operations? How integrated (or isolated) is the organization's cyber security staff with other key players such as cyber defenders, malware analysts, and tool developers?
- Architecture & Engineering: How well defined, and integrated with mission operations, is the organization's security architecture? Are the organization's security capabilities focused on some or all of the CSF core functions; do they go beyond the CSF and address aspects of cyber resiliency? What is the organization's security engineering orientation?

The breadth of Cyber Prep – including adversary characteristics and characteristics of different preparedness strategies – can be used to identify the most relevant and useful aspects of other resources. Some frameworks never articulate threat assumptions, while others do not assume an APT; some guidelines only focus on cyber defense operations; some information sharing efforts assume a specific industry sector. Because organizations are often asked whether or how they are using existing frameworks or maturity models, Cyber Prep can be used to index into a variety of other frameworks and models. Also, Cyber Prep can link synergistically various other resources that focus on disparate aspects of an organization's threat or defender perspectives (e.g., pointing to the threat component of one, the operations component of another, the governance component of a third). This allows the relative strengths of those resources to be complementary, preventing the gaps or organization-irrelevant aspects of those resources from being weaknesses.

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

1 Introduction

As the size, number, and variety of publicly acknowledged cyber attacks has increased, many organizational leaders – Chief Executive Officers, Agency heads, members of corporate Boards – have come to recognize that an organization that is not prepared to deal with cyber threats is not exercising due diligence with respect to a class of expected risks.[1] As illustrated in Figure 1-1, an increasing number and variety of resources[2] are offered to help organizations define and execute a strategy for cybersecurity risk management. The NIST Cybersecurity Framework (CSF, [1] [2]) is one such resource, intended for use by organizations in critical infrastructure (CI) sectors. However, while the CSF – like the multi-tiered approach to risk management created by the Joint Task Force Transformation Initiative (JTF) – calls for an organization to calibrate its risk management strategy to the threat it faces, it offers no guidance on how to do this.

These resources vary in their underlying assumptions about the nature of the cyber threat. Some explicitly assume conventional threats. Others, while mentioning advanced adversarial threats, do not consider the need for resilience in the face of ongoing, stealthy campaigns. Some focus on technical solutions, while others emphasize operations. Any organization that seeks to improve its preparedness for cyber threats must navigate this increasingly large and complex landscape of cybersecurity resources to determine which resources will be relevant and useful. Cyber Prep is a threat-informed risk management approach which can be used as a stand-alone methodology, as well as to help organizations navigate this landscape.

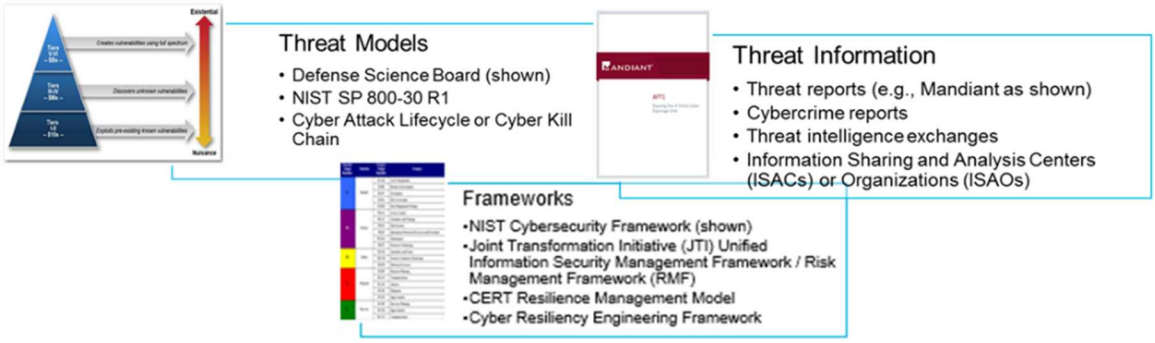

Figure 1-1. Organizations Must Navigate an Increasingly Complex Landscape of Cybersecurity Resources

Cyber Prep recognizes that cyber preparedness – preparedness to handle cyber attacks as well as stealthy malicious cyber activities over extended periods – has become an integral part of cyber risk management,[3] which in turn has become integral to enterprise risk management [3] [4] [5]. Cyber Prep provides a methodology – a process informed by a conceptual framework and supported by tools – that systems security engineers and organizational change management analysts can use to help organizations determine their current preparedness posture, characterize the adversaries which could be expected to target them, identify the corresponding desired preparedness posture, and develop a roadmap for moving from the current to the desired posture.

[1] See, for example, [5] [95] [96] [112].

[2] The JTF publications, including NIST SP 800-39 [6], NIST SP 800-30R1 [26], NIST SP 800-37 [85], and NIST SP 800-53 [38], represent a reasoned (albeit culturally challenging [54]) movement from compliance to risk management. Other frameworks and models include the CERT Resilience Management Model (RMM) [12], MITRE's Cyber Resiliency Engineering Framework [63] [64], and cybersecurity maturity models [13] [15] [22] [61] [19] [21] [16] [17] [18] [20]. Examples of reports on the cyber threat ecosystem include the Trend Micro Criminal Underground Economy series (e.g., [84]). Examples of threat models include the Defense Science Board's model [27], as well as models of the cyber kill chain [25] or cyber attack lifecycle [26] [94].

[3] "Cyber risk management" is the management of cyber risks, specifically risks due to malicious cyber activities (MCA) [77] as well as risks due to dependence on cyberspace. Cyber risk intersects with information security risk, as defined in NIST SP 800-30R1 [26], in its consideration of MCA.

This paper is intended to serve as a reference for those who apply Cyber Prep, e.g., systems engineers, organizational change management analysts, senior cybersecurity staff – for simplicity collectively referred to as analysts. The Cyber Prep toolset includes a small set of instruments: a threat-oriented questionnaire and a preparedness-oriented questionnaire, analysis guidelines which translate answers to threat-oriented questions into adversary characteristics and then into recommended levels of different aspects of preparedness, and worked examples. Those instruments are supported by the threat modeling framework and the framework for characterizing preparedness strategies as described in this paper.

As an expository device, Cyber Prep[4] defines five broad classes of adversarial threats and five corresponding classes of organizational preparedness strategies. These serve as a basic orientation to the idea that cyber preparedness must be threat-informed. To move beyond these broad classes, Cyber Prep defines adversary characteristics and three areas of preparedness strategies: Governance, Operations, and Architecture & Engineering. For each area, multiple aspects (e.g., Governance Structure, Security Posture Assessment, Architectural Definition) are defined, as illustrated in Figure 1-2. Cyber Prep enables an organization's approach to a given aspect to be motivated by the characteristics of the adversaries it faces. ***Because of this threat orientation, Cyber Prep is not a capability maturity model. The level of capability an organization seeks to achieve for a given aspect of preparedness is driven by specific characteristics of its adversaries, and different characteristics drive different aspects of preparedness.***

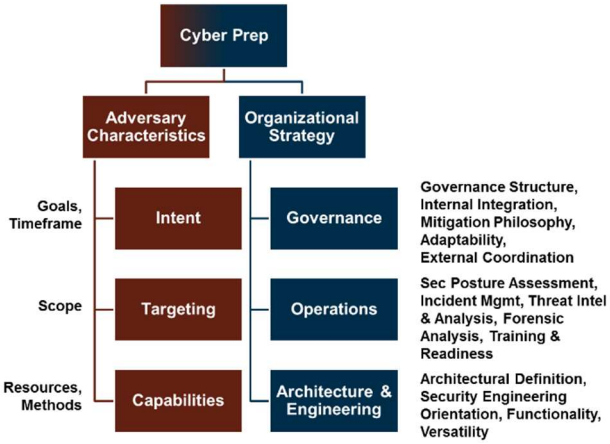

Figure 1-2. Cyber Prep Enables Aspects of Organizational Strategy to Match Adversary Characteristics

Cyber Prep can be described and used with varying degrees of specificity and detail. As Figure 1-3 illustrates, senior cybersecurity staff (e.g., staff directly supporting a Chief Information Security Officer or CISO) and analysts (including systems engineers and organizational change management analysts) can use Table 2-1 and a few questions to identify key characteristics of adversaries which can be expected to target the organization, as well as consequences of concern to the organization based on such factors as its size, sector, and role in that sector. They can then use Tables 2-2 through 2-4 to help identify mismatches between the classes of adversary the organization faces and its current preparedness strategy, using Tables 2-2 through 2-4. These materials aid in the preparation and presentation of briefings on Cyber Prep to organizational leadership.

[4] Cyber Prep 2.0 updates MITRE's previous Cyber Prep methodology [82] [83] [81], which has been used in other guidance [97]. Cyber Prep 2.0 provides more details in the areas of threat, operations, and architecture & engineering, while maintaining the original Cyber Prep approach of using five classes of threat. Aspects of governance in Cyber Prep 2.0 are based on those in the original Cyber Prep [83], but have been reorganized to reflect changes in practice and evolving guidance (e.g., [58] [86]). For readability, in this paper, "Cyber Prep" refers to Cyber Prep 2.0.

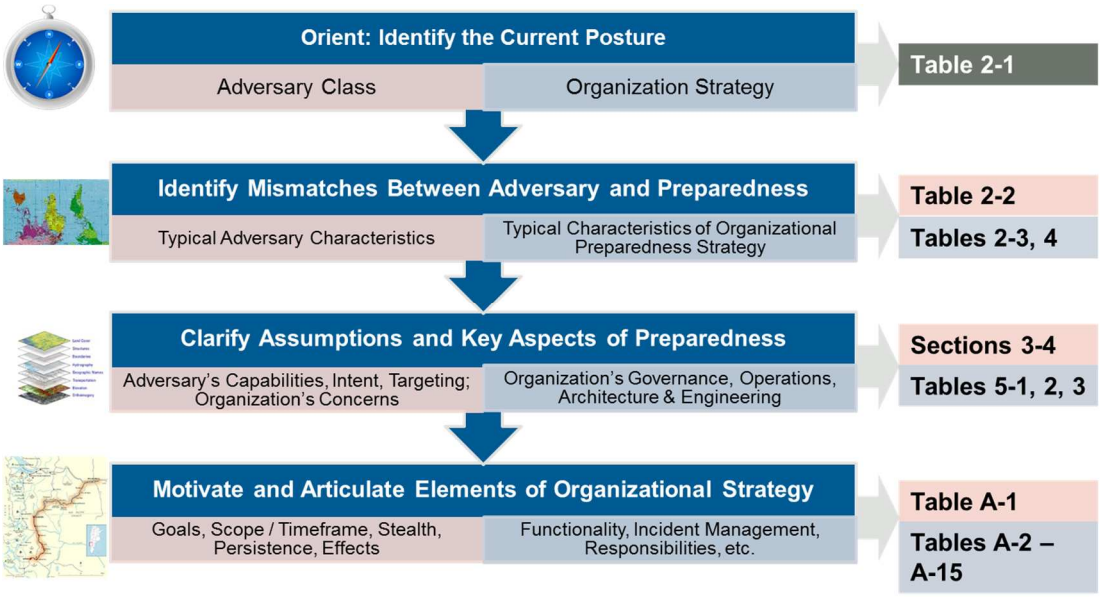

Figure 1-3. Describing and Using Cyber Prep

The materials in Sections 3 and 4 enable an organization to characterize its adversaries and concerns in more detail. These materials underpin the threat-oriented questionnaire and the determination of levels of adversary characteristics in the analysis guidelines. The tables in Section 5 characterize an organization's overall strategy in terms of Governance, Operations, and Architecture & Engineering. These tables underpin the preparedness-oriented questionnaire; in addition, analysts can use these tables to explain different levels and aspects of strategy in a succinct way. Finally, the materials in Appendix A underpin the determination of recommended levels of aspects of preparedness in the analysis guidelines. That is, these materials motivate (in terms of adversary characteristics) and articulate (in terms of aspects of Governance, Operations, and Architecture & Engineering) specific recommended approaches to preparedness, thus helping an organization to develop a strategic roadmap. Section 6 and Appendix B give analysts a key to the maps provided by various frameworks and guidelines. Section 7 provides a notional worked example. The rest of this Introduction situates Cyber Prep in terms of the multi-tiered approach to risk management defined by the JTF and other contexts in which cyber preparedness can be discussed.

1.1 Cyber Prep and the Multi-Tiered Approach to Risk Management

Risk management can be viewed as consisting of four components: risk framing, risk assessment, risk response, and risk monitoring [6]. Figure 1-4[5] illustrates the fact that in terms of the multi-tiered approach to risk management described in NIST SP 800-39 [6], Cyber Prep is intended primarily to support *risk framing* at the Organizational Tier, although it can be used at the Mission / Business Function Tier, particularly when the organization is large and diverse. That is, Cyber Prep helps an organization articulate its assumptions about the threat it faces, the consequences of greatest concern, and its overall approach to managing risk. As a result, the organization can execute its risk management processes at all tiers more efficiently and consistently.

[5] Figure 1-4 is derived from Figures 1 and 2 in NIST SP 800-39 [6].

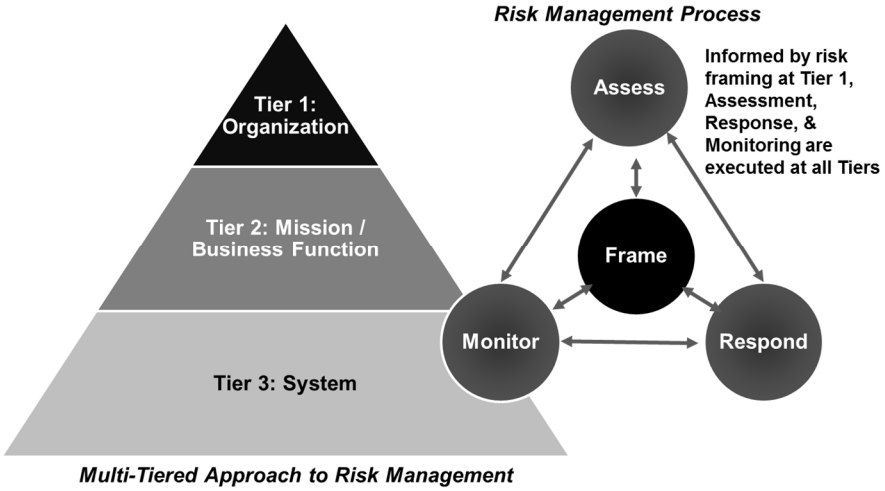

Figure 1-4. Cyber Prep Helps an Organization Frame Its Risks

Note that the CSF also uses three decision-making levels – Executive, Business / Process, and Implementation / Operations. While the Implementation / Operations level overlaps with both the Mission / Business and System Tiers, the Executive level coincides with the Organizational Tier.

1.2 Cyber Preparedness and Cyber Threat Modeling

Cyber threat modeling is the process of developing and applying a representation of adversarial threats (sources, scenarios, and specific events) in cyberspace. The assumed targets of adversarial threats can vary in scope / scale (e.g., device, organization) as well as in type (e.g., information, system, mission function). Cyber threat modeling can be performed for many reasons, including security operations and analysis, any of the four steps in the risk management process described in NIST SP 800-39, systems security engineering, motivating research problems and evaluating the relative effectiveness of solutions, penetration testing, cyber wargaming, and technology foraging. Depending on the purpose for which a cyber threat model – a representation of the adversarial threat or threats of concern – is to be used, a cyber threat model can focus on one aspect (e.g., characteristics of adversaries / threat actors; set of events; scenario or set of scenarios) or represent multiple aspects; can assume or represent characteristics or properties of the environment(s) in which the threat could materialize; and can include assessments or be entirely narrative.

The threat modeling framework in Cyber Prep, as described in Section 3, is designed to support the risk framing component of risk management. It therefore focuses on characteristics of adversaries and representative high-level threat scenarios, and enables an organization to describe its general threat model using relatively few constructs, with only a few representative values for each construct (e.g., timeframe, persistence). It does not include threat events or detailed threat scenarios, since these typically assume or represent system properties (e.g., specific technologies or types of technologies, common vulnerabilities). Such details can be added to the general threat model as needed by sub-organizations (e.g., acquisition program offices, mission or business functional units, a security operations center) for threat modeling purposes other than risk framing.

1.3 Cyber Preparedness in Multiple Contexts

As illustrated in Figure 1-5, an organization's preparedness to address the cyber threat can be considered in different and interrelated contexts, where each context is characterized by a specific scope of decisions or actions [7]. Cyber Prep focuses on preparedness for the enterprise or organization. Organizational preparedness determines the resources and options available to cyber defenders within the organization as they define strategies to identify and mitigate the effects of concerted campaigns against the organization's systems, operations, and information (Operations / Campaign) and as they use tools, and

apply defensive tactics, techniques, and procedures (TTPs) to handle events involving a limited subset of the organization's systems (Localized Engagement).

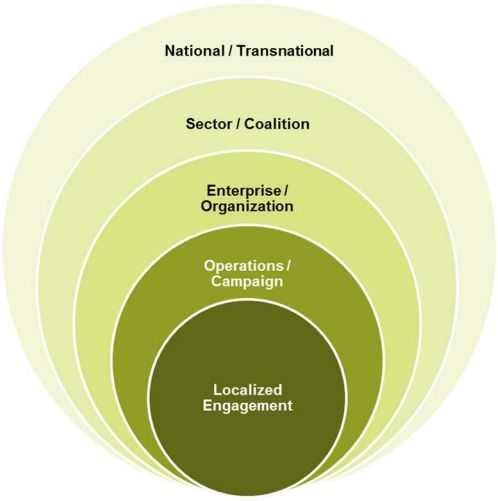

Figure 1-5. Cyber Preparedness at Multiple Levels

However, the organization does not stand alone in dealing with cyber threats. Each organization is part of multiple ecosystems of cyber-dependent entities. The organization is part of a sector ecosystem that includes its customers or end users, its partners and suppliers, its regulators, and (as the organization deals with cyber attacks on its systems or on those of its partners or suppliers) law enforcement. The organization can also be part of a coalition of entities that collectively commit to improving their overall cybersecurity posture and improving their cyber preparedness, by sharing information, coordinating, and collaborating. Cyber Prep helps the organization identify its strategy for participating in the cyber ecosystem, especially in the Sector / Coalition context.[6]

[6] See Section 6.1. At the National / Transnational level, the organization's systems form part of a broad ecosystem which includes, for example, all critical infrastructure sectors [111]. For further discussion of the cyber ecosystem, the April 2015 special issue of *Computer*, and [111] [122] [109] [113].

2 Cyber Prep Overview

This section provides an overview of Cyber Prep which analysts can use to develop briefings and other orientation materials, to explain what Cyber Prep is and how it can be used. It describes a high-level process framework in which analysts, in conjunction with organizational leadership and cybersecurity staff,

- Identify the organization's general threat assumptions and risk management philosophy;
- Identify mismatches between the organization's current risk management strategy and the characteristics of the cyber adversaries the organization faces;
- Clarify threat assumptions and articulate high-level targets for the three areas of preparedness (Governance, Operations, and Architecture & Engineering); and
- Use Cyber Prep with other frameworks to motivate and articulate strategic goals.

Cyber Prep provides a high-level construct that an organization can use to characterize the cyber threats it faces. In effect, Cyber Prep challenges the organization to apply "pre-hindsight" – if, tomorrow or six months from now, a news story identifying the organization as the target of attack by a given category of adversary appeared, how surprised would organizational leaders be? Based on the characterization of the threats it faces, the organization can characterize its strategy for preparing for those threats. Two types of adversary –1) *conventional* or 2) *advanced* – correspond to two risk management philosophies – 1) *practice-driven* or 2) *threat-informed and anticipatory*.

However, while these broad types and philosophies provide an initial step toward articulating the organization's *risk frame* – i.e., how it thinks about risk, including its assumptions about threats and its concern for consequences – they are too general to drive the definition of a risk management strategy. Therefore, Cyber Prep defines five classes of adversary, based primarily on the adversary's goals, and five corresponding preparedness strategies. These provide an initial orientation, as a starting point for discussion.

Figure 2-1. Cyber Prep Classes

Beyond this high-level construct, Cyber Prep is a practical approach, providing multiple tools which an organization can use to articulate its strategy for addressing cyber threats – particularly the advanced persistent threat (APT)[7] – and determining the appropriate mitigations to those threats. It provides

[7] The Joint Task Force Transformation Initiative (DoD, ODNI, and NIST) defines the APT as: "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending

motivation for technical investments and organizational evolution. Distinguishing characteristics of Cyber Prep include:

- Cyber Prep looks at both the *threat* that organizations face and the *measures* that organizations may take to defend themselves, as well as the *relationship* between these two components. Many frameworks focus on one dimension (e.g., the adversary's capability level, the defender's operational process maturity). Cyber Prep uses multiple dimensions to characterize both the attacker and defender:
    - For the Attacker, Cyber Prep considers Intent (e.g., goals such as financial gain or geopolitical advantage, timeframe), Targeting (e.g., scope), and Capabilities (e.g., resources, expertise). These are driven by representative attack scenarios, which in turn are driven by organizational characteristics (e.g., assets, missions, role in the cyber ecosystem).
    - For the Defender, Cyber Prep considers Governance (e.g., organizational roles), Operations (e.g., proactive vs. reactive posture, stages of the cyber attack lifecycle addressed), and Architecture & Engineering (e.g., how well-defined the security architecture is, the organization's security engineering orientation).
- Cyber Prep facilitates definition and articulation of threat assumptions and concerns, and identification of tailored mitigations, appropriate for the organization based on the threat. *It is emphatically not intended to serve as either a compliance vehicle, or a maturity model.* Thus, while the Governance, Operations, and Architecture & Engineering areas are described in an incremental manner for the five preparedness strategies, Cyber Prep assumes that the organization will pick and choose strategic goals based on such considerations as (i) size, culture, and legal, regulatory, and contractual constraints and (ii) the threats of greatest concern to the organization. This contrasts with the all-or-nothing approach typical of compliance or maturity models.
- Cyber Prep can be used in standalone fashion. It can also be used to complement, link and extend the use of other frameworks. Examples include (1) the CSF and sector-specific approaches such as the financial sector using the FFIEC Cybersecurity Assessment Tool [8], the energy sector [9] [10], and the healthcare sector [11]; (2) the CERT Resilience Management Model [12]; and (3) any of a variety of capability maturity models and frameworks [13] [14] [15] [16] [17] [18] [19] [20] [21] [22].

As was described in Section 1, Cyber Prep is supported by expository material, tables, descriptions, and pointers to other resources. These materials enable an organization to orient to the threat; identify mismatches between the class(es) of adversary it faces and its cyber preparedness strategy; characterize its adversaries and concerns in more detail and define its overall strategies in the areas of Governance, Operations, and Architecture & Engineering; and articulate its specific approaches to various aspects of those areas. These activities are described in the next four subsections.

footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives." [6] The term "advanced cyber threat" is also used. [27]

2.1 Identify General Threat Assumptions and Risk Management Philosophy

Analysts can help an organization define its overall orientation using a few general characteristics of threat an organization might assume it faces, and corresponding organizational preparedness strategies.

Table 2-1. Defining the Overall Threat Orientation and Organizational Strategy

Threat Assumptions	Organizational Strategy
Cyber Vandalism One-time or periodic attacks by a relatively unsophisticated adversary	***Basic Hygiene*** Emphasis: Basic security tools. Define and protect the enterprise perimeter. Use malware protection products within the enterprise.
Cyber Incursion Periodic or sustained attacks by an adversary that views the organization as a worthwhile target	***Critical Information Protection*** Emphasis: Processes, procedures, and better tools. Recognize cyber attack as an ongoing challenge. Implement data protection. Define incident response processes. Use limited threat information sharing, primarily as a consumer.
Cyber Breach & Organizational Disruption Sustained campaign by a stealthy, moderately-resourced adversary (e.g., professional organized crime), seeking a significant gain or a long-term advantage	***Responsive Awareness*** Emphasis: Cybersecurity operations and supportive technologies. Execute cybersecurity risk management processes. Implement a balanced set of controls to protect against, detect, and recover from attack activities, rather than simply responding to the consequences of an incident.
Cyber Espionage & Extensive Disruption Sustained campaigns by a stealthy, well-resourced adversary (e.g., nation state, terrorist organization), seeking long-term gains or advantages, often operating on a large scale	***Architectural Resilience*** Emphasis: Organizational integration. Make cybersecurity and resilience part of enterprise risk management. Define architectures and implement controls to provide operational and cyber resilience. Make cyber situational awareness (SA) part of mission SA, and jointly manage cyber and mission risks during operations.
Cyber-Supported Strategic Disruption Sustained campaigns, integrated across different attack venues (cyber, supply chain, physical), by a stealthy, strategic adversary (e.g., nation state), seeking geopolitical advantages	***Pervasive Agility*** Emphasis: Collaboration and integration to meet broad-scale threats. Make cybersecurity and resilience an integral part of mission assurance and strategic planning. Define architectures for adaptability and agility. Integrate SOC (Security Operations Center) and mission operations.

