Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Threat Preparedness

Deb Bodeau
dbodeau@mitre.org

Richard Graubart
rdg@mitre.org

As cyber threats evolve, organizations increasingly need to define their strategies for cyber security, defense, and resilience. Cyber Prep 2.0 is a threat-oriented approach that allows an organization to define and articulate its threat assumptions, and to develop organization-appropriate, tailored strategic elements. While Cyber Prep 2.0 focuses on advanced threats and corresponding elements of organizational strategy, it includes material related to conventional cyber threats. Cyber Prep 2.0 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.

1 Organizations Need to Prepare for Cyber Threats

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 Reports of major data breaches, campaigns by advanced actors, and marketplaces in malware and unpublished vulnerabilities have raised the awareness of Government and business leaders that cybersecurity and resilience must be considered as part of enterprise risk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

At the same time, as depicted in Figure 1, the landscape of resources – frameworks, guidelines, information sharing efforts, and commercial services – related to cyber risk management continues to increase in size and complexity. Government has undertaken the transition from compliance-oriented to risk-management thinking, while the private sector and public-private partnerships have promulgated numerous cybersecurity-related frameworks and guidance. Threat information sharing – in the form of reports, mechanisms for automated exchange, and partnerships or other efforts – is recognized as vital to cyber defense.

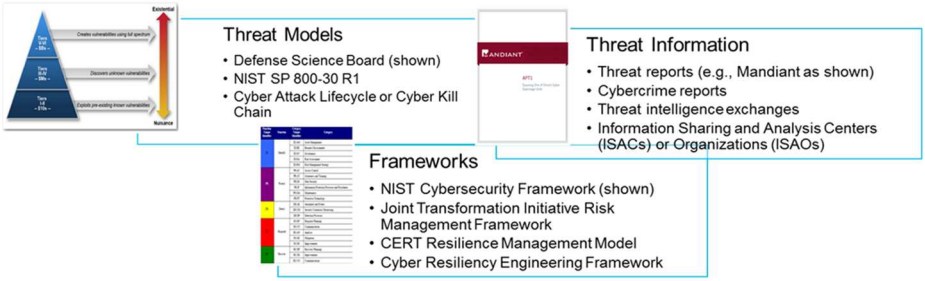

Figure 1. Organizations Must Navigate an Increasingly Complex Cybersecurity Landscape

These resources vary in their underlying assumptions about the nature of the cyber threat. Some explicitly assume conventional threats (e.g., disgruntled or suborned insiders, denial-of-service attacks, hackers who have obtained legitimate user credentials). Others, while mentioning advanced cyber threats, do not consider the need for resilience in the face of ongoing, stealthy campaigns, or the need to prepare for attacks which cross organizational boundaries. 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 cybersecurity resources landscape to determine which resources will be relevant and useful.

2 Cyber Prep

Cyber Prep recognizes that cyber preparedness – organizational preparedness to handle cyber attacks – has become an integral part of cyber risk management,[1] which in turn has become integral to enterprise risk management [1]. For ease of exposition, Cyber Prep[2] defines five broad classes or levels of adversarial threats and five corresponding classes of organizational preparedness strategies. To move beyond these broad classes, Cyber Prep provides a threat modeling framework; it then links uses adversary characteristics to motivate aspects of strategy in three interdependent areas:

- 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 advanced persistent threat (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 NIST Cybersecurity Framework (CSF) core functions; do they go beyond the CSF and address aspects of cyber resiliency? What is the organization's security engineering orientation?

The choice of a target level for a given aspect in an area (e.g., the level of Internal Integration in the area of Governance) is driven by specific adversary characteristics (e.g., persistence, capabilities).

2.1 The Cyber Prep Toolset

Cyber Prep is designed to be used at successive levels of refinement and detail, in terms of both its threat model and the aspects of the three strategic areas (Governance, Operations, and Architecture & Engineering). Thus, Cyber Prep provides a toolset of models, questions, and tables at different levels of detail. As described in Section 3 below, a first approximation is the assumption about the type of threat (conventional vs. advanced) and the corresponding risk management philosophy (practice-driven vs. threat-oriented); a second approximation uses the five broad classes of adversaries and strategies to help an organization characterize its preparedness posture.

