Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels

Deb Bodeau (db@mitre.org),
Richard Graubart (rdg@mitre.org),
Jennifer Fabius Greene (jgreene@mitre.org)

Executive Summary

The MITRE-developed cyber preparedness (Cyber Prep) framework provides an approach for

- addressing the cyber threats that an organization or mission faces;
- determining the level of preparedness necessary to ensure mission success;
- facilitating strategic planning for cyber security by setting preparedness objectives; and
- assisting in the prioritization of cyber security investment planning and management decisions.

The nature of cyber threats in general – and advanced cyber threats in particular – requires a longer-term commitment from senior leadership, including vision, strategy, and investment prioritization as well as the organizational agility to respond to ever-changing tactics and techniques. This paper provides recommendations on how to characterize an organization's cyber threat environment and identifies a number of defensive tools and techniques that will provide a solid start for improving security and resiliency against advanced cyber threats. With broad adoption, the five Cyber Prep levels are expected to provide a simple and common method for assessing the degree of cyber preparedness associated with an organization and/or its components.

Background

Much has been written and discussed during the last several years about advanced cyber threats and their impact, both potential and actual, on the nation's information infrastructure. Cyber threats vary in sophistication and intent and the consequences to the targeted system/network can vary widely as well. The one consistent theme is that the cyber defenses commonly used today are simply not effective against most forms of advanced cyber attack. The question is: Can we characterize such advanced threats and devise ways to overcome or minimize them?

This paper describes a framework for thinking about cyber threats and determining the appropriate level of preparedness for a particular organization or mission. It recommends representative defensive tools and techniques that form a good starting point for improving security against modern cyber threats and strategies for operating through attacks.

To be useful at the organizational level, a cyber preparedness framework should provide some insight into the organization's current posture with respect to threats as well as ideas about the defenses that can be used to counter such threats. In addition, a framework should aid in identifying the organizational cyber threat environment as well as a strategy for improving the enterprise's approach to addressing cyber threats. A framework needs to be useful for multiple types of enterprises and environments because most organizations' missions and adversaries will have at least some unique aspects.

The growing number and variety of cyber threats can be categorized in many different ways. MITRE defined the five Cyber Prep levels to correspond to fairly distinct break points in adversary capabilities, intent, and technical sophistication, as well as in the operational complexity involved in an attack. Each Cyber Prep level builds on the defenses and activities an organization has taken to prepare itself against lower-level adversaries.[1] For example, an organization that encounters Level 3 threats would also need to prepare for Level 1 and Level 2 threats, since a Level 3 adversary will use lower-level attack techniques if those techniques achieve the adversary's desired results.

One of the most difficult questions to answer relating to security is about the benefits from investing in specific security safeguards. If an organization implements these safeguards, how much better protected will it be? Solid quantitative answers are difficult to come by, particularly for a single defensive technique. The best approach is to look at the ensemble of defensive techniques that have been implemented and see the difference they make together. For example, to assess its preparedness for attacks at its perimeter, an organization can measure intrusions that successfully penetrate the firewall, where detectable, threats detected within the firewall, and threats eliminated within the firewall. An organization's or a mission's preparedness can also be actively tested and measured through the use of red teams. Red teams can be highly effective at providing concrete information regarding the effectiveness of an organization's security safeguards.

Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness. A major financial institution may be targeted by organized crime with the goal of transferring money. A defense think tank may be targeted by nation states with the goal of covertly acquiring sensitive information. A defense-parts supplier may be targeted by an adversary whose goal is to corrupt the produced parts. Each of these organizations will in turn require a different level of preparedness and different defenses tailored to the nature of the attacks they face.

Cyber Prep Framework Approach

The Cyber Prep levels are characterized by three factors:

- The nature or *caliber and intent of the threat* with which an organization is prepared to address.
- The *technical and operational capabilities* the organization uses to assure its missions and provide security to counter the threat it faces. Types of controls or capabilities can be defined, and for each type of control or capability, multiple levels can be defined.
- The *process capabilities* – i.e., the risk assessment and governance policies and processes – the organization uses to determine its cyber threat level and (as appropriate) to characterize the specific threats it faces; to determine and deploy technical and

[1] Cyber Prep levels are intended to be strategic in nature and may take multiple years to achieve. Thus, Cyber Prep, complements, but does not replace, more tactical cyber threat levels or security measures that may change corresponding to the daily security assessments of cyber threats.

operational capabilities in a manner calibrated to counter its threats; and to manage, assess, and adapt those capabilities to address the changing threat environment.