If an organization does not resonate with the descriptions in the preceding table, a few questions can help analysts identify the type of adversary an organization should expect to face, and the corresponding overall risk management philosophy. An organization that is a likely target for the APT needs a *threat-informed and anticipatory risk management* philosophy.

- *In what sector does the organization operate?* Organizations in CI sectors are more likely targets for the APT; sector-specific threat information sharing will support *threat-informed and anticipatory risk management*. However, not every organization in a CI sector will automatically be a target.
- *How critical is the organization to its sector?* Sector-critical organizations are more likely targets for the APT. Depending on the sector, a sector-critical organization could even be a target for cyber warfare. Sector-critical organizations are often distinguished by the value of the CI components they manage, the services they provide to other CI organizations, their position in the supply chain, or the number of customers or the size of the region they serve.
- *How valuable are the resources (e.g., information, products, services) that the organization holds, manages, or provides?* The more valuable the resources are – the more widespread or harmful the consequences of compromise could be to the organization or its stakeholders, or the more potentially useful to competitors or adversaries – the more likely the organization is to be

the target of the APT. Note that the value to an adversary could exceed the value to the organization.[8]

- *Who are the organization's customers and partners?* An organization that serves or partners with a sector-critical organization, or one that holds highly sensitive information about its customers or partners, is more likely to be the target of the APT.

It must be noted that Cyber Prep is most relevant to large and mid-size organizations. Smaller organizations often struggle even to provide foundational cybersecurity functions (often referred to as basic hygiene), and lack the resources for threat-informed risk management; a *practice-informed risk management* philosophy is often the best fit (see [23] for additional guidance). However, an organization which is sector-critical, due to the functions it performs or its role in the supply chain, is a likely target for cyber disruption or espionage, even if it is small. Similarly, an organization that holds information about high-value targets (whether individual or organizational) is a likely target for data breach attacks by APT actors. Sector-critical small organizations need to consider partnering with or participating in larger efforts.

2.2 Identify Strategy Mismatches

The two tables in this section provide characterizations of the five classes of adversaries and the corresponding five cyber preparedness strategies. It must be emphasized that a given organization may need to be prepared for a range of adversaries. (This is discussed in more detail in Section 3.2 below.) For each class of adversary, the organization needs to focus on the *goals* and *scope*, and ask: *How surprised would any reasonable person be to learn that we had been attacked by such a threat actor?* Table 2-2 provides characterizations the organization can use.

A cyber attack lifecycle (CAL, [24]) or cyber kill chain (CKC, [25]) model, such as the one shown below,[9] is helpful in understanding attacker characteristics. Conventional adversaries are not expected to craft malware (Weaponize), nor to seek to Maintain a persistent presence on organizational systems.

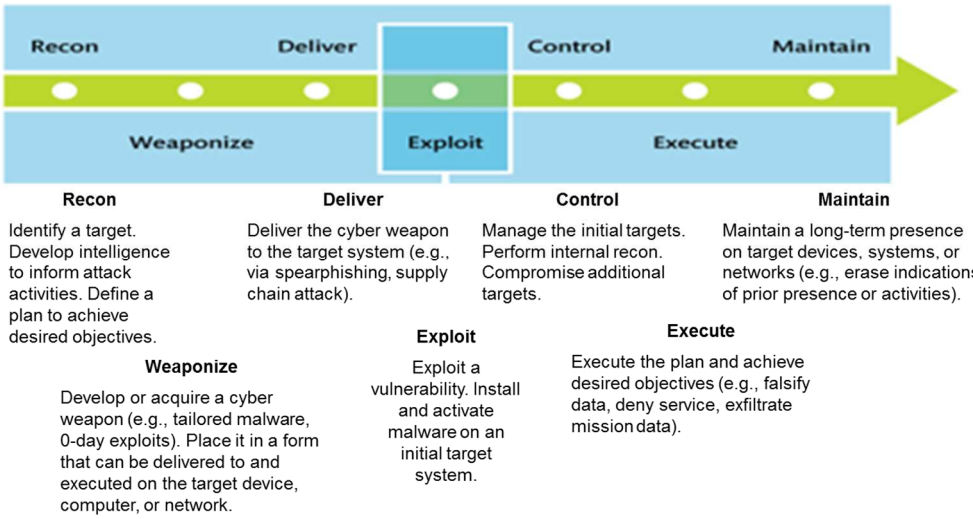

Figure 2-2. General Cyber Attack Lifecycle Model

[8] The idea of value-at-risk, originally defined in the financial services domain, has been adapted to the cyber domain and applies to assets and reputation. [113] While the cyber value-at-risk model [37] is useful, it cannot fully account for value-to-adversaries. For example, an asset such as a company phone book could be more valuable to an adversary than to the organization that owns it, even taking into consideration the possibility that its compromise leads to some negative publicity. In addition, an organization can inaccurately value some of its resources (e.g., by not drawing relationships between cyber and non-cyber resources, by not fully executing a Business Impact Analysis or Mission Impact Analysis) in the context of malicious cyber activity.

[9] The cyber attack lifecycle model is discussed further in Section 4.2.

Table 2-2. Representative Characteristics of Cyber Adversaries

Adversary Class	Representative Characteristics
Cyber Vandalism	**Goals**: Personal motives (e.g., attention, malice), Financial gain (fraud) **Scope**: Organizational subset (e.g., public-facing service or Web site) **Timeframe, Persistence, and Stealth**: Attacker revisits periodically, but is not persistent, nor stealthy **Examples of Effects**: Web site defacement, DoS attack, Falsification of selected records **Capability Examples**: Freeware or purchased malware, purchased botnets, purchased or stolen credentials
Cyber Incursion	**Goals**: Personal motives (e.g., acquire personally identifiable information or PII about targeted individuals), Financial gain (fraud, salable information, extortion), Stepping-stone **Scope**: Organizational Operations; Organizational Associates **Timeframe, Persistence, and Stealth**: Sustained, persistent activities in selected stages of CAL: recon, deliver, exploit, execute; limited concern for stealth **Examples of Effects**: Data breach, Data unavailability due to ransomware, Extended DoS **Capability Examples**: Freeware or purchased malware, purchased botnets, purchased or stolen credentials used to acquire more credentials and further escalate privileges
Cyber Breach & Organizational Disruption	**Goals**: Financial gain (large-scale fraud or theft, salable information, extortion), Geopolitical advantage (economic), Stepping-stone **Scope**: Organizational Operations; Organizational Associates **Timeframe, Persistence, and Stealth**: Sustained with persistent, stealthy activities in most stages of CAL: recon, deliver, exploit, control, execute, maintain **Examples of Effects**: Extensive data breach, Establish foothold for attacks on other organizations **Capability Examples**: Adversary developed malware (e.g., 0-day exploits)
Cyber Espionage & Extensive Disruption	**Goals**: Financial gain (fraud, salable information, extortion), Geopolitical advantage (political, economic, social, or military) **Scope**: Organizational Operations; Sector **Timeframe, Persistence, and Stealth**: Sustained with persistent, stealthy activities in all stages of CAL **Examples of Effects**: Extensive or repeated data breaches, Extensive or repeated DoS **Capability Examples**: Malware crafted to the target environment, to maintain long-term presence in systems
Cyber-Supported Strategic Disruption	**Goals**: Geopolitical advantage (political, economic, social, and/or military) **Scope**: Organizational Operations for selected organizations; Sector; Nation **Timeframe, Persistence, and Stealth**: Enduring with persistent, stealthy activities in all stages of CAL, covert activities against supply chains or supporting infrastructures, and covert intelligence-gathering **Examples of Effects**: Subverted or degraded critical infrastructure **Capability Examples**: Stealthy, destructive adversary-crafted malware, supply chain subversion, kinetic attacks

After characterizing the adversary using Table 2-2, analysts can identify the types of organizational or operational consequences of adversary activities with which it is concerned. In effect, analysts and organizational leaders ask: *How much impact would result if an adversary successfully achieves its goals?* The impacts can range from limited or near-term to severe and long-term.

To understand how significant the effects of an adversary attack on or campaign against the organization might be, the organization needs to consider the potential cyber effects (e.g., degradation or disruption of service; corruption, modification, or insertion of information; or exfiltration, interception, or other compromise of information), and relate these to organizational missions or critical business functions.

To manage risks associated with the relevant adversary classes, the organization needs to ask: *How prepared are we to detect – or anticipate – adversary activities characterized by such timeframe, persistence, stealth, and capabilities? How prepared are we to handle such effects?* Alternately, the organization can ask: What is our current preparedness posture? What are we prepared to detect or defend against? What are we prepared to do? How do our enterprise architecture and our engineering processes

support being prepared for such threats? Analysts can use the capsule characterizations in Table 2-3[10] to help organizational leadership get a sense of the organization's current cyber preparedness posture.[11]

Table 2-3. Representative Characteristics of Cyber Preparedness Strategies

Preparedness Strategy	Representative Characteristics
Basic Hygiene	Prepared to Detect or Defend Against: One-time or periodic attacks by a relatively unsophisticated adversary, with limited or near-term effects. Capability, Intent, and Targeting: Very Low[12]. Prepared How: An ad-hoc, informal decision process is used for cybersecurity (CS), focusing on compliance with good practice. Minimal investment in assessing organizational security posture. CS staff respond to incidents post Execution. Security capabilities: CSF functions of Protect, Detect and Respond.
Critical Information Protection	Prepared to Detect or Defend Against: **Sustained** attacks by **an unsophisticated** adversary, with limited or near-term effects. Capability, Intent, and Targeting: **Low**. Prepared How: **The Security Program Officer** handles CS decisions. **The organization shares threat information with partners. Organization monitors cyber resources.** CS staff respond to **Exploit and Execution stage** incidents. Security capabilities: CSF functions of Protect, Detect, Respond, **and Recover**.
Responsive Awareness	Prepared to Detect or Defend Against: A sustained **campaign** by a **stealthy, moderately-resourced** adversary, **seeking a significant, long-term advantage and extensive** or mid-term effects. Capability, Intent, and Targeting: **Medium**. Prepared How: **A responsible corporate officer** handles CS decisions. **CS is integrated with related disciplines**. **CS staff cooperate with counterparts at peer, partner, supplier, and customer organizations**. The organization **uses updated threat intelligence in monitoring**. CS staff **manage events across the cyber attack lifecycle**. Security capabilities: **all CSF functions and some limited cyber resiliency objectives**.
Architectural Resilience	Prepared to Detect or Defend Against: **Multiple** sustained campaigns by stealthy, **well**-resourced adversaries, seeking **long-term** advantages, **often on a large scale**, with **severe or long-term** effects. Capability, Intent, and Targeting: **High**. Prepared How: A **dedicated** corporate officer handles CS decisions. CS **and related disciplines** are integrated with **mission assurance (MA**). **Cyber defense and strategic planning staff** coordinate with counterparts at peer, partner, supplier, and customer organizations. The organization **maintains** cyber **situation awareness (SA**). **An integrated team of cyber defenders, malware analysts and tool developers jointly develop tailored response tools**. Security capabilities: all CSF functions and **most** resiliency objectives.
Pervasive Agility	Prepared to Detect or Defend Against: Multiple sustained campaigns**, integrated across different attack venues (cyber, supply chain, physical)**, by stealthy, **enduring** adversaries, **seeking geopolitical advantages**, with severe or long-term effects. Capability, Intent, and Targeting: **Very High**. Prepared How: The **CEO is engaged in MA** decisions. CS and related disciplines **collaborate to ensure** MA. Cyber defense and strategic planning staff **collaborate** with **relevant mission or critical infrastructure sector entities**. Cyber SA **and mission SA integrated**. **Cyber defenders** develop **and use new threat analytic methods.** An integrated team **develops and uses new forensics methods**. **Contingency plans, COOP and cyber responses developed jointly. Coordination or collaboration with other organizations central to planning**. Security capabilities: all CSF functions and **all** resiliency objectives.

2.3 Clarify Threat Assumptions and Target Areas of Preparedness

Using the threat modeling framework described in Section 3 and reflected in the threat-oriented questionnaire and analysis guide, analysts can help the organization further clarify assumptions about the adversaries it faces. The organization can make further use of that clarification: The framework is

[10] For ease of understanding, differences between one class and the next are **bolded**. However, it must be emphasized that, as the organization develops its cyber preparedness strategy, it will tailor and make use of those aspects that best enable it to address the threat it faces, often mixing strategic elements from different classes; Cyber Prep is not a maturity model.

[11] Note that the functional areas of Identify, Protect, Detect, Respond, and Recover in the tables are drawn from the NIST Cybersecurity Framework. If the organization uses a different framework, it will need to reword the characteristics of its strategy to be consistent with the framework it uses. Cyber resiliency objectives are defined in the Cyber Resiliency Engineering Framework (CREF, [63] [64] [65] [66]).

[12] Levels of Capability, Intent and Targeting are as defined in NIST SP 800-30 [26].

consistent with the underlying model and levels of Capability, Intent, and Targeting in NIST SP 800-30 [26], and therefore can be expected to be consistent with sector-specific threat models or modeling frameworks. The organization's cybersecurity staff can combine identified or assumed adversary characteristics with expected impacts to define its overall inherent cyber risk.[13]

Based on the results of the analysis, the organization can identify the characteristics of Governance, Operations, and Architecture & Engineering that will best serve to manage its cyber risk. Table 2-4 presents a high-level summary of those characteristics, as mapped to the five Cyber Prep strategies.

Table 2-4. Summary of Governance, Operations, and Architecture & Engineering Aspects of Cyber Prep Classes

Strategy	Organizational Cyber Preparedness Posture: Summary
Basic Hygiene	Governance: **The organization uses an informal decision process for cybersecurity (CS), which is not integrated with other disciplines. The focus is on compliance with good practice. Information sharing is limited to information and communications technology (ICT) staff.** Operations: **The organization invests minimally in assessing its security posture. CS staff are reactive and respond to incidents as they become aware of a situation.** Architecture & Engineering: **The organization informally defines its security architecture, focusing on security for the perimeter and selected internal resources.**
Critical Information Protection	Governance**:** The **Security Program Officer handles CS** decisions. **CS is aligned with related disciplines. The organization is able to handle short-term decision making disruptions informally**. **The organization shares threat information with partners and suppliers.** Operations**:** The organization **performs monitoring of cyber resources.** CS staff **perform ongoing review of threat intelligence on attack patterns**. Architecture & Engineering**:** The organization's security architecture **may be** informally defined**, to include data loss protection as well as** security for the perimeter and **internal resources**.
Responsive Awareness	Governance**:** The **responsible corporate officer** handles CS decisions. The organization is able to handle **decision making disruptions as part of continuity of operations**. CS is **integrated** with related disciplines and **pushes the state of the practice to address APT**. **CS staff cooperate** with **counterparts at peer, partner,** supplier**, and customer organizations**. Operations: The organization **uses updated threat intelligence** in ongoing monitoring. CS staff manage events **across the cyber attack lifecycle (CAL)**, and perform ongoing review of threat intelligence, **including looking at future** attack patterns. Architecture & Engineering**:** The organization's security architecture is **defined, and includes mission/CS dependency analysis. Security capabilities support** a**chievement of some limited cyber resiliency objectives, informed by security risk management**.
Architectural Resilience	Governance: A **dedicated** corporate officer handles CS decisions. CS and related disciplines are **integrated with mission assurance (MA) or continuity of operations. Cyber defense and strategic planning** staff **coordinate** with counterparts at peer, partner, supplier, and customer organizations. Operations: The organization **maintains situation awareness (SA) of cyber resources and threats**. **An integrated team of cyber defenders, malware analysts and tool developers jointly develop cyber courses of action (COAs) in response to malware**. The organization's tailored training includes **updated** threat intelligence**.** Architecture & Engineering**:** The organization's security architecture is defined, and includes mission/CS dependency analysis. Security capabilities are provided to achieve **most** resiliency objectives, informed by **mission** risk management.
Pervasive Agility	Governance**: The CEO** is engaged in **MA** decisions. CS and related disciplines **collaborate to ensure** MA and continuity. Cyber defense and strategic planning staff **collaborate** with **relevant mission or critical infrastructure sector entities**. Operations: **Cyber SA is integrated with mission SA.** Cyber defenders **develop and use new threat analytic methods. Contingency plans, COOP and cyber COAs are developed jointly.**

[13] "Inherent cyber risk" is the risk posed to the organization by the technologies and connection types, delivery channels, online/mobile products and technology services required for its operations, as well as by organizational characteristics and external threats [8].

Strategy	Organizational Cyber Preparedness Posture: Summary
	Architecture & Engineering: The organization's security architecture is defined, includes mission/CS dependency analysis, **and identifies dependencies on external systems**. Security capabilities are provided **for a full range** of CS functions, and **all** resiliency objectives, informed by mission **and strategic** risk management.

Even when the characteristics are described in such high-level terms, it will often be the case that an organization's strategy is – and, based on adversary characteristics, should be – a hybrid, for example combining the Governance, Operations, and Architecture & Engineering aspects from different levels. Cyber Prep is designed to support such variation. Section 5 and Appendix A provide more detail on these aspects, recommended levels of which are determined based on adversary characteristics.

2.4 Using Cyber Prep with Other Frameworks to Motivate and Articulate Strategic Goals

Cyber Prep can be used alone or with other frameworks to motivate and articulate aspects of an organization's cyber preparedness or risk management strategy. Cyber Prep provides information in the areas of adversary Capabilities, Intent, and Targeting and of the Governance, Operations, and Architecture & Engineering areas in an organization's preparedness strategy. The aspects of these areas can be used to build out a description of an organization's threat assumptions and preparedness strategy; they can also be used to index into other frameworks.

This enables Cyber Prep to help an organization make simultaneous use of other resources as illustrated below, without tying the organization to a single framework or model. For example, the adversary Capabilities area in Cyber Prep roughly corresponds to the Tiers of the DSB threat model [27], the Governance area of Cyber Prep strategies other than Pervasive Agility roughly correspond to Tiers 1-4 of the NIST Cybersecurity Framework [1] [2], and some of the specific aspects of Governance in Cyber Prep are analogous to aspects of the governance and risk assessment capabilities of the CSF Core.

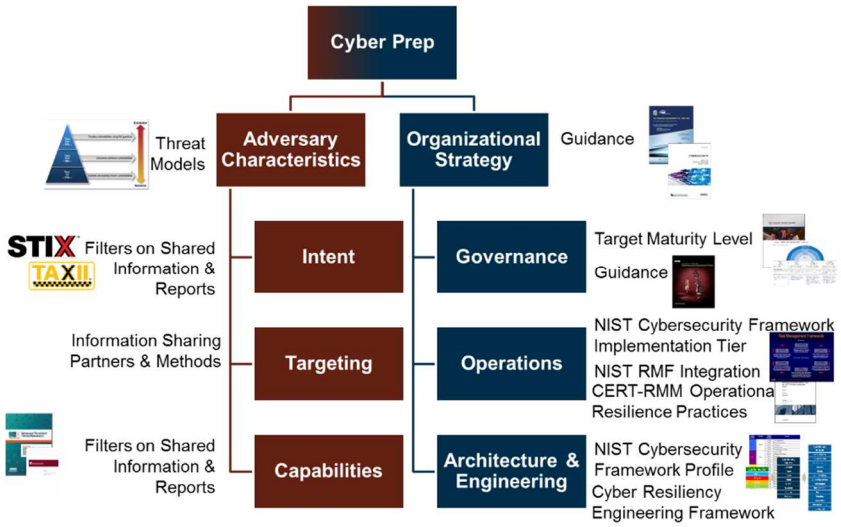

Figure 2-3. Cyber Prep Enables the Organization to Use Appropriate Resources

An organization's ability to select or use a cybersecurity, resilience, or threat framework can be limited by its resources, organizational culture, sector, mission, or business model; and/or risk frame [4]. Some frameworks never articulate threat assumptions; some assume only focus on the operations aspect of the defender; other frameworks are not intended to deal with APT. Using Cyber Prep, an organization can select the relevant portion(s) of one or more cybersecurity or resilience frameworks or guidelines. Cyber Prep can be used to index into another framework, so that an organization can decide how to use that framework in its cybersecurity strategy. In addition, Cyber Prep can be used to link synergistically various other frameworks and guidance that focus on disparate aspects of an organization's threat or

defender perspectives (e.g., pointing to the threat component of one framework, the operations component of another framework, the governance component of a third framework). This allows the relative strengths of those resources to be complementary, preventing the gaps or organization-irrelevant aspects of those resources from being weaknesses.

3 Threat Modeling Framework

This section describes the threat modeling framework which underpins the Cyber Prep analysis and motivates the threat-oriented questionnaire. That analysis uses information about an organization to determine the characteristics of adversaries which could be expected to target its systems. The analysis then uses those characteristics to recommend levels for different aspects of preparedness. This section includes

- A high-level discussion of why an organization needs a threat model;
- A representative set of threat scenarios to be considered when constructing an organizational threat model;
- The framework for identifying (and assigning levels or nominal values to) adversary characteristics, consisting of terminology, definitions of levels, and relationships among adversary goals, scope, timeframe, persistence, stealth, and capabilities; and
- Examples of adversary profiles.

This material is intended primarily to help analysts understand the analysis guidance. However, it can also be used by organizational cybersecurity staff, in support of risk assessment.

3.1 The Need for an Organizational Threat Model

As the cyber threat ecosystem has grown in size and complexity, the number of threat reports, threat information sharing mechanisms, and frameworks for characterizing adversarial threats have increased. These sources can be overwhelming – *which ones are meaningful, and which are distracting?* The organization needs to articulate its assumptions about the adversarial threat[14] it faces, so that it can make effective use of these sources. One approach is to characterize the types of actors, as shown in Table 3-1, identifying typical goals for each class of adversary. It must be emphasized that this is a very rough characterization, useful for orientation but not for analysis, and that any real-world case study is likely to provide more nuanced characteristics of actors and their goals.

Table 3-1. Typical Threat Actors and Their Goals

Threat Class	Typical Actors	Typical Goals
Cyber Vandalism	Hackers, taggers, and "script kiddies;" small disaffected groups of the above	Obtain information or falsify records for personal gain. Disrupt and/or embarrass the victimized organization or type of organization based on personal agenda.
Cyber Incursion	Individuals or small, loosely affiliated groups; criminal teams; political or ideological activists; terrorists; insiders; industrial espionage; spammers	Obtain critical or resalable information and/or usurp or disrupt the organization's business or mission functions for profit or ideological cause.
Cyber Breach & Organizational Disruption	Nation-state sponsored team; professional organized criminal enterprise	Obtain critical or resalable information over an extended period. Increase knowledge of general infrastructure; plant seeds for future attacks; obtain or modify specific information and/or disrupt cyber resources, specifically resources associated with missions or even information types.

[14] Cyber Prep focuses on threat actors external to the organization. However, as illustrated in Appendix B, the set of adversary characteristics used in Cyber Prep can be mapped to those in an insider threat framework [87].