Next, as discussed in Section 4, Cyber Prep provides a threat modeling framework, focused on why an adversary might persistently target an organization. This enables an organization to clarify its threat assumptions – to define its threat model. Cyber Prep then enables an organization to motivate (in terms of adversary characteristics) and articulate (in terms of aspects of architecture, operations, and governance) the elements of its preparedness strategy, thus helping the organization to develop a strategic roadmap. As a next approximation, Section 5 presents an initial high-level characterization of preparedness strategies. In more detail, Cyber Prep includes tables defining tailorable descriptions of

[1] "Cyber risk management" is the management of cyber risks, i.e., risks of depending on cyberspace, particularly risks due to malicious cyber activities (MCA) [12]. Cyber risk is a subset of information security risk, as defined in NIST SP 800-30R1 [3].
[2] Cyber Prep 2.0 updates and supersedes MITRE's previous Cyber Prep methodology [13].

each aspect of the three strategic areas, for five classes of preparedness. Cyber Prep also includes mappings from adversary characteristics to target classes of preparedness for each aspect.

Finally, as described in Section 6, by enabling an organization to clarify its assumptions and describe key aspects of its cybersecurity strategy, Cyber Prep enables an organization to tailor and integrate concepts, guidance, and elements from a variety of frameworks and guidelines. In particular, Cyber Prep enables an organization to decide which portions of other frameworks (e.g., NIST Cybersecurity Framework) are relevant, and to develop a roadmap for applying those portions over time.

As the threat landscape has evolved, an understanding of adversaries and the potential impacts of their activities has become more important to organizations seeking to define a tailored and cost-effective cyber strategy. An organization can use the Cyber Prep threat model and 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 establish supporting policies and procedures or to resource the products and tools to make them operational.

2.2 Distinguishing Features of Cyber Prep

Cyber Prep is a practical approach, providing multiple tools which an organization can use to articulate its strategy for addressing advanced cyber threats. It provides motivation for technical investments and organizational evolution. Distinguishing characteristics of Cyber Prep include:

- Cyber Prep looks at both the *threat* organizations face and the *measures* that organizations may take to defend themselves, making explicit the *relationship* between the 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 thus to motivate specific elements of its cyber preparedness strategy.
- While many frameworks focus on one dimension (e.g., adversary capabilities, or the operational aspect of the defender), Cyber Prep represents multiple dimensions of both the attacker and defender:
    - For the Attacker, Cyber Prep considers Intent (e.g., financial gain, geopolitical advantage), Scope, Timeframe, and Capabilities (e.g., resources, expertise).
    - For the Defender, Cyber Prep considers Governance (e.g., organizational roles), Operations (e.g., proactive vs. reactive posture, stages of the cyber attack lifecycle[3] (CAL) addressed), and Architecture & Engineering (e.g., how well-defined the security architecture is, how the organization approaches security engineering).
- Cyber Prep facilitates definition and articulation of threat assumptions and concerns, and identification of tailored strategic elements, 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 five different preparedness strategies, Cyber Prep assumes that the organization will pick and choose strategic goals based on such considerations

[3] Cyber attack lifecycle stages used in this paper are based on the structure of an APT campaign as defined in NIST 800-30 Rev 1, App E [2].

as size, culture, and legal, regulatory, and contractual constraints, rather than taking an all-or-nothing approach as in a compliance or maturity model.

- Cyber Prep can be used in standalone fashion and/or it can be used to complement, link and extend the use of other, more detailed frameworks (e.g., the NIST Cybersecurity Framework) and threat models.[4]

3 Initial Orientation

The first tools in the Cyber Prep toolset are intended to help an organization orient to the threat, rather than taking a compliance mindset. As a first approximation, Cyber Prep identifies two types of adversary – 1) *conventional* and 2) *advanced* – which correspond to two risk management philosophies – 1) threat-agnostic or *practice-driven* and 2) *threat-oriented*. While malware and vulnerability marketplaces put sophisticated tools into the hands of conventional adversaries, the strategies and procedures of such adversaries are relatively static, and can largely be addressed by standards of good practice. Advanced adversaries, by contrast, learn, evolve, and cannot be addressed by a good-practice, compliance-oriented strategy. A threat-oriented preparedness strategy builds on good practice, but provides ways to make trade-offs based on an appreciation of why an advanced adversary might target the organization.