This paper focuses on the first two areas.

The characterization of adversaries and their motivations in Tables 1, 2, and 3 are for descriptive purposes to demonstrate the evolution of cyber threats and associated preparedness approach. Based on the way attackers generally tend to operate, a more competent and determined group may first use techniques that are also available to less capable, less motivated attackers. If those attacks were blocked then the adversary would escalate to a higher-level attack. Insight into this escalation can be helpful for future planning of safeguards and can also help increase the cost of attack for different adversaries.

Ideally an organization facing cyber threats at a certain level should look to have a commensurate level of preparedness — organizations facing a Level 4 threat should generally employ a Level 4 degree of cyber preparedness. The five levels of cyber threat and preparedness are labeled consistent with the nature and severity of the adversary and attacks, as well as with the strategy for preparedness to counter such threats. However, each successive level of preparedness adds more expense, more complexity and generally more overhead to an organization's information systems and management processes. The level of resources required by an organization to reach a higher level will be quite significant. Achieving a higher level of preparedness requires addressing architectural, cultural, process, management and technical areas. Therefore, an organization's determination of its target level of cyber preparedness must be made carefully in conjunction with proper planning and funding.

Table 1: Cyber Threat and Preparedness Levels

Level	Cyber Threat Level	Cyber Preparedness Level
1	Cyber Vandalism	Perimeter Defense
2	Cyber Theft/Crime	Critical Information Protection
3	Cyber Incursion/Surveillance	Responsive Awareness
4	Cyber Sabotage/Espionage	Architectural Resilience
5	Cyber Conflict/Warfare	Pervasive Agility

A description of each level and its associated characteristics (adversaries, techniques, defensive schemes, etc.) is provided in the following tables. Without senior leadership understanding the range of issues and a serious commitment to improvement, an organization's progress from one level to the next will be erratic and incomplete. Representative existing and future capabilities to address these threats are also described; they are listed as existing, emerging or future due to their availability and production maturity.

Table 2: Characteristics Associated with Cyber Preparedness Levels

Preparedness Level	Organizational Perspective	Organizational Objective	Organizational Strategy
Level 1 *Foundational Defense*	Believes the cyber threat is largely external and can keep adversaries from penetrating perimeter defenses; the situation is largely manageable via due diligence.	Prepares for known external attacks and minor internal incidents.	Establishes and defends the information system perimeter. Protects against introduction of known malicious code/malware and discourages unauthorized internal access. Uses commercial security products, and professionally manages perimeter and desktops
Level 2 *Critical Information Protection*	Recognizes the importance of identifying and safeguarding critical information, whether internal, external or transiting the organization's perimeter.	Prevents unauthorized access to critical or sensitive information.	Identifies and protects critical data regardless of location, using encryption, enhanced identification & authentication and access control methods.
Level 3 *Responsive Awareness*	Understands that adversaries are penetrating the organization's information infrastructure; can no longer assume that perimeter based protection will keep internal systems secure. Recognizes the need for a high degree of awareness to identify and respond to attempted incursions.	Deters adversaries from gaining a foothold in the organization's information infrastructure.	Deploys capabilities to detect and respond to targeted penetration attempts within the organization's information infrastructure. Complement with procedures to better understand methods of adversary.
Level 4 *Architectural Resilience*	Recognizes that it is not possible to keep the persistent adversary from, over time, establishing footholds within the organization's information infrastructure, including some which will remain undetected. Understands the importance of maintaining an operational capability in the face of adversaries who can launch successful cyber attacks from their persistent footholds.	Constrains exfiltrations of critical data, continues critical operations, minimizes damage despite successful attacks from adversaries who have established a foothold.	Designs and operates systems with the concepts of resilience and protection through multiple distinct enclaves, so that the organization can limit exfiltration of critical information , contain adversaries, and operate through (even in degraded mode), and recover from a successful attack.
Level 5 *Pervasive Agility*	Assumes that the adversary is taking continuous, overt actions against the organization from its persistent foothold within the information infrastructure , including a compromised supply chain, that will result in loss of some key systems and services; assume data has been purposely been modified to mislead and confuse. Recognizes need for agility and flexibility to ensure mission operations.	Maintains operations on a continuing basis and adapts to current and future coordinated, successful attacks, regardless of their origins.	Employs a highly agile, adaptive, and flexible structure that permeates all aspects of the organization (including planning, supply chains, collaboration, architecture, governance, and resources), allowing the organization to continually and dynamically reshape all aspects of its operations in face of changing, successful attacks.