Threat Class	Typical Actors	Typical Goals
Cyber Espionage & Extensive Disruption	Professional intelligence organization or military service operative; sophisticated terrorist group; state-aligned professional criminal enterprise	Obtain specific, high value information; undermine or impede critical aspects of a critical infrastructure sector, mission, program, or enterprise; or place itself in a position to do so in the future.
Cyber-Supported Strategic Disruption	Nation-state military possibly supported by their intelligence service; very sophisticated and capable insurgent or terrorist group	Severely undermine or destroy an organization's mission capabilities or a nation's critical infrastructures, by disrupting or denying use of cyber resources (e.g., information, information and communications technology infrastructure, applications) and/or by undermining dependability and confidence.

However, such a characterization does not provide enough detail to inform an organization's strategic planning. The growth of the cyber threat ecosystem to include markets for malware and information about target organizations or technology enables motivated threat actors to acquire the capabilities they need to execute effective attacks. Therefore, the first questions for the organization to ask are:

- *Why might a cyber adversary target the organization?* An organization can be a direct target, due to its mission or business sector, the financial assets it controls, or the volume of salable or competitively useful information it handles. Alternately, an organization can be an indirect target, due to its relationship with one or more direct targets. A small set of representative high-level threat scenarios is presented in Section 3.2.
- *What goals would a cyber adversary have?* Adversary goals can include financial gain, personal motives, geopolitical advantage, or using the organization as a stepping stone in an attack on another target. Adversary goals are discussed in slightly more detail in Section 3.3.1, and are related to organizational concerns in Section 4.1.
- *At what scope or in what arena would such an adversary operate?* Depending on their goals, an adversary can operate against a subset of the organization's systems (e.g., its external-facing services); the organization's operations; the organization's associates (customers, users, or partners); the organization's critical infrastructure or industry sector; or the nation. Scope is discussed in more detail in Section 3.3.2.
- *In what timeframe would such an adversary operate?* Will the adversary's activities be periodic or episodic, or will the adversary commit to a sustained effort against the organization? Timeframe is discussed in more detail in Section 3.3.3.
- *What are the likely capabilities and resources of the adversary?* Are they minimal, causing the adversary to employ existing, known, malware? Or are they significant, allowing the adversary the benefit of being able to create their own malware, threat vectors, and possibly introduce vulnerabilities into the organization? Capabilities are discussed in more detail in Section 3.3.4.

The answers to these questions will drive different aspects of the organization's preparedness strategy. The organization may well have multiple answers to these questions, identifying multiple types of adversaries. Because different approaches address different types of adversaries, the organization may need to consider each type in developing strategic plans, rather than simply making a worst-case assumption. That is, the organization may develop a set of adversary profiles. Examples of adversary profiles are given in Section 3.5.

The organization can use the representative adversary characteristics shown in Table 2-1 to summarize its threat assumptions. Alternately, the organization can draw from relevant threat intelligence reports[15] to develop more specific descriptions of the adversaries it faces. In so doing, the organization can use the

[15] See Section 6.1 below for more information about how an organization can identify relevant sources of threat information.

characteristics described in the subsections below. In the general threat modeling construct of Capabilities, Intent, and Targeting in NIST SP 800-30R1, Goals and Timeframe have to do with Intent, while Scope has to do with Targeting. Timeframe determines several other adversary characteristics to be considered in an organization's preparedness strategy, specifically Persistence, Stealth, and the stages in the cyber attack lifecycle in which adversary activities can be expected. Capabilities are described last in this section, and in general terms, since in today's cyber threat landscape, a strongly motivated adversary with some financial resources can use malware and vulnerabilities marketplaces to increase technical capabilities.

Note that while Cyber Prep is consistent with the high-level risk model in NIST SP 800-30R1, it does not present a detailed threat model such as would be used in a risk assessment. The answers to the questions above, and the relationship of the answers to the five classes of adversaries, are designed to provide sufficient motivation for the selection of different approaches to aspects of an organization's cyber strategy. An organization would develop one or more detailed threat models (informed, as appropriate to its desired preparedness strategy, by threat intelligence and analysis) consistent with the use of risk assessment in the organization's security engineering orientation.

3.2 Motivating Threat Scenarios

A small set of highly general threat scenarios is used to motivate and organize the threat-oriented questionnaire:

- *An adversary obtains sensitive information from the organization's systems.* This scenario includes data breaches of personally identifiable information (PII), as well as large-scale exfiltration of proprietary information, trade secrets, or other highly sensitive information.
- *An adversary modifies or fabricates information on the organization's systems so that the organization will disburse money or transfer other assets at the adversary's direction.* This scenario focuses on fraudulent transactions.
- *An adversary modifies or fabricates software or configuration data on the organization's systems so that the adversary can direct their use (typically to resell capacity, as with botnet farms).* This scenario focuses on usurpation of resources, which is typically highly surreptitious.
- *An adversary modifies or destroys organizational assets in order to prevent the organization from accomplishing its primary mission.* This scenario includes adversary denial, disruption, or subversion of mission operations. It also includes ways in which an adversary deceives mission operators into taking mission-disruptive actions. While the details of attack scenarios related to denial, disruption, subversion, and deception can be quite different, those differences do not result in different targeting questions, the adversary characteristics resulting from different answers to the targeting questions, or the aspects of preparedness determined by those adversary characteristics.
- *An adversary compromises a supplier of the organization in order to increase the organization's vulnerability to attack.* This scenario includes attacks on partner organizations as well as those in the organization's supply chain.
- *An adversary disrupts organizational operations or fabricates information the organization presents to its constituency, damaging its reputation and the trust of its constituency.* This scenario is closely related to those involving disruption or denial of mission functions, but also includes modification of inessential but externally visible information or services in ways that undermine confidence in the organization.
- *An adversary compromises the organization's systems in order to attack downstream entities (e.g., customers, customers of customers).* Like the preceding scenario, this scenario is related to those involving disruption of mission functions. However, it is also related to scenarios involving acquisition of sensitive information, or fraudulent transactions.

- *An adversary modifies or incapacitates mission assets for financial gain (e.g., ransomware).* This scenario is closely related to those involving modification for purposes of fraud and for disruption or denial of mission functions.

The primary purpose of these scenarios in Cyber Prep is to determine what organizational characteristics could make an organization a target, and then what adversary characteristics can be inferred from those organizational characteristics. However, these high-level scenarios can also serve as starting points for the development of organization-specific scenarios, as part of risk assessment activities.

3.3 Adversary Characteristics

This subsection describes adversary characteristics used to determine recommended levels for different aspects of preparedness. These include goals, scope, timeframe, persistence, stealth, and capabilities.[16] Table A-1 in Appendix A provides a mapping from adversary characteristics to aspects of preparedness.

3.3.1 Goals

Adversary goals and timeframe (discussed below) are defining characteristics of an adversary's intent. Types of adversary goals include

- Financial gain. Specific goals include fraud or theft, acquisition of salable or usable personally identifiable information (PII) such as credit card numbers, acquisition of salable or usable competitive information, and extortion (e.g., via ransomware). Financial gain is typically associated with Cyber Incursion and Cyber Breach.
- Personal motives. Specific goals include attention (e.g., bragging rights in a hacking community, news coverage), malice (the desire to harm someone, some set of people, or the organization, e.g., via cyberstalking), and acquisition of PII about targeted individuals (e.g., via spearphishing). Personal motives are typical of Cyber Vandalism, but can also be associated with Cyber Incursion.
- Geopolitical advantage. Specific goals include undermining public confidence in government (e.g., data breaches, disruption of public services), terrorism, acquiring a national economic advantage (e.g., by acquiring competitive information related to a sector), acquiring and using a military advantage (e.g., by subverting military systems or by acquiring military plans), and acquiring and using an ability to threaten homeland security (e.g., by subverting critical infrastructure systems in such sectors as energy and telecommunications). Geopolitical advantage is typical of Cyber Espionage & Extensive Disruption and Cyber-Supported Strategic Disruption, but can also be associated with Cyber Breach & Organizational Disruption.
- Stepping-stone. The goal is to use the organization as an intermediate point in, or a launch point for, an attack on another target. Typical activities include acquiring information (e.g., about the organization's customers, users, or partners), compromising organizational systems on which other organizations depend, and tainting the supply chain.

These goals are not mutually exclusive. For example, in a compound attack [28], an adversary might compromise an organization's systems with the intent of acquiring financially valuable information, and then use those systems as a stepping stone in an attack on one of the organization's partners.

3.3.2 Adversary Scope

Depending on their goals, an adversary can operate with a narrow or broad scope, ranging from

[16] This threat modeling framework is deliberately incomplete. It provides enough modeling constructs to support risk framing, while accommodating the fact that different organizations will prefer different approaches to modeling adversary behavior or to characterizing specific types of adversaries.

- Very Narrow (Organizational Subset): A subset of the organization's systems or business functions (e.g., public-facing Web services). This will result in a *localized engagement* with the adversary.
- Narrow (Critical Organizational Operations or Targeted Information): Those organization's systems, infrastructure, or business functions that are critical to its operations or that handle specific information. The organization will need to deal with *structured campaigns*.
- Broad (Organizational Operations and Associates): Any of the organization's systems, infrastructure, or business functions, as well as the organization's customers, users, or partners. The organization will need to deal with *structured campaigns, including campaigns that span organizational elements or multiple organizations*. The organization will need to work out *agreements for information sharing, and possibly coordination*.
- Strategic (Sector or Community): Interdependent critical infrastructure or industry sector systems, or set of systems spanning multiple organizations to accomplish a collective mission. The organization will need to consider *participating in an ongoing body or community*, for information sharing and common defense.
- Broadly Strategic (National or Transnational): Systems critical to the nation or to interrelated infrastructure or industry entities. The organization will need to consider how it will *interact with national-level cyber defense efforts*.

The range of scopes corresponds to the contexts identified in Figure 1-3. The scope of adversary activities will drive the organization's strategy for information sharing and coordination. Note that many organizations become aware of adversary activities across a sector via commercial reporting (e.g., [28]).

3.3.3 Adversary Timeframe

The timeframe in which an adversary operates is driven by their goals and scope, and implies answers to three additional questions: *How persistent is such an adversary likely to be? How concerned is such an adversary likely to be about revealing their capabilities? How can adversary activities best be modeled?* Three general timeframes can be identified:

- Episodic. Adversary activities are limited in duration, in order to achieve a specific effect or goal – or to determine that the intended effect cannot be achieved without sustained effort. Episodic operations can be one-time attacks, or the adversary can perform them periodically or in response to triggering events.

  Episodic operations imply no or limited persistence, and no concern for revealing capabilities. Adversary activities can be characterized using a taxonomy of consequences (e.g., loss of confidentiality, integrity, or availability).

- Sustained. Adversary activities occur over an extended time period (e.g., months to a couple of years), requiring the adversary to make sustained investments of time, effort, or other resources.

  Sustained operations imply persistence, involving a series integrated cyber-attacks resulting in a cyber campaign. The adversary's need for a sustained attack will likely mean that they are going to be stealthy to avoid premature disclosure of their presence or tactics, techniques, and procedures (TTPs), and may seek to conceal some of the consequences of their actions. Adversary cyber activities can be structured or described using a cyber attack lifecycle, cyber campaign, or cyber kill chain model; activities internal to the organization's systems can be described using a categorization such as ATT&CK [29].

- Enduring. Adversary activities occur over a significant time period (several years, or into the future without bounds) and with a scope that require the adversary to define an investment strategy and a strategic plan for achieving goals.

Enduring operations imply a high degree of persistence. They also imply a high level of concern for revealing capabilities and strategy; the adversary may use deception as well as stealth. They may include supply chain attacks.

The following table summarizes, for each class of adversary, the *typical* timeframe, persistence, and concern for stealth; in addition, the stages in the cyber attack lifecycle are identified.[17]

Table 3-2. Adversary Timeframe and Related Characteristics

Class	Timeframe	Persistence	Stealth	CAL Stages
Cyber Vandalism	One-time or Episodic	None	No concern for stealth, although some concern for attribution is possible	Deliver, Exploit, Execute
Cyber Incursion	Episodic or Sustained	Limited, with near-term (tactical) planning	Limited concern, focused on concealing evidence of presence	Recon, Deliver, Exploit, Execute
Cyber Breach & Organizational Disruption	Sustained	Persistent, with planning for a cyber campaign	Moderate concern, focused on concealing evidence of presence, TTPs, and capabilities	All, but Weaponize is limited
Cyber Espionage & Extended Disruption	Sustained or Enduring	Strategically Persistent, with long-term planning for multiple campaigns	High concern, focused on concealment and deception; may use OPSEC	All
Cyber-Supported Strategic Disruption	Enduring	Strategically Persistent, with long-term planning for multiple coordinated campaigns	Very high concern; may use OPSEC, counterintelligence, and partnerships or other relationships	All, including multiple CALs (e.g., cyber, supply chain, physical or kinetic)

3.3.4 Adversary Capabilities

Adversary capabilities can generally be characterized in terms of *resources* that can be directed or allocated, and *methods* (pre-planned applications of resources), as shown below. In a more detailed threat model, more information on methods would be represented, e.g., by using attack patterns, CAL stages, and threat scenarios.

Table 3-3. Adversary Capabilities

Capability	Typical of Class	Resources	Methods
Acquired	Cyber Vandalism	The adversary has very limited resources or expertise of their own.	The adversary tends to employ malware, tools, delivery mechanisms and strategies developed by others.
Augmented	Cyber Incursion	The adversary some expertise and limited resources of their own.	The adversary builds upon known vulnerabilities and publicly available malware, to augment, configure, and modify existing malware.
Developed	Cyber Breach & Organizational Disruption	The adversary has a moderate degree of resources and expertise.	The adversary discovers unknown vulnerabilities, and develops their own malware (e.g., zero day) utilizing those vulnerabilities, and their own delivery mechanism. Alternately, the adversary purchases vulnerability information and tailored malware.

[17] The organization can also find it useful to characterize adversary attack patterns. For Cyber Vandalism, typical cyber effects can help to motivate good practices; for Cyber Incursion, common attack vectors such as those identified in CAPEC can be helpful in assigning relative priorities to additional controls; and for the remaining (APT) adversary classes, cyber defenders and system architects can use CAL or CKC stages and ATT&CK as part of analyzing which defensive methods, security controls, and architectural decisions promise the most effectiveness against the adversary.

Capability	Typical of Class	Resources	Methods
Advanced	Cyber Espionage & Extended Disruption	The adversary has a significant degree of resources and expertise.	The adversary "influences" commercial products and services (or free and open source software) during design, development, manufacturing, or acquisition (supply chain), allowing them to introduce vulnerabilities into such products.
Integrated	Cyber-Supported Strategic Disruption	The adversary is sophisticated and very well resourced.	The adversary generates its own opportunities to successfully execute attacks that combine cyber and non-cyber threads in support of a larger, non-cyber goal.

Because Cyber Prep is intended for use at the Organizational Tier (and, to a lesser extent, at the Mission/Business Function Tier) of the NIST SP 800-39 multi-tiered approach to risk management, it does not include further details on adversary capabilities and behavior. Specific capabilities (e.g., technical expertise) and behavior (e.g., TTPs) are tactical characteristics of the adversary, and may change more quickly than can be represented in an organizational strategy.[18] As an organization executes a threat-informed and anticipatory cyber preparedness strategy, it may need to develop more detailed threat models that include specific types of capabilities (e.g., relationships, intelligence, financial or technical resources) and behavior (e.g., attack patterns or TTPs, including non-cyber or partially cyber as well as fully cyber TTPs). Alternately, it can rely on shared threat intelligence.

3.4 Examples of Adversary Profiles

A few examples of adversary profiles for a notional single organization (a large company with significant intellectual property, which – by virtue of the services it provides – has connections into the internal networks of multiple customers) are given in the following table.[19] As noted in Table A-1, different adversary characteristics can motivate different aspects of an organization's cyber preparedness strategy. The organization can treat the adversary in the first example as a cautionary tale (used in an anonymized way in Training & Readiness), to motivate better implementation of Cyber Hygiene. Particularly if the organization's customers are important players in a critical infrastructure sector, the adversary in the second example can motivate changes in Governance to provide a higher degree of External Coordination. Finally, the adversary in the third example can motivate a transition from the organization's current preparedness posture to one of Architectural Resilience, including transformations across the areas of Operations and Architecture & Engineering.

Table 3-4. Examples of Adversary Profiles

Adversary	Class	Characteristics
Disaffected former employee [30]	Cyber Incursion	**Goals**: Personal motives – embarrass or stalk former co-workers **Scope**: Organizational Subset – email and messaging services **Timeframe, Persistence, and Stealth**: Episodic, limited planning, moderate concern for concealing methods **Effects**: Fabricated messages; non-physical harm to targeted individuals **Capabilities**: Use credentials (userid and password) which were not decommissioned when the employee was terminated; perform spear-phishing of former co-workers to obtain their credentials

[18] Some TTPs can be characterized in such a way that they can serve as the basis for specific countermeasures; see, for example, the list of attack types in [39].

[19] A larger set can be found in Intel's Threat Agent Library [124] [125].

Adversary	Class	Characteristics
Criminal organization [31]	Cyber Breach	**Goals**: Stepping-stone **Scope**: Organizational Associates; Sector **Timeframe, Persistence, and Stealth**: Sustained with persistent, stealthy activities in most stages of CAL: recon, deliver, exploit, control, execute, maintain **Effects**: Establish foothold for attacks on a customer organization **Capabilities**: Adversary developed malware
APT team [32]	Cyber Espionage & Extended Disruption	**Goals**: Economic advantage **Scope**: Organizational Operations; Sector **Timeframe, Persistence, and Stealth**: Sustained with persistent, stealthy activities in all stages of CAL **Effects**: Extensive or repeated data breaches, Extensive or repeated DoS **Capabilities**: Malware crafted to the target environment, and maintain long-term presence in systems

4 Identify Concerns

Activities of cyber adversaries – whether or not they are successful – can have multiple consequences for an organization.[20] Based on the characteristics of the adversary (or set of adversaries) an organization seeks to be prepared for, it can identify and prioritize its concerns in three ways.

4.1 Cyber Effects and Organizational Consequences

First, an organization can consider the degree of organizational or operational consequences of successful adversary activities targeting the organization. In effect, the organization asks: *How much of an impact would successful achievement of adversary goals have?*[21] This question applies to all classes of adversaries. Degrees of consequences can range from

- **Limited or near-term**: Little or no impact on critical mission operations. Consequences can be handled within an operational planning or funding cycle (e.g., within a business quarter) or within the duration of a mission operation.
- **Extensive or mid-term**: Significant impact on critical mission operations, the organization, or its associates. Consequences require remediation or mitigation efforts that extend across operational planning or funding cycles.
- **Severe or long-term**: Extremely significant, potentially catastrophic impact on mission operations, the organization, or its associates. Consequences are of a duration or extent that must be considered by strategic planning.

To understand how significant the effects of an adversary attack on or campaign against the organization might be, the organization needs to consider the cyber effects [33], whether those effects apply to critical or non-critical resources, and what the associated consequences might be.[22] Table 4-1 provides a starting point.[23]

Table 4-1. Typical Cyber Effects and Organizational Consequences

Adversary Goal	Typical Cyber Effects	Typical Organizational Consequences
Financial gain		
• Fraud against or theft from the organization	Corruption, Modification, or Insertion	Financial loss, Reputation damage
• Acquire salable / usable PII (e.g., credit card numbers)	Exfiltration, Interception	Liability due to non-physical harm to individuals, Reputation damage
• Acquire salable / usable competitive information (e.g., intellectual property, plans, information about customers or partners)	Exfiltration, Interception	Liability due to failure to meet contractual obligations, Loss of future competitive advantage
• Extortion	Degradation or Interruption Corruption, Modification, or Insertion Exfiltration	Financial loss (ransom paid to avert denial-of-service, destructive malware, adversary release of sensitive information)

[20] "Along with the rapidly expanding "digitization" of corporate assets, there has been a corresponding digitization of corporate risk. Accordingly, policymakers, regulators, shareholders, and the public are more attuned to corporate cybersecurity risks than ever before. Organizations are at risk from the loss of IP and trading algorithms, destroyed or altered data, declining public confidence, harm to reputation, disruption to critical infrastructure, and new legal and regulatory sanctions." [3]
[21] An alternative question is, "What does the organization have to lose?" [10]
[22] Multiple taxonomies or lists of possible organizational consequences are available. The typical organizational consequences in Table 4-1 are derived in part from [93] [27] [103].
[23] A more nuanced approach to classifying and estimating disruptive cyber effects on an organization is provided in [123].

Adversary Goal	Typical Cyber Effects	Typical Organizational Consequences
• Fraud against or theft from the organization's customers, suppliers, or partners	Unauthorized use	Financial loss (indirect, through theft of services), Reputation damage, Liability
Personal motives		
• Attention	Degradation, Interruption Corruption, Modification, or Insertion	Reputation damage
• Malice	Degradation, Interruption Corruption, Modification, or Insertion	Reputation damage, Liability due to physical or non-physical harm to individuals
• Acquire PII about targeted individuals	Exfiltration, Interception	Reputation damage, Liability due to non-physical harm to individuals
Geopolitical advantage		
• Undermine public confidence in government	Degradation, Interruption Corruption, Modification, or Insertion Exfiltration, Interception	Physical or non-physical harm to individuals, Reputation loss
• Terrorism	Degradation, Interruption	Physical or non-physical harm to individuals, Reputation loss
• Acquire information that improves national economic advantage	Exfiltration, Interception	Loss of future competitive advantage
• Acquire / use military advantage	Degradation, Interruption Corruption, Modification, or Insertion	Military mission failure, Loss of future military advantage
• Acquire / use ability to threaten homeland security	Degradation, Interruption Corruption, Modification, or Insertion	Homeland security mission failure, Loss of future capabilities abilities
Positional / Stepping Stone		
• Acquire a launching point for targeted attacks	Corruption, Modification, or Insertion Unauthorized use	Reputation damage, Liability due to harm to other entities
• Acquire resources that can be used in targeted attacks (e.g., DDoS)	Unauthorized use	Reputation damage, Liability due to harm to other entities
• Acquire intelligence about other entities	Exfiltration, Interception	Liability due to harm to other entities

4.2 Disruption from Adversary Activities

Second, an organization can consider the consequences of adversary activities targeting the organization, whether or not those activities result in adversary success. In effect, the organization asks: *How much disruption would adversary activities cause?* For *conventional threats*, disruption is largely a function of the scope of the adversary's operation, and results either directly from the adversary achieving one or more of their intended cyber effects, or indirectly from the organization's efforts to mitigate those effects. Data breach remediation is the primary concern [34]. However, disruption due to ransomware is also a concern; for example, if an adversary succeeds in disseminating and executing destructive malware across the organization, that disruption affects organizational operations directly; if an adversary succeeds in disseminating destructive malware across the organization and then threatens to detonate it on a certain date, the organization's remediation efforts (e.g., shutting down devices, isolating portions of the network) could have indirect effects on organizational operations.

For *advanced threats*, in which the adversary executes a campaign against the organization, the organization needs to look not only at the ultimate effects of a cyber attack, but also at intermediate effects of activities during the Control stage of the cyber attack lifecycle, such as establishing command

and control (C2) channels. To do so, the organization can use any of a variety of models of the cyber attack lifecycle or cyber kill chain.[24] These models allow the organization to characterize the activities that an adversary might carry out, and to define aspects of its strategy for Operations and Architecture & Engineering. One model is represented in Figure 2-2.

4.3 Stepping-Stone Attacks

Third, an organization might consider whether it could be an indirect target. The organization asks: *Which of our customers or partners could be high-value targets for an adversary?* Stepping-stone attacks – attacks designed to acquire and maintain a foothold in one organization's systems, as a launching point for attacks on another organization – could be a concern for an organization which otherwise views its adversary class as Cyber Vandalism.[25]

For example, subversion of the supply chain for a key component in a critical infrastructure – a goal characteristic of Cyber Espionage & Extensive Disruption or Cyber-Supported Strategic Disruption– could involve an attack on a small organization, which develops, sells, and maintains a piece of utility software used in many development environments. By modifying that utility, the attacker could obtain access to multiple development environments and thus could have the opportunity to modify the critical infrastructure component.