While Cyber Prep 2.0 focuses on advanced threats and corresponding elements of organizational strategy, it includes material related to conventional cyber threats. Advanced cyber threats often take advantage of weaknesses in an organization's foundational practices, using tactics, techniques, and procedures (TTPs) typical of conventional adversaries. Thus, an organization can and should take good practices into consideration, while recognizing that these are insufficient to address advanced threats.

One advantage of moving from a practice-driven to a threat-oriented approach is that any organization's cybersecurity resources are limited. In addition, an organization's strategic choices are constrained by such factors as organizational culture and risk tolerance, legacy investments, partnership or customer agreements, and the size and quality of the cybersecurity workforce. Thus, any organization must make trade-offs among the practices it implements. Cost-effectiveness can be improved by informing those trade-offs with an understanding of the cyber threats for which the organization must best be prepared.

While these two 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. As a second approximation, Cyber Prep defines five classes or levels of adversary, based primarily on the adversary's goals, and five corresponding preparedness strategies. These are illustrated in Figure 2.

[4] Examples of cybersecurity frameworks include the NIST Cybersecurity Framework (CSF) [2], the Joint Transformation Initiative risk management process [5], the CERT Resilience Management Model [6], the Booz | Allen | Hamilton Cyber Operations Maturity Framework [7], and the Cyber Resiliency Engineering Framework [8] [9]. Examples of threat models include the Defense Science Board's model [4], as well as models of the cyber kill chain [10] or cyber attack lifecycle [3] [11].

Figure 2. Cyber Prep Classes

The set of Cyber Prep classes provides a means for an organization to

- Articulate its risk frame, and in particular its understanding of cyber threats, as illustrated in Table 1. This risk framing focus allows Cyber Prep to complement various risk management processes (e.g., the NIST organizational risk management process) and frameworks (e.g., the NIST Cybersecurity Framework).
- Define its overall strategy succinctly, in terms of the types of adversaries it faces, and the approaches it takes in order to be prepared for attacks by such adversaries. This is illustrated in Table 2.[5]
- Identify high-level mismatches between its risk frame and its overall strategy. For example, a practice-driven organization might take a Critical Information Protection strategy, but face a persistent adversary seeking Cyber Breach.

The five classes are characterized in terms of the organization's cyber threat model[6] and its overall strategy for addressing the cyber threat. The statements in these tables are representative examples, and for the sake of brevity, use terminology from the NIST Cybersecurity Framework [2] and NIST SP 800-30R1 [3].

It must be emphasized that these characterizations are designed to serve as a starting point for discussion. Follow-on questions related to why an organization might be targeted can be accompanied by threat briefings illustrating ways in which the five classes overlap. For example, an attack might be typical of a Cyber Incursion, but involve more advanced capabilities. An organization's strategy might be primarily characterized as Responsive Awareness, but include elements of Critical Information Protection and Cyber Resilience.

[5] Note that bolding in these and other tables in this document indicates a change from the previous level.
[6] A threat model identifies the characteristics of a threat, can also identify a representative or comprehensive set of threat events, and can include one or more approaches to creating threat scenarios. Cyber Prep restricts attention to adversary characteristics, since adversary tactics, techniques, and procedures (TTPs) evolve quickly and organizations increasingly assemble sets of potentially relevant threat events through threat intelligence information sharing activities.

Table 1. Characterizing the Threat

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 Cyber Attack Lifecycle (CAL): recon, deliver, exploit, control (limited), execute; limited concern for stealth** Examples of Effects: **Data breach, 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 & Extended Disruption	Goals: Financial gain (fraud, salable information, extortion), Geopolitical advantage (**all types**) 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 (all types) Scope: Organizational Operations **for selected organizations**; Sector; **Nation** Timeframe, Persistence, and Stealth: **Strategic 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**

Table 2. Representative Characterization 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**[7]**.** 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**. 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**.
Cyber 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, **strategic** 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.