It is unrealistic to expect a small organization with one product to prepare for an adversary with the capabilities associated with Cyber Espionage & Extensive Disruption or Cyber-Supported Strategic Disruption.[26] However, stepping-stone attacks can leave an organization liable to contractual or other legal action. By identifying stepping-stone attacks as a concern, an organization can see how some aspects of Governance and Operations that it might otherwise view as unnecessary should be part of its cybersecurity strategy.

[24] The recognition that attacks or intrusions by advanced cyber adversaries against organizations or missions are multistage, and occur over periods of months or years, has led to the development of models of the cyber attack lifecycle. A model of the cyber attack lifecycle is frequently referred to as a "cyber kill chain." An initial cyber kill chain model was developed by Lockheed Martin [25] [88]. For more on cyber attack lifecycle models, see Appendix B of [90]. The model represented in Figure 2-2 is consistent with NIST SP 800-30R1 [26] and DoD guidance [89].

[25] The 2015 Verizon Data Breach Investigation Report [28] observes: "One of the most interesting changes in the threat actor category came to light when we started looking deeper into compound attacks (those with multiple motives). Last year, we added a motive to the Vocabulary for Event Recording and Incident Sharing (VERIS) called "secondary" to better track these. We use it in combination with a primary motive to indicate that the victim was targeted as a way to advance a different attack against another victim. Strategic web compromises are a good example. In these campaigns, a website is hacked to serve up malware to visitors in hopes that the actor's true target will become infected. The actors have no real interest in the owner of the website other than using the owner to further the real attack. In this year's data set, we found that nearly 70% of the attacks where a motive for the attack is known include a secondary victim. The majority of these were not from espionage campaigns (thankfully), but from opportunistically compromised servers used to participate in denial-of-service (DoS) attacks, host malware, or be repurposed for a phishing site."

[26] Small and medium sized enterprises are increasingly aware of the APT [91] [93], but existing frameworks and guidance assume an organization large enough to have an information security program. Guidance has been offered on how small and medium sized enterprises can deal with cyber risk [118] [119] or the APT [92].

5 Define the Organization's Cyber Preparedness Strategy

This section describes the framework for characterizing organizational cyber preparedness which underpins the Cyber Prep analysis and motivates the preparedness-oriented questionnaire.

An organization's cyber preparedness strategy is based on the adversary (or set of adversaries) that could affect its operations and future viability. Cyber Prep identifies aspects of preparedness in three areas: Governance, Operations, and Architecture & Engineering. An organization can use Cyber Prep to assess its current preparedness and to define its target cyber preparedness strategy. This initially can be done at a high level, using Tables 2-1 and 2-2 to define the organization's overall threat orientation, and Table 2-3 to characterize its current or desired preparedness strategy. In terms of Figure 2-1 and Figure 5-1 below, that high-level definition and characterization are designed to *identify mismatches between adversary & preparedness strategy*.

To *clarify assumptions and key areas of preparedness*, the organization can use the material in Sections 3 and 4 to make a clearer characterization of the threat and organizational concerns. The organization can use the more specific statements in Tables 5-1 through 5-3 to perform a self-assessment, asking: *Are these statements about the organization true? What evidence supports those claims?* The statements in these tables provide a starting point for articulating an organizational strategy.

To *articulate its strategy*, the organization will need to drill down, using the aspects of Governance, Operations, and Architecture & Engineering illustrated below and presented in Appendix A to define its desired preparedness strategy more precisely. The organization can tailor the statements, particularly for the specific aspects, to its mission, sector, governance structure, and operational processes. For example, within Governance for Responsive Awareness, the tailored statement could identify the corporate officer or agency official.

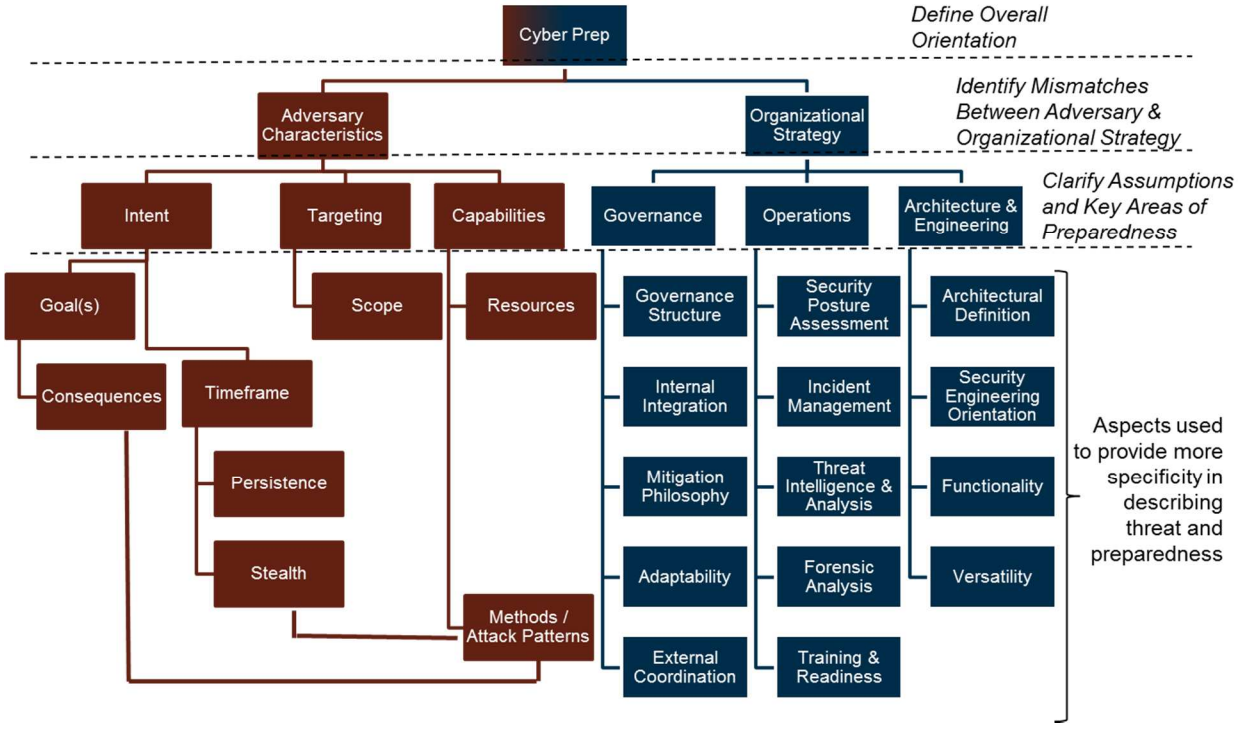

Figure 5-1. Cyber Prep Framework in Detail

The statements for aspects of an organization's cyber preparedness strategy range from weaker (in terms of ability to face a range of adversaries, and in terms of the organizational commitment and resources required) to stronger. However, Cyber Prep is not a Capability Maturity Model – an organization could, for example, select a target of Responsive Awareness Governance and Operations, but Critical Information Protection Architecture. Within each area, an organization can decide that some aspects should be targeted higher than others (e.g., within Governance, an organization might target Coordination for Internal Integration, but Risk Managed for Mitigation Philosophy and Limited Alternatives for Adaptability). However, an organization should be sure to look for potential inconsistences, due to linkages among the aspects.

Governance Is Fundamental to Effective Preparedness

One important linkage must be emphasized: The overall approach to Governance should be at least as strong as the approach to Operations, which in turn should be at least as powerful as the approach to Architecture & Engineering. An organization that seeks to improve its overall cybersecurity often starts by acquiring cybersecurity products and tools, and then abandoning them because it lacks the expertise or sufficient staff to use them effectively. Thus, without adequate resources in Operations, Architecture will fail to realize its promises. Similarly, cybersecurity staff in an organization that has not made a commitment to managing cybersecurity risk will be overburdened, often asked to perform security tasks as an additional duty, or will be under-resourced. Thus, without an organizational commitment to Governance, Operations will be unsatisfactory.

One aspect of Governance relates to law enforcement. Many organizations first learn of a breach when they are notified by law enforcement, either because the breach resulted in the loss of information in the organization's custody or because the organization's resources are being used to attack another organization (i.e., the organization has been the target of a positional or stepping stone attack). Thus, regardless of the organization's assumptions about the class of adversary that might attack it, as part of its governance responsibilities any organization should have identified a law enforcement point of contact.

Tables 5-1 through 5-3 are a summary of representative strategies; details of the different aspects of strategy are presented in Appendix A:

- Governance, in A.1, includes Governance Structure, Internal Integration, Mitigation Philosophy, Adaptability, and External Coordination.
- Operations, in A.2, includes Security Posture Assessment, Incident Management, Threat Intelligence & Analysis, Forensic Analysis, and Training & Readiness.
- Architecture & Engineering, in A.3, includes Architectural Definition, Security Engineering Orientation, Functionality, and Versatility.

See Table 5-4 for a capsule summary.

Table 5-1. Governance

Strategy	Governance Summary
Basic Hygiene	**Cybersecurity processes are ad-hoc and informal and not integrated with other disciplines. Efforts focus on compliance with standards of good practice. Only ad hoc processes exist to deal with disruption of decision making. Information sharing is limited to ICT staff.**
Critical Information Protection	**A Security Program Officer is engaged in information security decisions. Physical security**, **personnel security, and business continuity are** aligned with **cyber** security**.** Efforts focus on compliance with standards of good practice, **in the context of broader risk management. Informal** processes deal **with short term** disruption of decision making. **Cybersecurity personnel share information with counterparts in partner and supplier organizations in support of shared threat/incident awareness.**
Responsive Awareness	**A responsible corporate officer or agency official is actively engaged in enterprise-level cyber security decisions**. Physical security, personnel security, business continuity, **ICT architecture, and operations security are integrated** with cyber security. **Cybersecurity includes conformance** with standards of good practice, **but pushes the state of the practice to address the APT. A defined and implemented** process deals with disruption of **critical aspects** of decision making. **Cybersecurity staff cooperate** with counterparts **in peer, partner,** supplier**, and customer** organizations in support of shared threat/incident awareness**.**
Architectural Resilience	A **dedicated** corporate officer or agency official is actively engaged in enterprise-level cyber security decisions. Physical security, personnel security, business continuity, **supply chain risk management (SCRM)**, ICT architecture, **business process engineering**, operations security, **and cyber security are integrated with mission assurance.** Cybersecurity **builds on** standards of good practice, but pushes the state of the practice **by incorporating state of the art techniques, sometimes at the expense of non-compliance with standards of good practice. Processes are implemented and exercised** to deal with **long term** disruption of **key** aspects of decision making. **Cyber defense and strategic planning** staff **coordinate** with counterparts in peer, partner, supplier, and customer organizations in support of a shared threat/incident awareness **response.**
Pervasive Agility	**The CEO or Agency head** is actively engaged in **mission assurance** decisions. Physical security, personnel security, business continuity, SCRM, ICT architecture, business process engineering, operations security, and cyber security **collaborate to ensure** mission assurance. Cybersecurity builds on standards of good practice, but pushes **the state of the art to ensure continued security evolution in the face of an innovative adversary. Adaptable** processes are implemented and exercised to deal with long term **severe** disruption of key aspects of decision making processes. Cyber defense and strategic planning staff **collaborate** with cybersecurity counterparts in **other organizations in the organization's mission or critical infrastructure sector, as well as in** peer, partner, supplier, and customer organizations in support of a shared threat/incident awareness **preparation and** response.

Table 5-2. Operations

Strategy	Operations Summary
Basic Hygiene	**The organization invests minimal effort to understand its security posture. Cybersecurity staff respond to incidents, based on detection of Execute activities. Cybersecurity staff review threat intelligence reports on an intermittent, ad hoc basis. Cybersecurity staff perform reactive, after-the-fact analysis damage assessments. Cybersecurity staff and users receive training and awareness materials.**
Critical Information Protection	The organization **scans and monitors cyber resources on an ongoing basis**. Cybersecurity staff respond to incidents, based on detection of **activities in the Exploit and** Execute stages, **and to indications and warnings related to Recon and Control activities.** Cybersecurity staff review threat intelligence reports on an **ongoing** basis, **to identify relevant current threats or attack patterns.** Cybersecurity staff **support** after-the-fact analysis of damage assessments **and support external organizations doing malware analysis.** Cybersecurity staff and users receive **tailored** training and awareness materials. **Cybersecurity staff develop contingency plans, based on relatively static threat intelligence.**
Responsive Awareness	The organization scans and monitors cyber resources on an ongoing basis, **using updated threat information.** Cybersecurity staff **manage** incidents **relying on** indications and warnings **for activities throughout the cyber attack lifecycle**. Cybersecurity staff review threat intelligence reports on an ongoing basis, to identify relevant current **or future** threats or attack patterns. Cybersecurity staff **perform** after-the-fact analysis of damage assessments and **malware analysis.** Cybersecurity staff and users receive tailored training and awareness materials; and **coordinate with business continuity planners to** develop **integrated** contingency plans, based on relatively static threat intelligence**.**
Architectural Resilience	The organization **maintains situational awareness (SA) of its cyber resources and of the changing threat.** Cybersecurity staff manage events **jointly with cyber defenders who execute and adapt courses of action** throughout the cyber attack lifecycle**. Cyber defenders analyze** threat intelligence reports on an ongoing basis. **An integrated team of cyber defenders, including threat and forensic analysts, as well as tool developers, work together to detect, analyze and develop effective and timely courses of action against malware**. Cybersecurity staff and users receive tailored training and awareness materials **including those based on threat intelligence updates**; and coordinate with business continuity planners to develop contingency **and continuity of operations (COOP)** plans, **coordinating with cyber defenders and mission owners**.
Pervasive Agility	The organization **integrates cyber SA with mission SA, so that the mission implications of the cybersecurity posture can be understood and managed.** Cybersecurity staff manage events jointly with cyber defenders who execute and adapt courses of action throughout the cyber attack lifecycle. Cyber defenders analyze threat intelligence reports on an ongoing basis; **defining and using new threat analytic methods.** An integrated team of cyber defenders, including forensics analysts and threat analysts, as well as tool developers, work together to detect **(using organization developed forensics analysis methods),** analyze and develop effective and timely courses of action against malware. Cybersecurity staff and users receive tailored training and awareness materials including those based on threat intelligence updates**. Contingency plans, COOP plans, and cyber courses of action are jointly developed, to minimize mission disruption when executed.**

Table 5-3. Architecture & Engineering

Strategy	Architecture & Engineering Summary
Basic Hygiene	**The security architecture is informally defined, and focuses on the enterprise perimeter, and on selected internal security capabilities. Security engineering activities are informed by generally accepted standards of basic good practice for information security. Cybersecurity capabilities focus on the areas of Protect, Detect, and Respond. The organization has very few options for tailoring or extending its architecture to improve security.**
Critical Information Protection	The security architecture focuses on the enterprise perimeter, selected internal security capabilities**, and data loss prevention**. Security engineering activities are informed by enterprise standards, based on **standards of good practice** for information security. Cybersecurity capabilities focus on the areas of Protect, Detect, Respond**, and Recover**. The organization has **limited** options for tailoring or extending its architecture to improve security.
Responsive Awareness	The security architecture **is defined, to enable analysis of mission dependencies on and interactions with security capabilities**. Security engineering activities are informed by **analysis of security risks and potential effectiveness of alternative risk mitigations**. Cybersecurity capabilities focus on the areas of **Identify**, Protect, Detect, Respond, and Recover, **complemented with capabilities that provide some support to a limited set of cyber resiliency objectives.** The organization has **multiple** options for tailoring or extending its architecture to improve **cybersecurity; and some limited options for providing and improving cyber resiliency.**
Architectural Resilience	The security architecture is defined, to enable **analysis of cyber resiliency and mission resiliency capabilities, including those that involve dependencies on organization-external systems.** Security engineering activities are informed by analysis of **mission** risks and potential effectiveness of alternative risk mitigations. Cybersecurity capabilities **include those needed to support the full range of cybersecurity functional areas and most cyber resiliency objectives.** The organization has multiple options for tailoring or extending its architecture to improve cybersecurity **and cyber resiliency.**
Pervasive Agility	The security architecture is defined, to enable analysis of cyber resiliency and mission resiliency capabilities, including those that involve dependencies on **or interactions with** organization-external systems. Security engineering activities are informed by analysis of mission risks and potential effectiveness of alternative risk mitigations**, in the context of future strategic plans as well as current and anticipated mission needs**. The cybersecurity capabilities employed includes those needed to support the full range of cybersecurity functional areas and **all** cyber resiliency objectives. The organization has multiple options for tailoring or extending its architecture to improve cybersecurity, cyber resiliency, **and cyber defense, including the use of multiple architectures, tailored to different environments.**

Table 5-4 provides a key to the different aspects of the five overarching preparedness strategies. Once again, it must be emphasized that no organization can or should be expected to apply a given preparedness strategy in a uniform manner; the specific aspects must be selected based on the organization's risk management strategy and the threats the organization faces.

Table 5-4. Summary of Aspects of Preparedness Strategies

		Preparedness Strategy				
Area	**Aspect**	**Basic Hygiene**	**Critical Information Protection**	**Responsive Awareness**	**Architectural Resilience**	**Pervasive Agility**
Governance	Governance Structure	Ad hoc	Basic	Proactive Management	Continuously Improving	Intelligently Evolving
	Internal Integration	None	Friction Avoidance	Cooperation	Coordination	Collaboration
	Mitigation Philosophy	Compliance	Risk Aware	Risk Managed	Innovation Adoption	Innovation Leadership
	Adaptability	No Alternatives	Limited Alternatives	Established Alternatives	Exercised Alternatives	Adaptable Alternatives
	External Coordination	Informal	Avoidance of Imposed Risks	Cooperation	Coordination	Collaboration
Operations	Security Posture Assessment	Minimal	Ongoing Scanning & Monitoring	Threat-Informed Scanning & Monitoring	Cyber Situational Awareness	Integrated Mission Situational Awareness
	Incident Management	Ad hoc Response	Incident Response	Incident Management	Resilient Courses of Action	Integrated Defensive Operations
	Threat Intelligence & Analysis	Intermittent	Ongoing	Proactive	Integrated	Innovative
	Forensic Analysis	Reactive	Enabled	Proactive	Integrated	Innovative
	Training & Readiness	Training & Awareness	Risk-Informed Training & Awareness	Informed Readiness	Coordinated Readiness	Integrated Readiness
Architecture & Engineering	Architectural Definition	Basic	Data-Centric	Capability-Centric	Mission-Centric	Extensive
	Security Engineering Orientation	Compliance	Consequence	Information Security Risk	Mission Risk	Integrated Risk
	Functionality	Basic Cybersecurity	Moderate Cybersecurity	Full Cybersecurity	Cyber Resiliency	Extended Cyber Resiliency
	Versatility	Brittle	Rigid	Tailorable	Adaptable	Highly Evolvable

6 Select and Use Appropriate Resources

An organization can draw upon several types of resources as it defines and implements its cyber preparedness strategy. These include frameworks, guidelines, and threat information sharing efforts.

A growing number of cybersecurity or resilience frameworks are available to organizations. These frameworks define process or functional areas, identify controls to apply or measures to take in those areas, and sometimes provide a maturity model. Examples include the NIST Cybersecurity Framework, the CERT Resilience Management Model, the JTF risk management framework (RMF), and several cybersecurity maturity models [13] [15] [8] [19]. (See [35] for a survey of cybersecurity maturity models for critical infrastructure providers.) In addition, several frameworks for characterizing cyber threats are available [27] [29] [36] [37]. Appendix B describes the relationship between Cyber Prep and a variety of frameworks.

An organization's ability to select or use a cybersecurity, resilience, or threat framework can be limited or determined by its resources; its organizational culture; its sector, its mission, or its business model; and/or its risk frame [3]. Some CI sectors provide tailored versions of the CSF; for example, the Federal Financial Institutions Examination Council (FFIEC) has created its Cybersecurity Assessment Tool [8] for the financial sector, while the Department of Energy (DoE) has created implementation guidance for the CSF in the energy sector [9], and the Health Information Trust Alliance has defined an CSF-based maturity model for the healthcare sector [11].

Most frameworks are too large or complex for many organizations – particularly small-to-medium-sized enterprises – to adopt completely. Using Cyber Prep, an organization can select the relevant portion(s) of one or more cybersecurity or resilience frameworks. The five Cyber Prep strategies (and, as needed, specific aspects of Governance, Operations, and Architecture & Engineering) can be used to index into another framework, so that an organization can identify a starting point for using that framework in defining its cybersecurity strategy.

NIST publishes guidance on a wide spectrum of cybersecurity topics in its 800 and 1800 series of Special Publications. The series of publications by the Joint Transformation Initiative (JTF) – including NIST SP 800-39 [6], NIST SP 800-53R4 [38], and NIST SP 800-30R1 [26] – include consideration of the APT and cyber resiliency. However, organizations using those publications can restrict themselves to non-APT threats based on their risk framing.

The Critical Security Controls [39] address a combination of conventional and APT actors. For threat-informed and anticipatory Operations, guidance for Security Operations Centers (SOCs, [40]) or incident management can be useful.

The number and variety of threat information sharing efforts continues to increase. Efforts range from commercially published threat intelligence reports by large cybersecurity or Internet Service Provider (ISP) companies (e.g., Symantec, Mandiant, Kaspersky, Tripwire; Verizon), to sector-specific Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs), to regional consortia such as the Advanced Cyber Security Center (ACSC, [41]). An organization can use its characterization of the cyber adversaries it faces to make more effective use of such resources. An organization's cyber preparedness strategy includes two aspects that determine the type of information sharing it uses: External Coordination (part of Governance) and Threat Intelligence & Analysis (part of Operations).

7 Notional Worked Example

This subsection provides a notional worked example, applying Cyber Prep to a large regional logistics company (which falls in the Transportation Systems CI sector[27]). The company might initially consider orienting toward a conventional threat; given its size, it would at least expect Cyber Incursion. However, by virtue of its size, the company plays a key role in the supply chains of large organizations in multiple CI sectors.[28] Those customers need to worry about Cyber Disruption & Espionage.

Based on its role in the supply chain, the company leadership realizes the company needs to orient at least to Cyber Breach, and possibly to Cyber Disruption & Espionage, and therefore to define a strategy based on Responsive Awareness, with some aspects drawn from Architectural Resilience (particularly with respect to Governance). However, as the company leadership looks at the descriptions in Tables 2-3 and 5-1 through 5-3, they realize that the company currently has a hybrid of the Basic Hygiene and Critical Information Protection strategies toward Governance and Operations, and that (due to the way the company has evolved over time, via mergers, acquisitions, and spin-offs) its strategy in the area of Architecture & Engineering is one of Basic Hygiene.

As noted in Section 5, changes in aspects of Operations and Architecture & Engineering require senior leadership commitment. Therefore, the company's first step is to improve its Governance Structure, ensuring that cybersecurity becomes part of the responsibilities of a corporate officer. (This is part of transitioning from Critical Information Protection to Responsive Awareness; at Architectural Resilience, a *dedicated* corporate officer is called for, but company leadership opts for an evolutionary change.) That officer plans to use the CSF[29], and does not want to complement its use with any maturity model at this time. To achieve Architectural Resilience, the company might ultimately seek to achieve Tier 4 (Adaptive) in the CSF Framework Implementation Tiers, but evolution in that direction will take time. Initially, the goal will be to achieve at least Implementation Tier 2.

The CSF defines 22 Categories and 97 Subcategories within the five ongoing functions of Identify, Protect, Detect, Respond, and Recover. The prospect of creating a Current Profile using the CSF – that is, identifying which Category and Subcategory outcomes from the Framework Core the company currently achieves – seems daunting to the Preparedness Improvement Team that the officer appoints to determine the desired preparedness strategy and identify topics to be addressed in the strategic roadmap. They begin by developing a Cyber Prep profile: for each of the fourteen aspects of a preparedness strategy, they look at the descriptions of the alternative approaches, and determine which description best fits the company, based on answers to the preparedness questionnaire. The results of their assessment are illustrated in the table below.

Table 7-1. Initial Assessment

Aspect	Current Approach
Governance	
Governance Structure	Basic, but moving toward Proactive Management
Internal Integration	Friction Avoidance with respect to other security disciplines
Mitigation Philosophy	Compliance
Adaptability	No Alternatives
External Coordination	Informal
Operations	
Security Posture Assessment	Ongoing Scanning & Monitoring
Incident Management	Incident Response

[27] A growing body of reports raise cybersecurity concerns for the Transportation Systems sector [115], and for shipping in particular [100] [101] [99] [98] [102].
[28] See, for example, [116]
[29] This decision is influenced by the fact that the Federal Highway Administration is tailoring the CSF for transportation agencies [101].

Aspect	Current Approach
Threat Intelligence & Analysis	Intermittent
Forensic Analysis	Reactive
Training & Readiness	Training & Awareness
Architecture & Engineering	
Architectural Definition	Basic
Security Engineering Orientation	Basic
Functionality	Basic Cybersecurity
Versatility	Brittle

The Preparedness Improvement Team then defines the desired posture (shown in the figure below), using answers to the threat-oriented questionnaire and the analysis guidelines. This posture is to be achieved in a phased manner an 18-month timeframe, with the longer-term goal of moving the company to Responsive Awareness, with some aspects drawn from Architectural Resilience, and Implementation Tier 4.

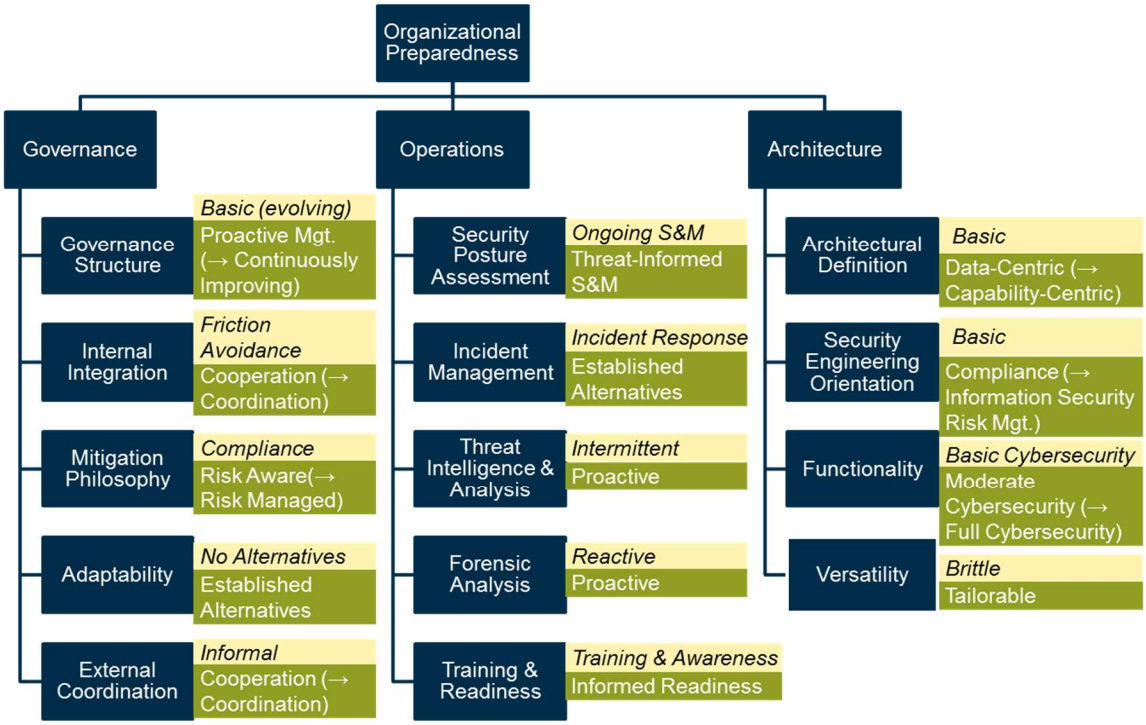

Figure 7-1. *Current* and Desired Approaches

The team can then identify the Categories and Subcategories in the Framework Core that are relevant to the desired approaches, thereby creating a Target Profile. (These in turn point to security controls in a number of informative references, including NIST SP 800-53R4.) These are shown in Table 6-2 below. Because the overall strategy is based on Responsive Awareness with some aspects drawn from Architectural Resilience, most of the Framework Core is covered. However, some Subcategories are omitted (e.g., DE.CM-6, due to contractual considerations), while others are identified as stretch goals (e.g., ID.BE-5).

The team observes that the Framework Core is sparse with respect to Architectural Definition, Security Engineering Orientation, and Versatility. These aspects of Architecture & Engineering, as well as the Threat Intelligence & Analysis and Forensic Analysis aspects of Operations, correspond more to the Implementation Tiers than to the Framework Core.

Table 7-2. Desired Approaches and Corresponding Elements of the CSF Framework Core

Area	*Aspect* & Desired Approach	CSF Framework Core Categories & Subcategories
Governance	*Governance Structure*: Proactive Management, moving toward Continuously Improving	ID.GV-1 through 4 ID.RM-1 and 2 PR.AT-4 PR.IP-11 DE.DP-1
	Internal Integration: Cooperation, moving toward Coordination	ID.GV-2 PR.AT-5 Process aspects of PR.IP (2, 5, 7, 8, 9, 10, 11, 12), PR.MA-1 and 2, and DE.CM-2 and 3 to be phased in as appropriate to the organization
	Mitigation Philosophy: Risk Aware, moving toward Risk Managed (Innovation Adoption is inconsistent with the organizational culture)	ID.RM-3
	Adaptability: Established Alternatives	RS.CO-1 Moving toward RS.IM-1 and 2
	External Coordination: Cooperation, moving toward Coordination	ID.AM-4 and 6 (with respect to external systems and parties) ID.BE-1 through 4, moving toward ID.BE-5 PR.AT-3 (Do not include DE.CM-6) Moving toward RS.CO-5 Moving toward RC.CO-1 through 3
Operations	*Security Posture Assessment*: Threat-Informed Scanning & Monitoring	ID.AM-1, 2, 3, 5, and 6 (for 6, with respect to internal stakeholders) ID.RA-1, 3, and 5 PR.PT-1 DE.CM-1, 4, 5, 7, and 8 Moving toward RS.MI-3
	Incident Management: Incident Management, moving toward Resilient Courses of Action to support Coordination in External Coordination	PR.IP-9, 10 DE.AE-1 through 4 DE.DP-2, moving toward DE.DP-2 through 5 RS.RP-1 RS.CO-2 through 4 RS.AN-1, 2, and 4 RS.MI-1 and 2 RC.RP-1, moving toward RC.IM-1 and 2
	Threat Intelligence & Analysis: Proactive	ID.RA-2, 4, 6
	Forensic Analysis: Proactive	RS.AN-3
	Training & Readiness: Informed Readiness	PR.AT-1, 2, and 4 PR.PT-3
Architecture & Engineering	*Architectural Definition*: Data-Centric, moving toward Capability-Centric	PR.IP-1, 4 RS.MI-1
	Security Engineering Orientation: Compliance, moving toward Information Security Risk Management	PR.IP-2, 3, 12 ID.RA (all)
	Functionality: Moderate Cybersecurity, moving toward Full Cybersecurity	PR.AC, PR.DS (all, but functionality may need to be phased in; PR.DS-7 may be inapplicable), PR.PT-3 and 4, DE.CM-1, 4, 5, 7, and 8
	Versatility: Tailorable (within the limits of organizational resource management strategy)	

The specific steps toward achieving the desired posture, and the time phasing of those steps, takes into consideration such factors as

- The need for internal education on cyber threats and associated organizational risks, to shift the culture within the organization from largely unconcerned with cyber risks to risk-aware. This educational process – starting at the top (as has already happened in this example, causing the company leadership to decide to define its cybersecurity strategy) and moving down the management chain – is crucial to making cultural and governance changes.
- The organization's budget cycle (including when funds must be requested, when funds are allocated, and when funds are actually disbursed). Budgeting is needed not only for technology investment, but for investment in development of the internal expertise needed to make effective use of security technologies.
- The organization's hiring practices. As the organization moves to have greater cybersecurity capabilities, it must make cybersecurity workforce planning part of its overall workforce planning and hiring processes.
- The organization's investment in information and operational technologies.

To support the transition in Governance to internal processes and procedures better suited to Architectural Resilience, the team determines that the company participates in a regional logistics council. While such councils usually do not consider cybersecurity, they are a venue for discussion with peer organizations about good practices (Mitigation Philosophy) and might become a venue for information sharing (External Coordination). In Governance and other areas, the CERT RMM provides descriptions of practices in 26 process areas, mapped to the CSF [42]. To support the transition to an Information Security Risk Management Security Engineering Orientation, the team identifies NIST SP 800-30 and NIST SP 800-53R4 as possible resources.

8 Conclusion

This paper serves as a reference for those who apply Cyber Prep, including systems engineers, organizational change management analysts, and senior cybersecurity staff. The Cyber Prep toolset includes a small set of instruments: a threat-oriented questionnaire and a preparedness-oriented questionnaire, analysis guidelines which translate answers to threat-oriented questions into adversary characteristics and then into recommended levels of different aspects of preparedness, and worked examples. Those instruments are supported by the threat modeling framework and the framework for characterizing preparedness strategies as described in this paper.

Cyber Prep provides a means for an organization to characterize the adversarial threat it faces; that characterization is a key component of risk framing. Cyber Prep also provides a means for an organization to define its overall strategy for preparedness against cyber threats, with the aspects of its strategy motivated by the threats it faces. While Cyber Prep can be used alone, it also provides an index into a variety of frameworks and sector-specific approaches to cybersecurity. However, unlike many frameworks, Cyber Prep is not intended to be a capability maturity model or a compliance vehicle. An organization can use Cyber Prep to determine its current approach to cyber preparedness, and to design its cybersecurity strategy in a way that considers such factors as size, culture, and legal, regulatory, and contractual constraints, drawing from multiple frameworks and guidelines as it sees fit.

9 References

[1] NIST, "Framework for Improving Critical Infrastructure Security, Version 1.0," 12 February 2014. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[2] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1," 10 January 2017. [Online]. Available: https://www.nist.gov/sites/default/files/documents/2017/01/17/draft-cybersecurity-framework-v1.1.pdf.

[3] NACD, "Cyber-Risk Oversight: Director's Handbook Series 2014," July 2014. [Online]. Available: http://www.nacdonline.org.

[4] NACD, "2016–2017 NACD Public Company Governance Survey," 30 November 2016. [Online]. Available: https://www.nacdonline.org/files/2016–2017%20NACD%20Public%20Company%20Governance%20Survey%20Executive%20Summary.pdf.

[5] NACD, "Cyber-Risk Oversight," 11 January 2017. [Online]. Available: https://www.nacdonline.org/cyber.

[6] NIST, "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[7] D. Bodeau and R. Graubart, "A Framework for Describing and Analyzing Cyber Strategies (MTR 140346, PR Case No. 14-3407)," The MITRE Corporation, Bedford, MA, 2014.

[8] Federal Financial Institutions Examination Council, "FFIEC Cybersecurity Assessment Tool, OMB Control 1557-0328," June 2015. [Online]. Available: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

[9] DoE, "Energy Sector Cybersecurity Framework Implementation Guidance," 5 January 2015. [Online]. Available: http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

[10] World Energy Council, "The Road to Resilience: Managing Cyber Risks," 5 October 2016. [Online]. Available: https://www.worldenergy.org/publications/2016/the-road-to-resilience-managing-cyber-risks/.

[11] HITRUST, "Healthcare's Model Approach to Critical Infrastructure Cybersecurity," 20 June 2014. [Online]. Available: https://hitrustalliance.net/content/uploads/2014/06/ImplementingNISTCybersecurityWhitepaper.pdf.

[12] CERT Program, "CERT® Resilience Management Model, Version 1.0: Improving Operational Resilience Processes," May 2010. [Online]. Available: http://www.cert.org/archive/pdf/10tr012.pdf. [Accessed 26 October 2011].

[13] Booz | Allen | Hamilton, "Cyber Operations Maturity Framework," 16 June 2011. [Online]. Available: http://www.boozallen.com/media/file/Cyber-Operations-Maturity-Framework-viewpoint.pdf.

[14] CREST, "The CREST Cybersecurity Incident Response Maturity Assessment Model," 16 October 2014. [Online]. Available: http://www.crest-approved.org/wp-content/uploads/CSIR-Maturity-assessment-tool_Info1.pdf.

[15] Center for Infrastructure Assurance and Security, "The Community Cyber Security Maturity Model," Center for Infrastructure Assurance and Security, 2013. [Online]. Available: http://cias.utsa.edu/the-ccsmm.html.

[16] DHS, "Cybersecurity Capability Maturity Model Version 1.0," 4 August 2014. [Online]. Available: https://niccs.us-cert.gov/sites/default/files/documents/files/Capability%20Maturity%20Model%20White%20Paper_0.pdf.

[17] Deloitte, "Cyber security: empowering the CIO," 18 November 2014. [Online]. Available: http://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-cyber-security-vigilance-resilience-181114.pdf.

[18] Global Cyber Security Capacity Centre, "Cyber Security Capability Maturity Model (CMM) - Pilot," 5 May 2015. [Online]. Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2.pdf.

[19] Information Risk Leadership Council, "The 4 Stages of Cyber Threat Defense Maturity," Corporate Executive Board, 2014.

[20] KPMG Cyber, "Connecting the dots: A proactive approach to cybersecurity oversight in the boardroom," 29 June 2015. [Online]. Available: http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/RiskConsulting/2015/cyber-security-and-board-oversight-whitepaper-v6-secured.pdf.

[21] R. Lentz, "Cyber Security Maturity Model," 21 September 2011. [Online]. Available: http://www.dintel.org/Documentos/2011/Foros/ses2Mcafee/lentz.pdf.

[22] G. White, "The Community Cyber Security Maturity Model," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007.

[23] C. Paulsen and P. Toth, "Small Business Information Security: The Fundamentals, NISTIR 7621 Revision 1," November 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[24] The MITRE Corporation, "Threat-Based Defense: A New Cyber Defense Playbook," July 2012. [Online]. Available: http://www.mitre.org/work/cybersecurity/pdf/cyber_defense_playbook.pdf.

[25] M. Cloppert, "Security Intelligence: Attacking the Kill Chain," 14 October 2009. [Online]. Available: http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/.

[26] NIST, "Guide for Conducting Risk Assessments, NIST SP 800-30 Rev.1," September 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[27] DoD Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013. [Online]. Available: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[28] Verizon, "Verizon Data Breach Investigation Report 2015," 15 April 2015. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf.

[29] The MITRE Corporation, "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)," The MITRE Corporation, 2015. [Online]. Available: https://attack.mitre.org/wiki/Main_Page.

[30] R. Moore, Cybercrime: Investigating High-Technology Computer Crime, Second Edition, Abingdon, England: Routledge, 2014.

[31] Majority Staff Report for Chairman Rockefeller, US Senate Committee on Commerce, Science, and Transportation, "A “Kill Chain” Analysis of the Target Data Breach," 26 March 2014. [Online]. Available: https://www.commerce.senate.gov/public/_cache/files/6e528123-41fc-4c22-a696-a224bbadb6b5/53810A4B7A5AF128030BF310B514BA78.2014-0325-target-kill-chain-analysis.pdf.

[32] S. Harris, "Exclusive: Inside the FBI’s Fight Against Chinese Cyber-Espionage," Foreign Policy, 27 May 2014. [Online]. Available: http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/.

[33] A. Temin and S. Musman, "A Language for Capturing Cyber Impact Effects, MTR 100344, PR 10-3793," The MITRE Corporation, Bedford, MA, 2010.

[34] M. Christian, "Corporate Perspectives On Cybersecurity: A Survey Of Execs," Law360, A LexisNexis Company, 6 May 2015. [Online]. Available: https://www.law360.com/articles/644868/corporate-perspectives-on-cybersecurity-a-survey-of-execs.

[35] W. Miron and K. Muita, "Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure," Technology Innovation Management Review, October 2014. [Online]. Available: http://timreview.ca/sites/default/files/article_PDF/MironMuita_TIMReview_October2014.pdf.

[36] D. P. Duggan, S. R. Thoomas, C. K. Veitch and L. Woodard, "Categorizing Threat: Building and Using a Generic Threat Matrix, SAND2007-5791," September 2007. [Online]. Available: http://energy.sandia.gov/wp-content/gallery/uploads/Duggan-2007-5791.pdf.

[37] World Economic Forum, "Partnering for Cyber Resilience: Toward the Quantification of Cyber Risks," 19 January 2015. [Online]. Available: http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

[38] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[39] Council on Cyber Security, "The Critical Security Controls for Effective Cyber Defense, Version 6.1," 31 August 2016. [Online]. Available: https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf.

[40] C. Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," October 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.

[41] ACSC, "Advanced Cyber Security Center," [Online]. Available: http://www.acscenter.org/.

[42] DHS, "Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalk," February 2014. [Online]. Available: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf.

[43] J. R. Westby, "Governance of Cybersecurity: 2015 Report," 2 October 2015. [Online]. Available: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/governance-of-cybersecurity.

[44] PwC, "PwC's Board Cybersecurity Governance Framework," 10 March 2016. [Online]. Available: https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf.

[45] World Economic Forum, "Advancing Cyber Resilience: Principles and Tools," January 2017. [Online]. Available: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

[46] C. Coulson-Thomas, "Risk Governance and the Board," *Director Today*, pp. 49-55, February 2017.

[47] J. Oltsik, "Research Report: The State of Cyber Security Professional Careers (Part I)," The Enterprise Strategy Group, Inc., and ISSA, October 2016. [Online]. Available: http://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-State-of-Cybersecurity-Professional-Careers-Oct-2016.pdf.

[48] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the STructured Information eXpression (STIX(TM)), Version 1.1, Revision 1," 20 February 2014. [Online]. Available: http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.

[49] J. Kick, "Cyber Exercise Playbook, MP140714," November 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf.

[50] NASCIO, "Cyber Disruption Response Planning Guide," April 2016. [Online]. Available: http://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf.

[51] CNSS, "National Information Assurance (IA) Glossary (CNSS Instruction No. 4009)," 26 April 2010. [Online]. Available: https://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[52] M. Rouse, "Enterprise Architecture Definition," SearchCIO at TechTarget, [Online]. Available: http://searchcio.techtarget.com/definition/enterprise-architecture.

[53] NIST, "NIST SP 800-160, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (Initial Public Draft)," May 2014. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf.

[54] J. Fabius and R. Graubart, "Beyond Compliance - Addressing the Political, Cultural and Technical Dimensions of Applying the Risk Management Framework (PR 14-3551)," January 2015. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr-14-3551-beyond-compliance-applying-risk-management-framework.pdf.

[55] IAB, "The Cyberspace Security Continuum: A People, Processes, and Technology Approach to Meeting Cyber Security Challenges in the 21st Century," December 2013. [Online]. Available: https://iab.gov/Uploads/IAB%20Cyberspace%20Security%20Continuum.pdf.

[56] K. G. Partridge and L. R. Young, "CERT Resilience Management Model (CERT-RMM) V1.1: NIST Special Publication Crosswalk Version 2," April 2011. [Online]. Available: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2011_004_001_15371.pdf.

[57] K. G. Partridge and L. R. Young, "CERT Resilience Management Model (CERT-RMM) v 1.1: Code of Practice Crosswalk Commercial Version 1.1," October 2011. [Online]. Available: http://www.sei.cmu.edu/reports/11tn012.pdf.

[58] ISA-ANSI, "The Financial Management of Cyber Risk: An Implementation Framework for CFOs," December 2010. [Online]. Available: http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf.

[59] HP, "2014 Report of Capabilities and Maturity of Cyber Defense Organizations," 20 January 2014. [Online]. Available: http://www.ten-inc.com/presentations/HP-State-of-Security-Operations-2014.pdf.

[60] DOE and DHS, "Cybersecurity Capability Maturity Model (C2M2) Version 1.1," February 2014. [Online]. Available: http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

[61] DOE, "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)," 31 May 2012. [Online]. Available: http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf.

[62] Deloitte, "Cyber Security in Switzerland: Finding the Balance Between Hype and Complacency," 20 March 2014. [Online]. Available: http://www2.deloitte.com/content/dam/Deloitte/ch/Documents/audit/ch-en-audit-advisory-cyber-security-in-switzerland-08052014.pdf.

[63] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework (MTR110237, PR 11-4436)," September 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

[64] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR 12-3795)," May 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf.

[65] D. Bodeau, R. Graubart, W. Heinbockel and E. Laderman, "Cyber Resiliency Engineering Aid - The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, MTR140499R1, PR 15-1334," May 2015. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf or http://www.defenseinnovationmarketplace.mil/resources/20150527_Cyber_Resiliency_Engineering_Aid-Cyber_Resiliency_Techniques.pdf.

[66] D. J. Bodeau and R. D. Graubart, "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines," January 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

[67] C. Petersen, "The Cyber Threat Risk - Oversight Guidance for CEOs and Boards," April 2015. [Online]. Available: https://www.logrhythm.com/Portals/0/White%20Papers/LR_Security_Intelligence_Maturity_Model_CEO_Whitepaper.pdf.

[68] C. Petersen, "Surfacing Critical Cyber Threats Through Security Intelligence: A Reference Model for IT Security Practicioners," April 2015. [Online]. Available: https://www.logrhythm.com/Portals/0/White%20Papers/LR_Security_Intelligence_Maturity_Model_CISO_Whitepaper.pdf.

[69] World Economic Forum, "Partnering for Cyber Resilience: Risk and Responsibilities in a Hyperconnected World - Principles and Guidelines," March 2012. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

[70] CNSS, "Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009," 26 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/openDoc.cfm?YH/iRvGNV4+nJi4p6bfGkA==.

[71] NIST, "2nd Public Draft, NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," 4 May 2016. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf.

[72] NIST, "NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," 15 November 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf.

[73] NIST, "Federal Information Processing Standards Publication (FIPS PUB) 199: Standards for Security Categorization of Federal Information and Information Systems," February 2004. [Online]. Available: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[74] NIST, "Glossary of Key Information Security Terms, NISTIR 7298, Revision 2," May 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[75] JCS, "Joint Publication 3-12 (R), Cyberspace Operations," 5 February 2013. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[76] Office of the President, "The Common Approach to Federal Enterprise Architecture," 2 May 2012. [Online]. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf.

[77] National Science and Technology Council, "Federal Cybersecurity Research and Development Strategic Plan," February 2016. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf.

[78] The MITRE Corporation, "Systems Engineering for Mission Assurance," Systems Engineering Guide, September 2013. [Online]. Available: http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance.

[79] DoD, "Department of Defense Mission Assurance Strategy," April 2012.

[80] Office of the President, "Presidential Policy Directive (PPD) 21 -- Critical Infrastructure Security and Resilience," 12 February 2013. [Online]. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[81] D. Bodeau, R. Graubart and J. Fabius-Greene, "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels," in *IEEE International Conference on Privacy, Security, Risk and Trust*, 2010.

[82] D. Bodeau, J. Fabius-Greene and R. Graubart, "How Do You Assess Your Organization's Cyber Threat Level?," August 2010. [Online]. Available: http://www.mitre.org/work/tech_papers/2010/10_2914/10_2914.pdf.

[83] D. J. Bodeau, R. D. Graubart and J. Fabius-Greene, "Cyber Security Governance," September 2010. [Online]. Available: http://www.mitre.org/work/tech_papers/2010/10_3710/10_3710.pdf.

[84] F. Mercês, "The Brazilian Underground Market: The Market for Cybercriminal Wannabes?," 17 November 2014. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf.

[85] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems, NIST SP 800-37 Rev. 1," February 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[86] National Association of Corporate Directors, "Highlights of the 2014–2015 NACD," December 2014. [Online]. Available: http://nataofcd.informz.net/NatAofCD/data/images/NACD%202014-2015%20Public%20Company%20Governance%20Survey%20Highlights%20(5).pdf.