4 Orient to the Threat

Cyber Prep provides a threat modeling framework to enable an organization to orient to the threat. An organization begins by considering why an adversary might target organizational systems. An organization can be profiled in terms of four aspects:

- Assets: What the organization *has*. Assets are categorized as information, money, and capacity.
- Missions: What the organization *does*. This includes not only key mission or business functions, but also supporting functions, and in abnormal as well as normal circumstances.

[7] Levels of Capability, Intent and Targeting are as defined in NIST SP 800-30 [3].

- Role: What the organization's *place* in the cyber ecosystem is. In particular, an organization can be attacked as a stepping stone in an attack on one of its partners or customers.
- Symbolism: What the organization *represents*.

A set of questions help develop the organization's profile as a target. Based on that profile, its cyber adversaries can be characterized, and organizational concerns for consequences of attacks can be elicited.

4.1 Characterize the Adversary

The first key characteristic, related to why an adversary might persistently and stealthily target the organization, is the adversary goal or goals corresponding to assets, mission, role, and symbolism. Typical adversary goals include

- Financial gain (e.g., fraud, theft, or exfiltration of salable information)
- Geopolitical advantage (e.g., terrorism; undermining public confidence in institutions or infrastructures; or economic, diplomatic, or military advantage)
- Cyber advantage (e.g., acquiring stepping stones or resources for future attacks)
- Personal motives (e.g., attention, malice)

Other characteristics are driven by how valuable a target the organization is – for example, how much money it handles, how much sensitive information it retains, how crucial its missions are. These characteristics include:

- At what scope or in what arena does the 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.
- 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?
- In what timeframe does the adversary operate? Will the adversary's activities be periodic or episodic, or will the adversary commit to a sustained effort against the organization?

An organization may well have multiple answers to these questions, identifying multiple types of adversaries, based on the different ways in which it could be a target. Because the strategies to address different types of adversaries can differ, an organization may need to consider each type in developing strategic plans, rather than simply making a worst-case assumption. However, for ease of exposition, the worst-case assumption or high-water mark of these characteristics can be used to describe the organization's adversary class.

4.2 Consider Potential Consequences

After characterizing the adversary, an organization can make an assessment of the types of organizational or operational consequences of adversary activities. In effect, an organization asks: *How much impact would result if an adversary successfully achieves its goals?* The impacts can range from

- Limited or near-term: Will have 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: Will have 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: Will have 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 an organization might be, Cyber Prep provides a mapping from potential cyber effects (e.g., degradation or disruption of service; corruption, modification, or insertion of information; or exfiltration, interception, or other compromise of information) to adversary goals as well as to organizational assets, missions, or critical business functions.

5 Characterize Target Organizational Preparedness

An organization's target cyber preparedness strategy is based on the adversary (or set of adversaries) that could affect its operations and future viability. An organization can use the characterizations of Cyber Prep classes to assess its current strategy and to define its target strategy. As a next approximation, an organization can do this initially at a high level, as illustrated in Table 3 on the following page. Note that the table identifies only a few typical characteristics of an organization for each class. An organization can choose to use Cyber Prep to drill down in the areas of Governance, Operations, and Architecture & Engineering, and in selected key aspects of these areas, as needed to define its target strategy well enough to use a more detailed framework and/or to develop a strategic roadmap.

Even when the characteristics are described in such high-level terms, it will often be the case that an organization's strategy is a hybrid, for example combining the Governance aspects of one class with the Operations aspect of another, and the Architecture & Engineering aspects of a third. When the organization drills down, Cyber Prep is designed to support such variation. Moreover, the three broad areas (Governance, Operations, and Architecture & Engineering) are themselves comprised of various aspects, accommodating further organization-specific tailoring. Organizations can use various factors, including risk tolerance and resource limitations, to determine which characteristics of each aspect are most appropriate for the organization to select and emphasize.