[87] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright and M. Whitty, "Understanding Insider Threat: A Framework for Characterising Attacks," in *2014 IEEE Security and Privacy Workshops*, 2014.

[88] E. M. Hutchins, M. J. Cloppert and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proceedings of the 6th International Conference on Information-Warfare & Security (ICIW 2011), March 2011. [Online]. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

[89] Office of the DASD (DT&E), "Guidelines for Cybersecurity DT&E, version 1.0," 19 April 2013. [Online]. Available: https://acc.dau.mil/adl/en-US/649632/file/71914/Guidelines%20for%20Cybersecurity%20DTE%20v1.0%2020130419.pdf.

[90] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment (MTR 130432, PR 13-4173)," November 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf.

[91] ISMG, "Advanced Persistent Threats Survey," Palo Alto Networks, 2014.

[92] Internet Security Alliance, "The Advanced Persistent Threat: Practical Controls That Small and Medium-Sized Business Leaders Should Consider Implementing," 6 June 2013. [Online]. Available: http://isalliance.org/publications/2013-06-06-ISA_APT_Paper-Practical_Controls_for_SMBs.pdf.

[93] ISACA, "Cybersecurity Nexus: Advanced Persistent Threat Awareness Study Results," ISACA, Rolling Meadows, IL, 2014.

[94] The MITRE Corporation, "Cybersecurity: Threat-Based Defense," 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/cyber_defense_playbook.pdf.

[95] C3 Voluntary Program, "Cyber Risk Management Primer for CEOs," 11 February 2014. [Online]. Available: http://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf.

[96] The Institute of Risk Management, "Cyber Risk: Executive Summary," 2 February 2014. [Online]. Available: https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf.

[97] Civil Air Navigation Services Organisation, "CANSO Cyber Security and Risk Assessment Guide," June 2014. [Online]. Available: https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf.

[98] D. Stevens, "Transport & logistics companies – cyber security is relevant to you too!," PwC, 2 April 2015. [Online]. Available: http://pwc.blogs.com/cyber_security_updates/2015/04/transport-logistics-companies-cyber-security-is-relevant-to-you-too.html.

[99] E. Kovacs, "Hackers Attack Shipping and Logistics Firms Using Malware-Laden Handheld Scanners," 2014, 12 July. [Online]. Available: http://www.securityweek.com/hackers-attack-shipping-and-logistics-firms-using-malware-laden-handheld-scanners.

[100] NRC, Committee on Freight Transportation Information Systems Security, "Cybersecurity of Freight Information Systems: A Scoping Study," 2003. [Online]. Available: http://onlinepubs.trb.org/onlinepubs/sr/sr274.pdf.

[101] E. Fok, "An Introduction to Cybersecurity Issues in Modern Transportation Systems," *ITE Journal,* pp. 18-21, July 2013.

[102] Commercial Crime Services, "IMB: Guard against threat of cyber attacks," International Chamber of Commerce, 20 August 2014. [Online]. Available: https://icc-ccs.org/news/1011-imb-guard-against-threat-of-cyber-attacks.

[103] Global Justice Information Sharing Initiative, "Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers," May 2015. [Online]. Available: http://www.cisecurity.org/documents/CyberIntegrationforFusionCenters_000.pdf.

[104] W. Miron, "Adoption of Cybersecurity Capability Maturity Models in Municipal Governments," May 2015. [Online]. Available: https://curve.carleton.ca/system/files/etd/2738d232-c0c2-49fc-90ef-f5664ba6b27a/etd_pdf/b361458c3c8581d512cdc1da916606ab/miron-adoptionofcybersecuritycapabilitymaturity.pdf.

[105] J. Oltsik, "The ESG Cybersecurity Maturity Model," October 2014. [Online]. Available: http://resources.idgenterprise.com/original/AST-0135469_ESG-Brief-HP-Maturity-Model-Oct-2014.pdf.

[106] J. Couch, "The Need for a Threat Intelligence Maturity Model – Pt 1," iSIGHT, 10 July 2015. [Online]. Available: http://www.isightpartners.com/2015/07/the-need-for-a-threat-intelligence-maturity-model-pt-1/.

[107] Core Security, "The Threat and Vulnerability Management Maturity Model," 23 October 2014. [Online]. Available: http://www.coresecurity.com/system/files/attachments/vulnerability-management-maturity-model-white-paper_0.pdf.

[108] F Secure, "The Dukes: 7 years of Russian cyberespionage," 15 September 2015. [Online]. Available: https://cdn3.vox-cdn.com/uploads/chorus_asset/file/4069940/The_Dukes_whitepaper.0.pdf.

[109] Ernst & Young, "Insights on governance, risk, and compliance: Achieving resilience in the cyber ecosystems," December 2014. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf.

[110] I. Bryant and J. Mahrra, "Challenges to a Trustworthy Cyber Ecosystem," *CrossTalk,* pp. 8-10, September/October 2012.

[111] DHS, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action," 23 March 2011. [Online]. Available: http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

[112] M. Rosenquist (ed.), Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, Chicago, IL: Caxton Business & Legal, Inc., 2015.

[113] World Economic Forum, "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience," 4 November 2014. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.

[114] W. Miron and K. Muita, "Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure," *Technology Innovation Management Review*, pp. 33-39, October 2014.

[115] National Infrastructure Advisory Council (NIAC), "Transportation Sector Resilience: Final Report and Recommendations," 10 July 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/niac-transportation-resilience-final-report-07-10-15-508.pdf.

[116] DHS, "Sector Risk Snapshots," May 2014. [Online]. Available: https://www.hsdl.org/?view&did=754033.

[117] E. Fok, R. Murphy, E. Phomsavath and J. Walker, "Taming Cyber Security," *Public Roads, FHWA-HRT-15-006*, vol. 79, no. 2, September/October 2015.

[118] Goldenson Center, "Cyber Risk for Small and Medium-Sized Enterprises," August 2016. [Online]. Available: http://goldensoncenter.uconn.edu/wp-content/uploads/sites/912/2014/09/CyberRiskDraftReport-9-27-2016-Final-without-comments.pdf.

[119] FireEye, "Five Reasons Small and Midsize Enterprises Are Prime Targets for Cyber Attacks," 20 June 2016. [Online]. Available: https://www2.fireeye.com/5-reasons-SMEs-target-cyber-attacks-web.html.

[120] Communications Security, Reliability and Interoperability Council IV, "Cybersecurity Risk Management and Best Practices Working Group 4: Final Report," March 2015. [Online]. Available: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[121] Federal Communications Commission, "FCC White Paper: Cybersecurity Risk Reduction," 18 January 2017. [Online]. Available: http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0118/DOC-343096A1.pdf.

[122] CrossTalk, "CrossTalk, The Journal of Defense Software Engineering. Volume 25, Number 5, September/October 2012, Resilient Cyber Ecosystems," September 2012. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a565930.pdf.

[123] C. Harry, "A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact," Center for International & Security Studies at Maryland, University of Maryland School of Public Policy, July 2015. [Online]. Available: http://www.cissm.umd.edu/sites/default/files/CategorizingDisruptiveCyberActivity%20-%20080615.pdf.

[124] Intel, "Threat Agent Library Helps Identify Information Security Risks," September 2007. [Online]. Available: https://communities.intel.com/docs/DOC-23853.

[125] Intel, "Understanding Cyberthreat Motivations to Improve Defense," 13 February 2015. [Online]. Available: https://communities.intel.com/servlet/JiveServlet/previewBody/23856-102-1-28290/understanding-cyberthreat-motivations-to-improve-defense-paper-l.pdf.

Appendix A Cyber Prep Details

This appendix provides additional detail on the specific aspects of organizational preparedness. Table A-1 indicates which aspects of an organization's preparedness strategy are driven by the different aspects of threat. It must be emphasized, however, that an organization's strategy is shaped not only by the threat the organization faces, but also by such factors as the organization's culture, risk tolerance, and legal, regulatory, and contractual constraints.

Table A-1. Threat Drivers for Aspects of Organizational Strategy

Area	Aspect	Driving Adversary Characteristics
Governance	Governance Structure	Scope, Persistence
	Internal Integration	Persistence, Capabilities
	Mitigation Philosophy	Type (conventional vs. APT) *or* Timeframe, Persistence, Capabilities
	Adaptability	Goals (disruption), Scope
	External Coordination	Scope, Persistence
Operations	Security Posture Assessment	Persistence, Stealth
	Incident Management	Goals (disruption, fraud), Scope
	Threat Intelligence & Analysis	Persistence, Stealth, Capabilities
	Forensic Analysis	Persistence, Stealth, Capabilities
	Training & Readiness	Goals (disruption, fraud), Scope
Architecture & Engineering	Architectural Definition	Goals (disruption, usurpation), Timeframe, Capabilities
	Security Engineering Orientation	Type (conventional vs. APT) *or* Timeframe, Persistence, Capabilities, Scope
	Functionality	Goals (disruption, usurpation), Timeframe, Capabilities
	Versatility	Goals (disruption, usurpation), Timeframe, Capabilities

A.1 Governance

While some frameworks focus on operations, operational effectiveness will be limited by the organization's cybersecurity governance. Cybersecurity governance is the component of organizational governance that addresses the organization's dependence on cyberspace in the presence of adversaries. Organizational governance is the set of responsibilities and practices exercised by those responsible for an enterprise with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly. Resources related to cybersecurity governance focus on corporate boards [5] [4] [43] [44] [45] [46]. However, surveys of cybersecurity professionals provide insight into cybersecurity governance [47].

Five aspects of governance are described in more detail: Governance Structure, Internal Integration, Mitigation Approach, Adaptability, and External Coordination.

A.1.1 Governance Structure

Governance Structure characterizes the ways an organization chooses to organize its cybersecurity decision-making.[30] Cyber Prep does not specify a type of organizational structure for governance, but does assume some decisions must be centralized. This aspect of governance provides a foundation for effective realization of the other aspects of governance, as well as for Operations and Architecture & Engineering. Differences between levels of Governance Structure are based on the structure of governance processes and the relationship between those processes and other enterprise risk management

[30] The different approaches to governance structure are derived from Cyber Prep 1.0 (Senior Leadership), but add concepts related to the overall purpose of cybersecurity processes as well as to active cyber defense.

processes; establishment of roles and responsibilities related to cybersecurity; and whether and how senior organization officials are engaged in cybersecurity governance.

One key element of the External Coordination aspect of governance relates to law enforcement. Many organizations first learn of a breach when they are notified by law enforcement, either because the breach resulted in the loss of information in the organization's custody or because the organization's resources are being used to attack another organization (i.e., the organization has been the target of a positional or stepping stone attack). Thus, regardless of the organization's assumptions about the class of adversary that might attack it, as part of its governance responsibilities any organization should have identified an individual or office to serve as a point of contact for interactions with law enforcement.

Table A-2. Governance Structure

Approach	Governance Structure
Ad hoc	**Cybersecurity processes are informal, typically undocumented, and ad hoc. Responsibilities devolve to individual program managers, business process owners, or system administrators. The organization has designated an individual to serve as the point of contact for law enforcement (LE POC).**
Basic	Cybersecurity processes are **defined by policy, reflecting a set of *a priori* risk management decisions. Some positions in the workforce have designated cybersecurity responsibilities. An Information Security Manager or Officer** is engaged in information security decisions across multiple systems or programs, **and is** designated as the LE POC.
Proactive Management	Cybersecurity processes are **managed to implement an enterprise-wide** risk management **strategy, which includes identification and management of the cybersecurity workforce**. A **responsible corporate officer or agency official** is **actively** engaged in **enterprise-level cyber** security decisions, and is designated as the LE POC.
Continuously Improving	Cybersecurity processes are managed to implement an enterprise-wide risk management strategy **(of which cybersecurity workforce development is a component)**, **and improved based on observation, measurement, and analysis of effectiveness**. A **dedicated** corporate officer or agency official is actively engaged in enterprise-level cyber security decisions, is designated as the LE POC, and **closely coordinates with near-term decision-makers; some near-term decisions are reserved for the senior official (or designated alternate in cases of disruption). The organization has defined the scope of active cyber defense activities, and has defined the relationship between such activities and other mission / business processes.**
Intelligently Evolving	Cybersecurity processes are managed to **ensure ongoing evolution of the** enterprise-wide risk management strategy (of which cybersecurity workforce development is **an integral** component) **as the environment changes. The CEO or Agency head** is actively engaged in **mission assurance** decisions**; the senior official responsible for cyber security strategy** closely coordinates with near-term decision-makers, and is designated as the LE POC. Some near-term decisions are reserved for **the CEO or agency head** (or designated **senior official(s)** in cases of disruption). The organization has defined the scope of active cyber defense activities, has defined the relationship between such activities and other mission / business processes**, and has established the necessary policy, doctrine, and external relationships**.

A.1.2 Internal Integration

Cybersecurity relies on effective security measures outside of cyberspace. At a minimum, cybersecurity includes the disciplines of information system or IT security and communications security. However, other technical security disciplines, depending on how cyberspace is defined, can also be part of cybersecurity. In the more APT-driven Cyber Prep classes, the focus moves from cybersecurity to mission assurance in the presence of cyber threats.

The relationship between other disciplines and cybersecurity in the different Cyber Prep classes, particularly information security, is indicated below. A key difference is between *alignment* and *integration*. Alignment involves information sharing and coordination among operational managers in the different areas, as well as some coordination among the strategic planners in those areas. Integration involves a shared understanding of threats and consequences, and closely coupled risk management

strategies among the strategic planners for the different areas, possibly leading to changes in how the areas are defined or managed.[31]

Note that this aspect of governance is intended to support and leverage integration within the communities of practice or sub-organizations responsible for specific operational processes (e.g., incident management, malware or forensic analysis). That integration is addressed under the aspects of Operations, in A.2.2 below.

Table A-3. Internal Integration

Approach	Internal Integration
None	**No integration; information security is part of programmatic risk management.**
Friction Avoidance	**Physical security, personnel security, and business continuity are aligned with cyber** security, **which includes ICT (information and communications technology)** security. **Cyber** security is part of **larger-scale risk management (e.g., coordinated management of information, IT, compliance, and business risks) to avoid conflicts.**
Cooperation	Physical security, personnel security, business continuity, **ICT architecture, and operations security are integrated** with cyber security. **Organizational units responsible for cyber security, architectural, and acquisition strategies cooperate to ensure consistency; cyber** security is part of **enterprise** risk management.
Coordination	Physical security, personnel security, business continuity, **supply chain risk management (SCRM)**, ICT architecture, **business process engineering**, operations security, **and cyber security are integrated with mission assurance**. Organizational units responsible for cybersecurity, architectural, and acquisition strategies **coordinate to achieve synergies**; cyber security **strategy** is part of **mission assurance strategy, which** is part of **the organization's mission and** enterprise risk management **strategies**.
Collaboration	Physical security, personnel security, business continuity, SCRM, ICT architecture, business process engineering, operations security, and cyber security are integrated with mission assurance. **Organizational units (e.g., programs, business units) collaborate to implement the organization's mission assurance strategy, recognizing that cybersecurity is a significant** part of the organization's mission and enterprise risk management strategies.

A.1.3 Mitigation Philosophy

The organization's mitigation philosophy reflects its relative priorities regarding compliance with standards of good practice versus proactive investment in new mitigation techniques. To address the conventional threat, the organization can focus on compliance with standards of good practice, so that cyber security governance is strongly identified with compliance. With threat-informed and anticipatory risk management, the persistence, inventiveness, and adaptability of the adversary motivate the organization to push the state of the practice and even the state of the art.[32]

The mitigation philosophy provides a foundation for Operations and Architecture & Engineering, by identifying the set of stages of the cyber attack lifecycle to be considered. That consideration is reflected in organizational policies and resources for cyber defenders, which determines which types of attack activities defenders are authorized to look for and analyze. One distinction between levels is the stages of the cyber attack lifecycle defenders are authorized to consider. (Note that to gain information about some activities, defenders may need to look at or even participate in malware marketplaces; because this could incur risk to the organization, it will require authorization by appropriate organizational senior leadership.)

[31] Internal Integration merges two aspects of governance in Cyber Prep 1.0: Allied Disciplines and Integration of Cybersecurity Strategy with Other Organizational Strategies.

[32] Mitigation Philosophy builds on the Cyber Risk Mitigation Approach in Cyber Prep 1.0, adding material related to organizational intent from the DACS framework [7], in particular identifying the stages of the cyber attack lifecycle the organization seeks to address.

Table A-4. Mitigation Philosophy

Approach	Mitigation Philosophy
Compliance	**Information security is identified with compliance with standards of good practice. Trade-offs are made between alternative products, within cost constraints. The organization considers the adversary tactically; cybersecurity staff consider selected stages of the CAL (typically, Deliver, Exploit, and Execute).**
Risk Aware	Information security is identified with compliance with standards of good practice, **in the context of broader risk management**. **The organization makes trade-offs between cybersecurity and financial costs.** The organization **seeks to affect** the adversary tactically. **Cyber defenders are authorized to** consider selected stages of the CAL (typically, Recon, Deliver, Exploit, limited aspects of Control, and Execute).
Risk Managed	**Cybersecurity includes conformance** with standards of good practice, **but pushes the state of the practice to address the advanced threat**. The organization makes trade-offs between cybersecurity and financial costs, **including potential costs of compromise**. The organization seeks to affect the adversary **operationally as well as** tactically. Cyber defenders are authorized to consider **all stages of the CAL except Weaponize**.
Innovation Adoption	Cybersecurity **builds on** standards of good practice, but pushes the state of the practice **by incorporating state of the art techniques, sometimes at the expense of non-compliance with standards of good practice**. The organization makes trade-offs among cybersecurity, **mission resilience,** innovation **(including new business models)**, and financial costs (including potential costs of compromise **and loss of competitive advantage**). The organization seeks to affect the adversary **in limited strategic ways** as well as tactically and operationally. Cyber defenders are authorized to consider **all** stages of the CAL, **as well as some supply chain attack patterns**.
Innovation Leadership	Cybersecurity builds on standards of good practice, but pushes **the state of the art to ensure continued security evolution in the face of an innovative adversary**. The organization makes trade-offs among cybersecurity, mission resilience, innovation, financial costs, **and current and potential future relationships, missions, and competitive advantages**. The organization seeks to affect the adversary **strategically** as well as tactically and operationally. Cyber defenders are authorized to consider all stages of the CAL, as well as **all** supply chain attack patterns.

A.1.4 Adaptability

Adversary activities can affect the organization's ability to carry out its normal business or mission functions, including those functions that are designed to enable the organization to handle disruptions. Incident handling is part of generally accepted cybersecurity practices, and handling of ICT disruptions is commonly part of business continuity planning. However, business continuity planning does not usually address adversary activities, which can be intended to disrupt decision making (or can have such disruption as a side effect). Thus, adaptability and agility need to be built into cyber security decision making processes, providing alternative lines of communications, control, and processing.

With conventional threats, the effects of adversary activities are assumed to be only moderately disruptive; attacks are assumed to be of limited scope and duration, and not targeted at decision makers. Thus, disruption of decision making processes is also expected to be limited. In the more APT-driven Cyber Prep classes, the organization needs well-defined alternative processes for communications and decision making. These processes need to consider the fact that adversaries may target decision makers and decision processes.

Table A-5. Adaptability

Approach	Adaptability
No Alternatives	**The organization's processes for decision making in the event that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process are ad-hoc.**
Limited Alternatives	The organization **has an informal process intended to provide some limited alternate cyber decision making in the event** that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process**. The process may draw upon an existing COOP process, but cyber disruptions not actually considered in COOP planning.**
Established Alternatives	The organization has **defined and implemented a** process, **which may be integrated into COOP planning,** that provides for limited alternate cyber decision making in the event that the adversary's action **disrupts critical** aspects of the primary decision making process.
Exercised Alternatives	The organization has defined, **implemented, and exercised** a process, which may be integrated into COOP planning, that provides for alternate **critical** cyber decision making, **allowing for delegation of responsibilities**, in the event that the adversary's action **results in a successful long term disruption** of **key** aspects of the primary decision making process.
Adaptable Alternatives	The organization has defined, implemented and exercised **an adaptable** process, which **is** integrated into COOP planning, that provides for alternate cyber decision making, allowing for timely decisions and delegation of responsibilities, in the event that the adversary's actions results in a successful long term **destruction or severe** disruption of the primary decision making process, **or otherwise prevents it from acting in a timely manner**. **Alternatives can be modified or tailored based on circumstances.**

A.1.5 External Coordination

The importance of a "beyond the enterprise" component to an organization's strategy is increasingly recognized. The External Coordination aspect of governance reflects the ways in which the organization engages with service providers, business partners or suppliers, with customers, with other organizations in the organization's sector, and with Government agencies[33]. With respect to cyber security practices, this can take such forms as information sharing, coordination, agreement on standards for information exchange, agreement on standards of good practice, etc., and complements other forms of integration or collaboration beyond the enterprise. With respect to risk governance, external coordination can range from working in relative isolation to participation in the ongoing discussion which is shaping the collective understanding of the cyber security problem domain.[34]

Table A-6. External Coordination

Approach	External Coordination
Informal	**Cybersecurity staff share information about security needs and concerns with cybersecurity staff in ICT supplier organizations.**
Avoidance of Imposed Risks	Cybersecurity staff share information with **counterparts in partner and** supplier organizations, **to support shared awareness of threats and detect incidents. The organization engages with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization**. **The organization has defined procedures for cooperating with law enforcement.**

[33] In addition to law enforcement, these may include state and major urban area fusion centers [103].
[34] External Coordination is based on Strategic Integration Beyond the Enterprise in Cyber Prep 1.0, but adds concepts related to types of relationships from the DACS framework [7] as well as the potential for external relationships in active cyber defense.

Approach	External Coordination
Cooperation	**Cybersecurity staff cooperate** with counterparts in **peer**, partner, supplier, and **customer** organizations, to support shared awareness of threats and detect incidents. The organization engages with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization**, and to limit the risks the organization shares with or imposes on others**. **The organization maintains awareness of bodies working on better understanding of cyber threats, consequences, and risk mitigation approaches, since their work could impact organizational strategy.** The organization has defined procedures for cooperating with law enforcement**, including procedures for determining when and how to notify law enforcement**.
Coordination	**Cyber defense and strategic planning** staff **coordinate** with counterparts in peer, partner, supplier, and customer organizations, to support shared **response to** threats **and so that the organization's cybersecurity strategy is not undermined by strategic weaknesses in those organizations.** The organization **cooperates and selectively coordinates** with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization, to limit the risks the organization shares with or imposes on others**, and to reduce the risks of cascading failures or unintended consequences of active cyber defense**. The organization **cooperates with or participates in** bodies working on better understanding of cyber threats, consequences, and risk mitigation approaches, since their work could impact organizational strategy. The organization has defined procedures for cooperating with law enforcement**,** including procedures for determining when and how to notify law enforcement.
Collaboration	Cyber defense and strategic planning **staff collaborate** with cybersecurity counterparts in **other organizations in the organization's mission or critical infrastructure sector, as well as in** peer, partner, supplier, and customer organizations, to support shared **information-gathering about, analysis of, preparation for, and** response to threats, **to increase the effectiveness of active cyber defense,** and so that the organization's cybersecurity strategy is **part of a mission-wide or sector-wide mission assurance strategy**. The organization **coordinates and selectively collaborates** with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization, to limit the risks the organization shares with or imposes on others, and to **jointly manage** the risks of cascading failures or unintended consequences of active cyber defense. The organization **collaborates** with bodies working on better understanding **the cybersecurity problem domain and related trade-offs, developing common solutions, and/or defining policies and joint strategies.**

A.2 Operations

Five aspects of operations are described in more detail: Security Posture Assessment, Incident Management, Threat Intelligence and Analysis, Forensic Analysis, and Training and Readiness. As noted in the discussion of Internal Integration under Governance, A.2.1.2 above, the Cyber Prep classes for threat-informed and anticipatory risk management are characterized by collaboration or integration among cybersecurity processes and specialties. In the Operations aspects of Cyber Prep, one key differentiation is between cybersecurity staff, who are responsible for implementing the organization's cybersecurity program and administering cybersecurity mechanisms such as identity and access management, and cyber defenders, who are responsible for defending the organization's cyber resources by detecting, analyzing, responding to, reporting on, and thwarting cyber attacks.[35] Among cyber defenders, specialists can include threat analysts, responsible for analyzing and generating cyber intelligence reports as well as for creating, sharing, and analyzing detailed threat information, and forensic analysts, responsible for analyzing artifacts (e.g., malware) and damage from cyber attacks. At and above Cyber Prep Level 3, the organization may create and operate its own Security Operations Center (SOC).[36]

[35] The area of responsibility for cyber defenders is defensive cyberspace operations [75].
[36] See [40] for a discussion of the circumstances under which an organization might create its own SOC.