One important linkage must be emphasized: Multiple aspects of Architecture & Engineering depend on aspects of Operations, and in turn multiple aspects of Operations depend on aspects of Governance. For example, an organization that seeks to improve its overall cybersecurity often starts by acquiring cybersecurity products and tools (Architecture & Engineering), and then abandoning them because it lacks the expertise or sufficient staff (Operations) to use them effectively. Similarly, cybersecurity staff (Operations) in an organization that has not made a commitment to managing cybersecurity risk (Governance) will be overburdened, often asked to perform security tasks as an additional duty, or under-resourced. And some organizations' risk mitigation philosophy (Governance) restricts the types of tools (Architecture & Engineering) they will use.

Table 3. Characterizing Organizational Preparedness

Class	Organizational Cyber Preparedness 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**.
Cyber 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,** 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.** 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.

6 Applying Cyber Prep with Other Frameworks

The breadth of Cyber Prep – including adversary characteristics and aspects of an organization's architectural, operational, and governance strategy – enables it to be used to index into other frameworks. For example, the capability aspect of Cyber Prep threat classes roughly correspond to the Tiers of the DSB threat model [4], the Governance area of the first four Cyber Prep classes roughly correspond to Tiers 1-4 of the NIST Cybersecurity Framework [2], and some of the aspects of Governance in Cyber Prep are analogous to aspects of the governance and risk assessment capabilities of the CSF Core.

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 [5]. 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 identify a starting point for using that framework in defining 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.

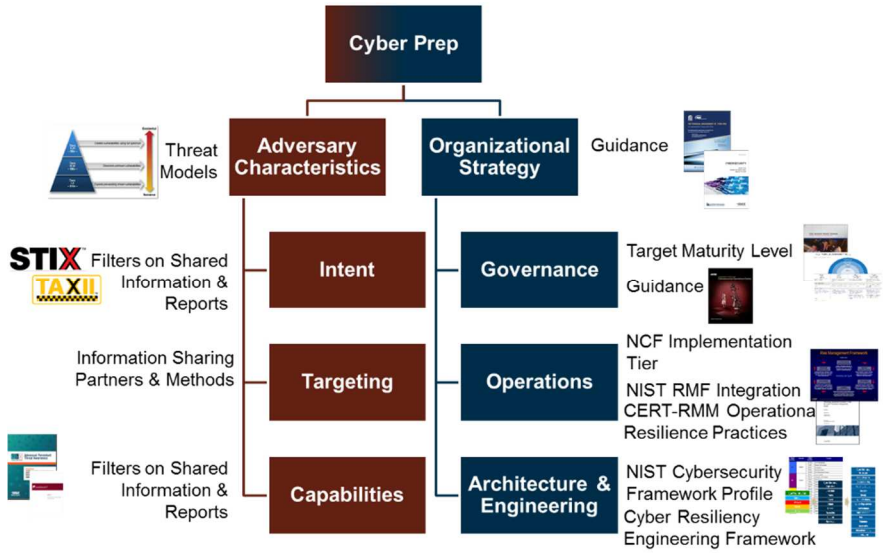

Figure 3. Cyber Prep 2.0 Enables the Organization to Use Appropriate Resources

7 Summary

Cyber Prep provides concepts, terminology, and characteristics that an organization can use to articulate its risk frame for cyber risks – its assumptions about the cyber threat it faces and the potential consequences of greatest concern, the constraints on its cyber risk management decisions, its cyber risk tolerance, and its risk-related strategic trade-offs. Cyber Prep enables an organization to characterize

the class of threat it faces and its overall approach to cyber preparedness. This high-level characterization provides motivation for the organization's cybersecurity strategy.

The organization's target cyber preparedness posture implies functional areas in which the organization needs capabilities, as well as its operational strategy for addressing activities at different stages in the cyber attack lifecycle. As an organization develops its cyber preparedness strategy, Cyber Prep provides characterizations in the areas of Governance, Operations, and Architecture & Engineering that the organization might target, and characteristics of more specific aspects if the organization seeks further details. Because Cyber Prep has been mapped to a variety of more detailed frameworks, an organization can use its target Cyber Prep class (or target class in the areas of governance, operations, architecture, or in more specific aspects) to identify the portions of those frameworks that are most relevant to the organization.

References

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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].

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

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.