A.2.1 Security Posture Assessment

Security Posture Assessment refers to how the organization maintains a sense of the current security status of its cyber resources, and manages that posture to address vulnerabilities. To address conventional cyber threats, Security Posture Assessment relies on resources such as continuous diagnostics and monitoring (CDM) tools and services, overseen by cybersecurity staff. In the more APT-driven Cyber Prep classes, Security Posture Assessment results in cyber situational awareness (SA).

Table A-7. Security Posture Assessment

Approach	Assessment and Awareness
Minimal	**The organization invests minimal effort to understand its security posture, relying on vulnerability assessment and malware protection tools to identify incidents.**
Ongoing Scanning & Monitoring	The organization **allocates resources** to understand its security posture, **scanning and monitoring cyber resources on an ongoing basis**.
Threat-Informed Scanning & Monitoring	The organization **applies** resources to understand its security posture, **including to understand how its threat environment is changing**, scanning and monitoring cyber resources on an ongoing basis **using updated threat information**.
Cyber Situational Awareness (SA)	The organization applies resources to **maintain situational awareness of its cyber resources and of the changing threat**.
Integrated Mission Situational Awareness (SA)	The organization **integrates cyber situational awareness with mission / organizational situational awareness, so that the mission implications of the cybersecurity posture can be understood and managed**.

A.2.2 Incident Management

Incident Management refers to organizational processes for responding to or managing incidents or indications that an incident could occur. For practice-driven risk management oriented toward conventional cyber threats, the focus is on event detection and incident response. For threat-informed and anticipatory risk management, cyber courses of action and active cyber defense become key processes. The processes can be limited to managing the effects of adversary activities late in the cyber attack lifecycle, or can span it.

Table A-8. Incident Management

Level	Incident Management
Ad hoc Response	**Cybersecurity staff respond to incidents to support policy enforcement, based on detection of Execute activities.**
Incident Response	Cybersecurity staff respond to incidents, based on detection of **activities in the Exploit and** Execute stages**.**
Incident Management	Cybersecurity staff **manage** incidents **and other events (e.g., potentially disruptive software changes, execution of contingency plans)** to support policy enforcement **and system resilience,** based on detection of activities in the Exploit and Execute stages **as well as indications and warning (I&W) for activities in the Recon and Control stages**.
Resilient Courses of Action	**Cyber defenders and tool developers work together to detect and analyze threats and develop effective and timely courses of action, including active cyber defense,** based on indications and warnings (I&W) for activities **throughout the cyber attack lifecycle**. Cybersecurity staff manage events **jointly with cyber defenders and mission owners**, **while cyber defenders execute and adapt courses of action** throughout the cyber attack lifecycle **to support mission resilience**. **Courses of action can include allowing limited adverse consequences as part of a deception strategy, and relying on alternative supply chains to address some supply chain attack patterns.**

Level	Incident Management
Integrated Defensive Operations	**An integrated team of** cyber defenders, **including forensics analysts and threat analysts,** and tool developers work together to detect, analyze and develop effective and timely courses of action, including active cyber defense, **cooperating or collaborating with external parties consistent with organizational policy**. Cybersecurity staff manage events jointly with cyber defenders and mission owners, while cyber defenders execute and adapt courses of action throughout the cyber attack lifecycle to support mission resilience. Courses of action can include allowing limited adverse consequences as part of a deception strategy, and relying on alternative supply chains to address **most if not all known** supply chain attack patterns.

A.2.3 Threat Intelligence and Analysis

Threat Intelligence and Analysis refers to organizational processes for using (and, at Architectural Resilience and Pervasive Agility, for developing) cyber threat intelligence information. This includes adversary tactics, techniques, and procedures (TTPs). In accordance with organizational policy, threat information may be shared, for example using STIX and TAXII [48]. For practice-driven risk management, cybersecurity staff are consumers of threat intelligence reports; for threat-informed and anticipatory risk management, cyber defenders both consume and create threat intelligence information.

Table A-9. Threat Intelligence and Analysis

Approach	Threat Intelligence Analysis
Intermittent	**Cybersecurity staff review threat intelligence reports on an intermittent, ad hoc basis.**
Ongoing	Cybersecurity staff review threat intelligence reports on an **ongoing** basis, **to identify threats or attack patterns that might apply to the organization**.
Proactive	Cybersecurity staff review threat intelligence reports **and shared threat information** on an ongoing basis, to identify **new** threats or attack patterns that might apply to the organization **currently or in the future**.
Integrated	**Cyber defenders analyze** threat intelligence reports and shared threat information on an ongoing basis. **Cyber defenders analyze adversary behavior to identify adversary TTPs. Cyber defenders work with cybersecurity staff to define and meet data collection needs, and work with mission owners to define courses of action related to current and anticipated threats.**
Innovative	Cyber defenders analyze threat intelligence reports and shared threat information on an ongoing basis. **Cyber defenders define new threat analytic methods, including** to identify adversary TTPs **and to assess the effects of defensive actions on adversary activities.** Cyber defenders work with cybersecurity staff to define and meet **analysis-driven** data collection needs, and work with mission owners to define courses of action related to current and anticipated threats.

A.2.4 Forensic Analysis

Forensic Analysis refers to organizational processes for analyzing (and, at for threat-informed and anticipatory risk management, developing new capabilities to analyze) artifacts such as malware, damage, and other evidence left by adversary activities. For practice-driven risk management, forensic analysis of malware is outsourced (or not performed); the focus is on identifying damage. In the more APT-driven Cyber Prep categories, forensic analysis can result in the development of indicators (i.e., "observable patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context" [48]), which can then be shared using STIX and TAXII.

Table A-10. Forensic Analysis

Approach	Forensic Analysis
Reactive	**Cybersecurity staff perform reactive, after-the-fact analysis focused on damage assessment; analysis is limited by the priority of restoring normal operations.**
Enabled	Cybersecurity staff **support** after-the-fact analysis of damage **and residual artifacts (e.g., malware), typically performed by another organization**.
Proactive	Cybersecurity staff **perform** after-the-fact analysis of damage and residual artifacts (e.g., malware).
Integrated	**Cyber defenders analyze cyber situational awareness and other data** on an ongoing basis, **to look for damage, artifacts, and observables related to any of the post-Exploit stages**. **Forensic analysts analyze malware, develop indicators, and work with tool developers to develop effective countermeasures against malware or to discern indicators. Forensic analysts and cyber defenders work with cybersecurity staff to define and meet data collection needs, particularly to enable rapid detection of intrusions, and work with mission owners to define courses of action related to current and anticipated threats.**
Innovative	Cyber defenders analyze cyber situational awareness and other data on an ongoing basis, to look for damage, artifacts, and observables related to any of the post-Exploit stages **as well as related to supply chain attack patterns**. Forensic analysts analyze malware, develop indicators, and **define new forensic analysis methods, and** work with tool developers to develop effective countermeasures against malware **and to implement new analysis tools.** Forensic analysts and cyber defenders work with cybersecurity staff to define and meet **analysis-driven** data collection needs, particularly to enable rapid detection of intrusions **and to identify evidence and support attribution**, and work with mission owners to define courses of action related to current and anticipated threats.

A.2.5 Training & Readiness

Training & Readiness refers to organizational processes for ensuring that the relevant staff are informed about the roles they play in addressing cyber threats, and are ready to fulfill those roles. For practice-driven risk management, readiness is aligned or integrated with business or mission continuity; for threat-informed and anticipatory risk management, readiness is part of mission assurance. For guidance on cyber exercises, see [49] [50].

Table A-11. Training & Readiness

Approach	Training and Readiness
Training & Awareness	**Cybersecurity staff and users receive training and awareness materials.**
Risk-Informed Training & Awareness	Cybersecurity staff and users receive **tailored** training and awareness materials, **based on the organization's risk tolerance and threat assumptions**. **Cybersecurity staff develop contingency plans, based on relatively static threat intelligence.**
Informed Readiness	Cybersecurity staff and users receive tailored training and awareness materials, based on the organization's risk tolerance and threat assumptions. Cybersecurity staff **coordinate with business continuity planners to** develop **integrated** contingency plans, based on relatively static threat intelligence.
Coordinated Readiness	Cybersecurity staff and users receive tailored training and awareness materials, based on the organization's risk tolerance and threat assumptions. **Additional training and awareness materials are developed and disseminated based on threat intelligence updates.** Cybersecurity staff coordinate with business continuity planners to develop integrated contingency **and continuity of operations (COOP)** plans, **coordinating with cyber defenders; cyber defenders develop alternative courses of action, coordinating with mission owners**.
Integrated Readiness	Cybersecurity staff and users receive tailored training and awareness materials, based on the organization's risk tolerance and threat assumptions. Additional training and awareness materials are developed and disseminated based on threat intelligence updates. **Contingency plans, COOP plans, and cyber courses of action are jointly developed, to minimize mission disruption when executed.**

A.3 Architecture & Engineering

Cyber Prep does not assume a specific architecture or architectural framework. Four aspects of architecture are identified: Architectural Definition, Security Engineering Orientation, Functionality, and Versatility.

A.3.1 Architectural Definition

Architectural Definition refers to how – and how well – the organization defines its security architecture. In the more APT-driven Cyber Prep classes, the security architecture is an integral part of the enterprise architecture. (Note that while enterprise architecture can be narrowly construed to refer to the organization's information systems [51], it can be more broadly construed to include the organization's business or mission processes and their relationships [52].)

Table A-12. Architectural Definition

Approach	Architectural Definition
Basic	**The security architecture is informally defined, and focuses on the enterprise perimeter, and on selected internal security capabilities.**
Data-Centric	**The security architecture is well-defined with respect to critical information and its uses.** The security architecture **may be** informally defined, and focuses on the enterprise perimeter, selected internal security capabilities**, and data loss prevention**.
Capability-Centric	The security architecture **is sufficiently well defined to enable analysis of mission dependencies on and interactions with security capabilities**. **The enterprise architecture is well-defined with respect to mission / business functions and supporting functionality, including critical information to be protected; the security architecture is recognized as a view into or as a key aspect of the enterprise architecture**.
Mission-Centric	The security architecture is defined, to enable **analysis of cyber resiliency and mission resiliency capabilities, including those that involve dependencies on organization-external systems**. The enterprise architecture is well-defined with respect to mission / business functions and supporting functionality, including critical information to be protected **and application of cyber resiliency design principles**; the security architecture is recognized as **integral to** the enterprise architecture.
Extensive	The security architecture is defined, to enable analysis of cyber resiliency and mission resiliency capabilities, including those that involve dependencies on **or interactions with** organization-external systems. The enterprise architecture is well-defined with respect to mission / business functions and supporting functionality, **including missions or business functions that go beyond the organization** and application of cyber resiliency design principles; the security architecture is recognized as a integral to the enterprise architecture.

A.3.2 Security Engineering Orientation

Security Engineering Orientation refers to the emphasis of engineering activities – particularly trade-off analyses – performed when the organization acquires, upgrades, or replaces its systems, services, and infrastructure components. See NIST SP 800-160 for more information about such activities [53].

In the context of the JTF and CNSS publications, a compliance-oriented philosophy often leads to blind selection of every control in a baseline; a consequence-oriented philosophy allows for some tailoring of baselines, recognizing trade-offs between the management of confidentiality, integrity, and availability risks, as well as consideration of overlays. It must be emphasized that neither of these orientations is true to the spirit of the JTF approach to risk management [54]. However, often an organization that has heretofore failed to apply any real security engineering needs to live with one of these philosophies long enough to recognize the limitations of the approach, and in particular how such an approach fails to address the APT. Consistent with the JTF approach, an orientation to information security risk management requires consideration of the full range of environmental factors to which a system, service, or infrastructure will be subject – including threat as well as operational and technical factors.

An organization's Security Engineering Orientation needs to be tightly coupled with its Mitigation Philosophy in order to ensure that engineering decisions will be consistent with the organizational risk management strategy.

Table A-13. Security Engineering Orientation

Approach	Security Engineering Orientation
Compliance-Oriented	**Security engineering activities focus on applying and establishing compliance with generally accepted standards of good practice.**
Consequence-Oriented	Security engineering activities focus on applying generally accepted standards of good practice, **selecting security controls based on an awareness of worst-case or expected consequences**. **Trade-off analyses consider different types of consequences, related to confidentiality, integrity, and availability.**
Oriented to Information Security Risk Management	Security engineering activities focus on **selecting and implementing effective** security controls, **based on consideration of different types of information security risks and of the environments in which the controls will be used**. Trade-off analyses consider different types **and levels of security risks, and relative effectiveness of alternative controls and implementations in risk reduction**.
Oriented to Mission Risk Management	Security engineering activities focus on selecting and implementing effective security **and resiliency** controls, based on consideration of different types of information security risks, the environments in which the controls will be used, **and ensuring that cyber security and resiliency mechanisms will support mission assurance**. Trade-off analyses consider different types and levels of security **and mission** risks, and relative effectiveness of alternative controls, **cyber resiliency techniques,** and implementations in risk reduction.
Fully Integrated with Mission and Organizational Risk Management	Security engineering activities focus on selecting and implementing effective security and resiliency controls, based on consideration of different types of information security risks, the environments in which the controls will be used, and ensuring that cyber security and resiliency mechanisms will support mission assurance. Trade-off analyses consider different types and levels of security and mission risks, and relative effectiveness of alternative controls and implementations in risk reduction, **in the context of future strategic plans as well as current and anticipated mission needs**.

A.3.3 Functionality

Functionality refers to the types of functions or capabilities the organization's security architecture provides. For ease of exposition, terminology is drawn from the NIST Cybersecurity Framework (the functional areas of Identify, Protect, Detect, Respond, and Recover) and MITRE's Cyber Resiliency Engineering Framework (the cyber resiliency goals of Anticipate, Withstand, Recover, and Evolve, and the cyber resiliency objectives of Understand, Prepare, Prevent / Avoid, Continue, Constrain, Reconstitute, Transform, and Re-Architect). See the glossary for definitions of these terms, and see Appendix B for a discussion of the relationship between Cyber Prep and these frameworks.

Table A-14. Functionality

Approach	Functionality
Basic Cybersecurity	**Cybersecurity capabilities focus on the functional areas of Identify, Protect, Detect, and Respond.**
Moderate Cybersecurity	Cybersecurity capabilities **cover** the functional areas of Identify, Protect, Detect, Respond**, and Recover**.
Full Cybersecurity	Cybersecurity capabilities cover the functional areas of Identify, Protect, Detect, Respond, and Recover, **complemented with capabilities that provide some support to a limited set of cyber resiliency objectives**.
Cyber Resiliency	Cybersecurity **and related** capabilities **include the full range of cybersecurity functional areas and most cyber resiliency goals (Anticipate, Withstand, Recover, and limited aspects of Evolve) and objectives**.

Approach	Functionality
Extended Cyber Resiliency	Cybersecurity and related capabilities includes the full range of cybersecurity functional areas and **all** cyber resiliency goals and objectives. **Capabilities for active cyber defense may also be defined, and their interactions with cybersecurity and cyber resiliency capabilities articulated.**

A.3.4 Versatility

Versatility refers to the extent to which the organization can modify, tailor, or extend its security architecture to improve cybersecurity, resilience, and defensibility, while continuing to adapt to changing technologies and operational uses. For practice-driven risk management, the organization is limited by resources or investments to commercial off-the-shelf (COTS) products.

Table A-15. Versatility

Approach	Versatility
Brittle	**The organization has very few options for tailoring or extending its architecture to improve security (e.g., the architecture is driven by legacy investments; the organization lacks the resources to tune COTS products). Changes in the technical or operational environment can break security functionality.**
Rigid	The organization has **limited** options for tailoring or extending its architecture to improve security (e.g., **by replacing or upgrading selected legacy components with known security issues; by tuning** COTS products**). The implementation of security functionality restricts options for architectural changes to accommodate** changes in the technical or operational environment.
Tailorable	The organization has **multiple** options for tailoring or extending its architecture to improve **cybersecurity** (e.g., by **phased replacement or upgrades to** legacy components **to reduce inherent vulnerabilities**; by tuning **and coordinating the use of** COTS products **using enterprise-level tools); and some limited options for providing and improving cyber resiliency**. **The security architecture includes numerous modular components which can be replaced without overhauling the entire architecture.**
Adaptable	The organization has multiple options for tailoring or extending its architecture to improve cybersecurity (e.g., by phased replacement or upgrades to legacy components to reduce vulnerabilities; by tuning and coordinating the use of COTS products using enterprise-level tools**; by modifying COTS products**) **and integrating cyber resiliency into technical and process architectures (e.g., by integrating technologies that implement different cyber resiliency techniques). The architecture is designed so that the replacement of components supporting one set of security functions may be done without adversely impacting some other set of security functions.**
Highly Evolvable	The organization has multiple options for tailoring or extending its architecture to improve cybersecurity, cyber resiliency, **and cyber defense, including the use of multiple architectures, tailored to different environments.** The architecture is designed so that the replacement of components supporting one set of security functions may be done without adversely impacting some other set of security functions. **In addition, the architecture is designed to support additional or alternate components that support a given set of security functions.**

Appendix B Mapping to Related Frameworks

This appendix identifies other frameworks that could be used in conjunction with Cyber Prep. Each framework is described in terms of its intended users (e.g., organizations, corporate officers and their staffs, managers), its focus in terms of the Cyber Prep framework (e.g., threat characteristics; aspects of governance, operations, architecture & engineering), and its relevance to users of Cyber Prep. Key elements of the framework that could be mapped to elements (**classes**, *areas*, and aspects) of Cyber Prep are also identified.

Table B-1. Mapping Cyber Prep to Other Frameworks

Source	Description	Elements	Corresponding Elements of Cyber Prep 2.0
NIST Cybersecurity Framework (CSF) [1] [2]	**Intended users**: Organizations in critical infrastructure sectors. **Focus**: Operations, Architecture, Governance **Relevance:** Four tiers characterize an organization's risk management practices and approaches. Like Cyber Prep strategies, the tiers do not constitute a maturity model. Cybersecurity practices are organized into five functional areas.	**Framework Implementation Tiers**: 1: Partial 2: Risk Informed 3: Repeatable 4: Adaptive	Partial ~ **Basic Hygiene** Risk Informed ~ **Critical Information Protection** Repeatable (extended to consider APT) ~ **Responsive Awareness** Adaptive ~ **Architectural Resilience**
		Key Aspects of Tiers: Risk Management Process Integrated Risk Management Program External Participation	Governance aspects**:** Governance Structure Internal Integration External Coordination
		Functions (with 22 categories and 97 sub-categories): Identify Protect Detect Respond Recover	Used in defining Functionality aspect of *Architecture & Engineering* Identify: All (note that only the Asset Management category applies; other Identify categories relate to Governance Structure and Mitigation Philosophy, and to Security Posture Assessment) Protect: All Detect: All Respond: All Recover: All but **Basic Hygiene**
DSB [27]	**Intended users:** Department of Defense, to define a strategy for improving the resilience of DoD systems to cyber attacks. **Relevance:** A threat hierarchy of potential attackers' capabilities characterizes six tiers of adversaries. A risk model	**Six tiers of potential attackers:** Tiers I and II: exploit known vulnerabilities Tiers III and IV: discover new vulnerabilities Tiers V and VI: create vulnerabilities	Cyber Prep Threat Classes: Tier I ~ **Cyber Vandalism** Tier II ~ **Cyber Incursion** Tier III ~ **Cyber Breach & Organizational Disruption** Tier IV, some Tier V ~ **Cyber Espionage & Extensive Disruption** Tier V, Tier VI ~ **Cyber Espionage & Extensive Disruption**, **Cyber-Supported Strategic Disruption**

Source	Description	Elements	Corresponding Elements of Cyber Prep 2.0
	motivates the definition of risk management approaches. **Focus**: Threats	**Risk model (and corresponding *risk management approaches*):** Threat: Intent (*Deter*) and Capabilities (*Disrupt*) Vulnerabilities: Inherent (*Defend*) and Introduced (*Detect*) Consequences: Fixable (*Restore*) and Fatal (*Discard*)	Cyber Prep enables the organization to apply the risk management approaches. Deter (subject to the organization's Mitigation Philosophy): **Pervasive Agility** (Incident Management) Disrupt: **Architectural Resilience** and **Pervasive Agility** (Incident Management) Defend: **Responsive Awareness** and **Pervasive Agility** (Incident Management) Detect: All Cyber Prep classes (Incident Management, Functionality) Restore: All but **Basic Hygiene** (Incident Management, Functionality) Discard: **Architectural Resilience** and **Pervasive Agility** (Versatility)
NIST SP 800-39 Tiers and Risk Management Process [6]	**Intended users:** Organizations seeking to manage information or cyber security risks. **Focus:** Governance **Relevance:** Three organizational tiers at which risk management activities are performed are identified. A four-step high-level risk management process is defined, and discussed in the context of the tiers.	**Organizational tiers:** 1: Organization 2: Mission / Business Process 3: Information System	Cyber Prep is intended for use at Tier 1. If the organization treats cyber defense as a mission or business area, the Operations aspects of Cyber Prep can be used to define organizational strategy at Tier 2 for that area. For a large or federated organization, Cyber Prep can be used for sub-organizations.
		Risk Management Process: Risk Framing Risk Assessment Risk Response Risk Monitoring	Cyber Prep provides an approach to risk framing with respect to cyber threats. The selection and tailoring of specific aspects can be viewed as risk response at the organizational tier. Threat Intelligence supports risk monitoring at all tiers.
NIST SP 800-30R1 Risk Model [26]	**Intended users:** Organizations performing cyber security risk assessments. **Relevance:** Adversaries are characterized in terms of five levels of capabilities, intent, and targeting. **Focus:** Threats, Consequences	**Types of threat sources** **Five levels of three attributes of adversarial threats:** Capabilities Intent Targeting	Cyber Prep is focused on adversarial threats. The Cyber Prep adversary classes roughly track the levels in NIST SP 800-30R1. The Cyber Prep adversary characteristics can be used to refine the NIST SP 800-30R1 threat model. The NIST SP 800-30R1 threat modeling framework includes representative threat events.
IAB Cyberspace Security Continuum [55]	**Intended users:** Organizational leaders and senior managers. **Relevance:** Organizational programs are characterized in terms of capabilities in six key areas. **Focus:** Governance, Operations	**Three levels of organizational capability** in the areas of governance, processes & procedures, and training & exercises **Matrix mapping capabilities in six functional areas** (security provision, operate and maintain, defend and protect, analyze, investigate, recovery) to the areas of people, processes, and technology	The IAB Cyberspace Security Continuum is brief and high-level guideline. Cyber Prep aspects for different classes can be mapped to the values used to define the three levels.

Source	Description	Elements	Corresponding Elements of Cyber Prep 2.0
CEB Threat Management Maturity Model [19]	**Intended users:** Members of the Information Risk Leadership Council to orient Corporate Information Security Officers (CISOs) to the threat-related aspects of information security risk management. **Relevance:** Four high-level stages of maturity characterize an organization's approach to cyber threats. **Focus**: Operations	**Stages:** 1: Basic Response 2: Organized Operations 3: Advanced Detection and Response 4: Intelligent Prediction and Automation	Correspond to Incident Management: Basic Response: **Basic Hygiene**, **Critical Information Protection** Organized Operations: **Responsive Awareness** Advanced Detection and Response: **Architectural Resilience** Intelligent Prediction and Automation: **Pervasive Agility**
CERT Resilience Management Model (RMM) [12]	**Intended users:** Organizations that seek to manage operational resilience. **Relevance:** Organizations can draw from 26 process areas to identify, assess, and improve their capabilities to continue operations (on a prioritized basis) in the face of adversity. Mapped to NIST SPs [56] and to commercial codes of practice [57]. **Focus**: Operations, Governance	**26 process areas** across **four categories:** Enterprise management Engineering Operations Process management Each process area has a set of goals; each goal has its own specific practices.	Aspects of Cyber Prep Operations and Governance highlight the importance of selected process area goals for cyber resilience.
NACD Cyber-Risk Oversight Director's Handbook [3]	**Intended users:** Members of a corporate Board of Directors. **Relevance:** Five principles are stated. Supporting discussion includes consideration of the CSF: "This level of management may be beyond the practical ability of all organizations, but some elements are available to all companies. Directors should set the expectation that management has considered the NIST Framework in developing the company's cyber-risk defense and response plans." **Focus**: Governance	**Five Principles:** 1. Cybersecurity as an enterprise-wide risk management issue. 2. Legal implications of cyber risks. 3. Adequate access to cybersecurity expertise. 4. Expectation of an enterprise-wide cyber-risk management framework with adequate staffing and budget. (Discusses CSF; cites ISA integrated approach to managing cyber risk.) 5. Risk management strategy.	Cyber Prep is intended to be used by an organization that has adopted the five principles.

Source	Description	Elements	Corresponding Elements of Cyber Prep 2.0
ISA-ANSI, The Financial Management of Cyber Risk [58]	**Intended users:** Chief Financial Officers (CFOs). **Relevance:** Key concepts, motivating questions, and frameworks are identified for activities in six framework areas. **Focus**: Governance, to a lesser extent Operations	**Framework areas:** Understanding and Managing Economic Aspects Managing the Human Element Managing Legal and Compliance Issues Operations and Technology Managing External Communications and Crisis Management Analyzing Financial Risk Transfer and Insurance	All *Governance* aspects corresponding to **Responsive Awareness**, **Cyber Resiliency**, or **Pervasive Agility** Security Posture Assessment, Incident Management, and Training & Readiness corresponding to **Responsive Awareness**, **Cyber Resiliency**, or **Pervasive Agility**
B|A|H Cyber Operations Maturity Framework [13]	**Intended users:** Organizations that seek to develop or improve operational effectiveness against cyber threats. **Relevance:** Eleven key process areas are grouped into four functional areas. Five internal maturity levels, consistent with CMMI, are defined for an organization. Four levels of external maturity are defined; these can be used to characterize the portion of the cyber ecosystem to which the organization belongs. **Focus**: Operations	**Four Operational Functions:** Anticipation Awareness Action After-Action **11 process areas within these**	Process areas correspond to Cyber Prep aspects: Threat Identification & Analysis, Indications & Warning ~ Threat Intelligence & Analysis Systemic Vulnerability Assessment, Continuous Scanning & Monitoring ~ Security Posture Assessment Contingency Planning ~ Adaptability Training & Exercises ~ Training & Readiness Intrusion Detection & Prevention ~ Functionality Impact Analysis, Incident Response ~ Incident Management Forensics & Analysis ~ Forensic Analysis
		Internal Maturity Levels: 1: Ad hoc (chaotic) 2: Defined (Repeatable / Codified) 3: Managed (Controlled) 4: Optimized (Measured) 5: Adaptive (Innovative)	While Cyber Prep is not a maturity model, the characteristics of the Internal Maturity levels correspond roughly to the Cyber Prep classes of *Operations*.
		External Maturity Levels: Isolated Coordinated Collaborative Megacommunity	Roughly correspond to approaches to External Coordination.
HP Security Operations Maturity Model [59]	**Intended users:** Organizations that seek to improve their cyber security posture. **Relevance:** Six maturity levels are defined, for areas in the categories of business (seven areas), people (seven), processes (five), and technology (five).	**Six maturity levels:** Incomplete Initial Repeatable Refined Managed Optimised	While Cyber Prep is not a maturity model, the characteristics of the top five maturity levels roughly track the Cyber Prep classes.

Source	Description	Elements	Corresponding Elements of Cyber Prep 2.0
	Focus: Operations, Governance, Architecture	**Areas:** Business People Processes Technology	People: General and Leadership ~ Governance Structure Process: Specific elements that HP assesses correspond to aspects of *Operations* Technology: Specific elements that HP assesses correspond to aspects of *Architecture & Engineering*
Cybersecurity Maturity Model [21]	**Intended users:** Organizations that seek to improve their cyber security posture. **Relevance:** Five maturity levels are defined, and mapped to three levels of threat. **Focus:** Threat; Operations, Governance, Architecture – but only described in general terms	**Three threat levels:** Conventional Threat Advanced Persistent Threat Nation State	Conventional Threat ~ **Cyber Vandalism**, **Cyber Breach & Organizational Disruption** APT ~ **Cyber Breach & Organizational Disruption** Nation State ~ **Cyber Espionage & Extensive Disruption**, **Cyber-Supported Strategic Disruption**
		Five maturity levels: Reactive and Manual Tools-Based Integrated Picture Dynamic Defense Resilient Enterprise	Reactive & Manual ~ **Basic Hygiene** Tools-Based ~ **Critical Information Protection** Integrated Picture ~ **Responsive Awareness** Dynamic Defense, Resilient Enterprise ~ **Architectural Resilience**
Cybersecurity Capability Maturity Model (C2M2) [60] (derived from [61])	**Intended users:** Organizations that seek to improve their cyber security posture. Particularly relevant to critical infrastructure organizations which manage operational technology (OT) as well as information technology (IT) **Relevance:** Three maturity levels are defined, for ten domains.	**Four maturity indicator levels (MILs)**, simply referred to as MIL0-MIL3	While Cyber Prep is not a maturity model, the characteristics of the maturity levels roughly track the top three Cyber Prep classes in the areas shown below. The descriptions of the maturity levels in those areas can be used to add more detail to a strategy developed using Cyber Prep.
		Ten domains: Risk Management Asset, Change, & Configuration Management Identify & Access Management Threat & Vulnerability Management Situational Awareness Information Sharing & Communications Event & Incident Response, Continuity of Operations Supply Chain & External Dependencies Management Workforce Management Cybersecurity Program Management	Risk Management ~ Internal Integration Asset, Change, & Configuration Management ~ Security Posture Assessment Identify & Access Management ~ Security Posture Assessment Threat & Vulnerability Management, Situational Awareness ~ Security Posture Assessment Information Sharing & Communications ~ External Coordination Event & Incident Response, Continuity of Operations ~ Adaptability, Incident Management Supply Chain & External Dependencies Management, Workforce Management ~ Governance Structure Cybersecurity Program Management ~ Governance Structure

Source	Description	Elements	Corresponding Elements of Cyber Prep 2.0
Cyber Maturity Scale [62]	**Intended users:** Organizations that seek to improve their cyber security posture. **Relevance:** Five maturity levels are defined, for the areas of people, processes, and technology. **Focus:** Threat; Operations, Governance, Architecture – but each organization must identify the key capabilities it seeks to mature	**Five maturity levels:** Initial Repeatable Refined Managed Optimised	While Cyber Prep is not a maturity model, the characteristics of the maturity levels roughly track the values of the aspects identified below.
		Areas: People Processes Technology	People ~ Governance Structure Processes ~ Internal Integration Technology ~ Mitigation Philosophy
Community Cyber Security Maturity Model (CCSMM) [22] [15]	**Intended users:** Organizations, communities, and states that seek to improve their cyber security posture. **Relevance:** Five maturity levels are defined, for six areas. **Focus:** Threat; Operations, Governance, Architecture – levels of each area are described in general terms	**Five maturity levels:** Initial Advanced Self-Assessed Integrated Vanguard	Initial ~ **Basic Hygiene**, **Critical Information Protection** Advanced, Self-Assessed ~ **Responsive Awareness** Integrated, Vanguard ~ **Architectural Resilience**
		Areas: Threats Metrics Information Sharing Technology Training Testing	Threats: Unstructured Threats ~ **Cyber Vandalism**, **Cyber Incursion**; Structured Threats ~ **Cyber Breach**; Highly Structured Threats ~ **Cyber Espionage & Extensive Disruption**, **Cyber-Supported Strategic Disruption** Information Sharing ~ External Coordination, Threat Intelligence & Analysis Training, Testing ~ Training & Awareness
Cyber Resiliency Engineering Framework (CREF) [63] [64] [65] [66]	**Intended users:** Systems engineers and enterprise architects, who seek to ensure system and mission resilience against advanced cyber threats **Focus:** Architecture **Relevance:** The Architecture aspects of Responsive Awareness, Architectural Resilience, and Pervasive Agility use the CREF goals and objectives.	**Goals:** Anticipate, Withstand, Recover, Evolve	**Architectural Resilience**, **Pervasive Agility** *Governance* **Responsive Awareness**, **Architectural Resilience**, **Pervasive Agility** *Architecture & Engineering* (Functionality, Versatility)
		Objectives: Understand, Prepare, Prevent / Avoid, Continue, Constrain, Reconstitute, Transform, and Re-Architect	**Responsive Awareness**, **Architectural Resilience**, **Pervasive Agility** *Architecture & Engineering* (Functionality, Versatility)
		Techniques: Adaptive Response, Analytic Monitoring, Coordinated Defense, Deception, Diversity, Dynamic Positioning, Dynamic Representation, Non-Persistence, Privilege Restriction, Realignment, Redundancy, Segmentation, Substantiated Integrity, Unpredictability	Can be used to achieve Functionality for **Responsive Awareness**, **Architectural Resilience**, **Pervasive Agility**

Source	Description	Elements	Corresponding Elements of Cyber Prep 2.0
LogRhythm Security Intelligence Maturity Model [67] [68]	**Intended users:** Organizations **Focus**: Operations **Relevance:** Links capability levels with time to respond	**Characteristics:** Defines two classes of characteristics: Organizational (five risk characteristics) and Security Intelligence (ten capabilities)	Organizational risk characteristics correspond to Threat type; Security Intelligence capabilities correspond to *Operations* and some Functionality
World Economic Forum Maturity Model for Organizational Cyber Resilience [69]	**Intended users:** Organizations **Focus:** Governance	**Characteristics:** Defines capabilities to be included in an organization's governance, cyber risk management program, and external relationships Provides a C-suite questionnaire to determine the organization's maturity level	Can be used in conjunction with Cyber Prep *Governance* aspects; describes some programmatic aspects in more detail

A variety of other frameworks and models are more specialized. These can be used to help develop more detailed strategies for specific aspects of Cyber Prep.

- The DHS Cybersecurity Capability Maturity Model [16] is designed to help organizations with cybersecurity workforce planning. It categorizes cybersecurity workforce development activities in three major areas: Process and Analytics, Integrated Governance, and Skilled Practicioners and Enabling Technologies. Workforce development is part of the Governance Structure aspect of the Cyber Prep area of Governance.
- The CREST Cybersecurity Incident Response Maturity Assessment Model [14] can be used for detailed planning in the Incident Management aspect of the Cyber Prep area of Operations.

Cyber Prep is informed by the DACS (Describing and Analyzing Cyber Strategies, [7]) framework, and an organization can use questions generated from, or alternatives articulated in, the DACS framework to articulate its strategy.

- DACS defines five strata of actors, on the defender and adversary sides. On the defender side, an organization (the target user of Cyber Prep) is the middle stratum. The five strata of adversary actors in DACS correspond to the five scopes of adversary activities in Cyber Prep (see Section 3.2).
- DACS defines three aspects of an actor's strategy that could be affected by the decisions and actions of actors on the other side: capabilities, intent, targeting, and timeframe. On the defender side, these aspects are represented in the areas and aspects of Cyber Prep.
    - DACS identifies three major types of capabilities: *methods* (pre-planned applications of resources), *resources* that can be directed or allocated, and *relationships*. DACS further identifies three broad types of *resources* that can be directed or allocated: technical, financial, and organizational. Consideration of financial and organizational resources in an organization's strategy is reflected in the Governance Structure aspect of Cyber Prep. Other governance-related organizational resources are reflected in the Adaptability and Internal Integration aspects. DACS identifies two sub-types of technical resources (technological and informational). *Technological resources* include tools (e.g., intrusion detection systems) and technologies (e.g., moving target defenses), supported by processes and personnel. *Informational resources* consist of sharable or reusable knowledge about vulnerabilities, strengths, and defensible configurations of specific technologies or products; malware, indicators, and adversary TTPs; and threat trends. Consideration of technological resources in an organization's strategy is reflected in the Architecture area Cyber Prep, particularly in Functionality, as well as in the Security Posture Assessment and Forensic Analysis aspects of Operations. Consideration of informational resources is reflected in Governance (External Coordination), Operations (Threat Intelligence & Analysis, Training & Readiness), and Architecture (Security Engineering Orientation).
    - DACS identifies three aspects of intent: non-cyber goals, cyber goals, and risk trade-offs. Consideration of non-cyber goals is reflected in the Internal Integration aspect of Governance, while cyber goals are reflected in the Incident Management aspect of Operations. Risk trade-offs are reflected in the Mitigation Philosophy aspect of Governance, and the Versatility aspect of Architecture.
    - Targeting – the prioritization of classes of adversaries, or of specific adversaries, against whose activities the organization will focus its efforts – is driven largely by the organization's intent, and its orientation to a class of adversaries. Thus, an organization's Cyber Prep class, and its characterization of its adversaries, are expressions of its targeting.

Appendix C Glossary and Abbreviations

C.1 Glossary

Term	Definition
Advanced Persistent Threat	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. [6]
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. [70] [26]
Adverse Cyber Event	An event involving cyber resources that has adverse consequences for cyber resources, mission or business functions, an organization, an individual or set of individuals, a critical infrastructure sector, a region, or the nation. Adverse cyber events include, but are not limited to, cyber attacks.
Anticipate	(Cyber Resiliency Goal) Maintain a state of informed preparedness for adversity. [71] [63] [64]
Asset	(1) An item of value to achievement of organizational mission/business objectives. *Note 1:* Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organizational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organization. *Note 2:* An asset may be tangible (e.g., physical item such as hardware, software, firmware, computing platform, network device, or other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation). [72] (2) An item, capability, or service of value to achievement of organizational mission or business objectives.
Availability	Ensuring timely and reliable access to and use of information. [73] *Note:* Mission/business resiliency objectives extend the concept of availability to refer to a point-in-time availability (i.e., the system, component, or device is usable when needed) and the continuity of availability (i.e., the system, component, or device remains usable for the duration of the time it is needed). [72]
Collaboration	The parties plan for, allocate resources to, and jointly manage activities to achieve a common goal or address a common problem; these activities are designed to avoid impeding or negating one another's efforts. [7]
Computer Network Defense (CND)	Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. [51] Note that this term has been superseded by defensive cyberspace operations.

Term	Definition
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [72] [73]
Constrain	(Cyber Resiliency Objective) Limit damage from adversity. [71] [63] [64]
Continue	(Cyber Resiliency Objective) Maximize the duration and viability of essential mission/business functions during adversity. [71] [63] [64]
Conventional Cyber Threat (or Cyber Adversary)	An adversary addressed by established standards of good practice, and in particular by the baselines in NIST SP 800-53R4 [38]. Conventional cyber adversaries include hackers using malware and TTPs easily recognized by malware and intrusion detection systems, as well as insiders abusing their privileges.
Cooperation	The parties seek to achieve a common goal or address a common problem, and to avoid impeding or negating one another's efforts. [7]
Coordination	The parties plan for, allocate resources to, and manage separate activities to achieve a common goal or address a common problem; these activities are designed to avoid impeding or negating one another's efforts. [7]
Criticality Level	Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level. [70]
Cyber	A modifier that indicates a presence in, or involvement with, cyberspace.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [51] [74]
Cyber Course of Action	A set of activities by cyber defenders (e.g., DCO staff; staff in a Security Operations Center or a Cyber Security Operations Center) and, as needed, other cyber staff (e.g., staff in a Cyber Operations Center, system administrators, network operators) and mission staff in response to adverse cyber events.
Cyber Defender	An individual responsible for defending organizational mission, systems, networks, and devices by detecting, analyzing, responding to, reporting on, and thwarting cyber attacks. Note: A cyber defender is typically assigned to a Security Operations Center (SOC). The role of cyber defender is distinct from that of a system administrator, security administrator, or cybersecurity staff member.
Cyber Event	An event involving cyber resources.[37]
Cyber Intelligence Report	Formal and informal reports from SOCs, commercial vendors, independent security researchers, or independent security research groups that discuss information about attempted or confirmed intrusion activity, threats, vulnerabilities, or adversary TTPs, often including specific attack indicators. [40]

[37] Note that [1] provides the following definition of "cybersecurity event": "A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)."

Cyber Preparedness	Preparedness to handle cyber attacks as well as stealthy malicious cyber activities over extended periods. Note: Cyber preparedness can be a property of an organization, region, sector, mission, or nation.
Cyber Resiliency	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks. [1]
Cybersecurity Staff	(1) Individuals, typically working in the office of a Chief Information Security Officer or equivalent role, responsible for performing analyses and drafting policies and procedures. (2) Individuals who have been assigned responsibility for enforcing some aspects of the organization's cybersecurity policies and/or carrying out specific cybersecurity procedures. Note: For purposes of distinguishing between preparedness levels, this phrase is used to contrast with "cyber defender." Defensive cyberspace operations are a secondary responsibility, at best, of cybersecurity staff.
Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [51]
Cyberspace Attack	Cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. [70]
Cyber Risk	Risk due to malicious cyber activity (MCA).
Cyber Threat Analyst	A cyber defender responsible for analyzing and generating cyber intelligence reports as well as for creating, sharing, and analyzing detailed cyber threat information.
Cyber Threat Information	Information about cyber attacks, activities by cyber adversaries, vulnerabilities, and potential defender actions, including observables, incidents, adversary TTPs, exploit targets, cyber courses of action, cyber campaigns, and cyber threat actors. (derived from [48])
Data Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. [70]
Defensive Cyberspace Operations	Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called DCO. [75]
Detect	(CSF Functional Area) Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. [1]
Disruption	An unplanned event that causes a system, application, or service to be inoperable or to operate at an unacceptable level of service, for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). ([70], adapted)

Enterprise Architecture (EA)	(1) The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. [51] (2) A strategic information asset base, which defines the mission; the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture, a target architecture, and a sequencing plan. [76] [70] (3) An enterprise architecture (EA) is a conceptual blueprint that defines the structure and operation of an organization. The intent of an enterprise architecture is to determine how an organization can most effectively achieve its current and future objectives. [52]
Evolve	(Cyber Resiliency Goal) Adapt mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments. [71] [63] [64]
Forensic Analyst	A cyber defender responsible for analyzing artifacts (e.g., malware) and damage from cyber attacks.
Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. [70]
Friction Avoidance	The parties seek to avoid impeding or negating one another's efforts to address a common problem. [7]
Identify	(CSF Functional Area) Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. [1]
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. [26]
Integrity	(Information) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [73] [72] Note: This term typically includes both data integrity and system integrity.
Malicious Cyber Activity	Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon. [77]

Mission Assurance	The ability of operators to achieve their mission, continue critical processes, and protect people and assets in the face of internal and external attack (both physical and cyber), unforeseen environmental or operational changes, and system malfunctions. [78] Both an integrative framework and a process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains - critical to the performance of DoD MEFs in any operating environment or condition. [79]
Operational Resilience	The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions. [70]
Prepare	(Cyber Resiliency Objective) Maintain a set of realistic courses of action that address predicted or anticipated adversity. [71] [63] [64]
Prevent / Avoid	(Cyber Resiliency Objective) Preclude successful execution of attack or the realization of adverse conditions. [71] [63] [64]
Protect	(CSF Functional Area) Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. [1]
Re-Architect	(Cyber Resiliency Objective) Modify architectures to handle adversity more effectively. [71] [63] [64]
Reconstitute	(Cyber Resiliency Objective) Restore as much mission/business functionality as possible subsequent to adversity. [71] [63] [64]
Recover	(Cyber Resiliency Goal) Restore mission/business functions during and after adversity. [71] [63] [64] (CSF Functional Area) Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. [1]
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. [70] [80]
Resource	An asset or a component of, or a service or capability provided by, a system, which can be used by multiple mission / business functions. This term is defined so that cyber resources can be defined.[38] General examples of cyber resources include capacity (bandwidth, processing, and storage), hardware, software, firmware, and services. Other examples are more system- or mission/business process-specific, and can include information (which can be in a specific form such as a database, or of a specified quality) as well as computing or networking services subject to service level agreements (SLAs).
Respond	(CSF Functional Area) Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. [1]

[38] Note that [51] provides the following definition of "information resources": "Information and related resources, such as personnel, equipment, funds, and information technology."

Risk Frame	The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. Establishing a realistic and credible risk frame requires that organizations identify: (i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses). [6]
Security Architecture	A description of the structure and behavior of an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. ([51], IA architecture, adapted)
Security Operations Center (SOC)	A team composed primarily of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents. [40]
Security Posture	The security status of an enterprise's networks, information, and systems, as determined by resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. ([51], adapted)
Sensitivity	A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. [70]
Situational Awareness (SA)	Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future. [51]
Stepping-Stone Attack	An attack designed to acquire and maintain a foothold in one organization's systems, as a launching point for attacks on another organization.
Supply Chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. [70]
Supply Chain Attack	Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. [70]
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. [70]
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [70] [26]

Transform	(Cyber Resiliency Objective) Modify mission / business functions and supporting processes to handle adversity more effectively. [71] [63] [64]
Understand	(Cyber Resiliency Objective) Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity. [71] [63] [64]
Withstand	(Cyber Resiliency Goal) Continue essential mission/business functions despite adversity. [71] [63] [64]

C.2 List of Abbreviations

ACSC	Advanced Cyber Security Center
APT	Advanced Persistent Threat
ATT&CK™	Adversarial Tactics, Techniques, and Common Knowledge
C2	Command and Control
CAL	Cyber Attack Lifecycle
CAPEC	Common Attack Pattern Enumeration and Classification
CDM	Continuous Diagnostics and Monitoring
CEO	Chief Executive Officer
CI	Critical Infrastructure (sector)
CKC	Cyber Kill Chain
CND	Computer Network Defense
CNSS	Committee on National Security Systems
COOP	Continuity of Operations (or Continuity of Operations Planning)
COTS	Commercial Off-the-Shelf
CP	Cyber Prep
CRR	(DHS) Cyber Resilience Review
CS	Cybersecurity
CSF	(NIST) Cybersecurity Framework
DACS	Describing and Analyzing Cyber Strategies (framework)
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DMD	Decision Making Disruptions
DoD	Department of Defense
DOE	Department of Energy

DoS	Denial of Service
DSB	Defense Science Board
EA	Enterprise Architecture
FFIEC	Federal Financial Institutions Examination Council
HITRUST	Health Information Trust Alliance
I&W	Indications and Warning
IAB	Inter Agency Board
ISAO	Information Sharing and Analysis Organization
ICT	Information and Communications Technology
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
JTF	Joint Task Force Transformation Initiative
LE	Law Enforcement
MA	Mission Assurance
MCA	Malicious Cyber Activities (or Activity)
MIL	Maturity Indicator Level
NACD	National Association of Corporate Directors
NIST	National Institute of Standards and Technology
OPSEC	Operations Security
OT	Operational Technology
PII	Personally Identifiable Information
POC	Point of Contact
RMM	(CERT) Resilience Management Model™
SA	Situational Awareness
SCRM	Supply Chain Risk Management
SLA	Service Level Agreement
SOC	Security Operations Center
SP	Special Publication
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TTPs	Tactics, Techniques, and Procedures