Table 3: Characteristics Associated with Cyber Threats

Level	Typical Actors	Typical Intent of Threat Actor
1	Hackers, Taggers, and –Script Kiddies;" small disaffected groups of the above.	Disruption and/or embarrassment of the victimized organization or type of organization (e.g., a specific Department or Federal government as a whole).
2	Individuals or small, loosely affiliated groups; political or ideological activists; terrorists; domestic insiders; industrial espionage; spammers.	Obtain critical information and/or usurp or disrupt the organization's business or mission functions for profit or ideological cause.
3	Nation-state government entity; patriotic hacker group; sophisticated terrorist group; professional organized criminal enterprise (e.g., RBN).	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.
4	Professional intelligence organization or military service operative.	Obtain specific, high value information, undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the future.
5	Nation-state military possibly supported by their intelligence service; very sophisticated and capable insurgent or terrorist group.	Severely undermine or destroy an organization's use of its mission, information and/or infrastructure.

In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered. Table 4 provides some representative examples of how the combination of threat factors come together to form actionable threats per level. Table 5 offers more concrete examples of the tactics, techniques, and procedures (TTPs) employed by adversaries at each level.

Table 6 provides a small sample of the types of safeguards and strategies that could address advanced cyber threats. Table 6 has three columns, Existing Solutions, Emerging Solutions, and Future Solutions. These three columns reflect the fact that as the sophistication of the adversary increases, so will the maturity of the proposed safeguards or strategies. At the higher threat levels, a greater percentage of the safeguards fall into the Emerging and Future Solutions area.

The entries in both Table 5 and Table 6 are representative; a complete set of TTPS or safeguards would be much more numerous, and could be classified. Because the specific TTPs of adversaries evolve rapidly, the assignment of a specific TTP or safeguard to a particular level is intended to serve only as a snapshot in time. As the threat level increases, the limitations of today's widely available solutions become more apparent. We need only look at some of the TTPs exercised by the more advanced threats today to understand what may very well be readily available to less sophisticated adversaries in the not too distant future. Investment in future architectural, operational, and technical solutions is essential for ending the cycle of reaction and delayed response. In the meantime, organizations need to be creative with the application of emerging solutions to address today's threats.

Table 4: Cyber Threat Capability Examples

Level	Threat Scenarios
1	The adversary uses simple attack tools (e.g., freeware vulnerability scanners) to launch well known attack methods (e.g., brute force password guessing) from outside the organization's cyber perimeter. The attack may cause minor disruption (e.g., cyber vandalism). Attacks may not be targeted at specific organizations but rather at any organization that the attacker can penetrate; alternatively, personally motivated attacks may be focused on a specific organization (e.g., a retailer that has alienated the attacker).
2	The adversary has access to and experience with tailorable attack tools (e.g., to custom-craft malware). The adversary is positioned opportunistically to target critical information external to or transiting the organization's cyber perimeter. The adversary attempts to steal or acquire information (e..g., SSNs) or resources (often for financial enrichment). Sample attack methods include stealing laptops left in vehicles in the organization's parking lot, intercepting email transiting the perimeter, and spam phishing emails.
3	The adversary is in position for limited infiltration across the organization's cyber perimeter resulting in a tentative foothold within the organization. Sample attack methods include some combination of internally (from foothold) and externally based cyber attacks, both employing non-targeted zero-day attacks. The adversary attempts to obtain and exfiltrate large quantities of high-value information from within the organization's infrastructure (e.g., proprietary plans, personal information about celebrities), in a covert manner, possibly supported by more overt mechanisms such as cyber extortion. Attacks are focused on specific high value organizations (e.g., IRS, Federal Reserve) thought to possess sensitive information with national security or financial implications.
4	The adversary has been able to breach the organization's cyber and/or physical perimeters and establish a persistent foothold within the organization. Sample attack methods include some combination of internally and externally based attacks, both employing targeted zero-day attacks, supply chain intercepts, and covert physical access (e.g., using a co-opted or unwitting insider). The adversary attempts to obtain and exfiltrate large quantities of specific, high value or mission-critical information, insert malicious components to support future attacks, feed false information to the organization to undermine its operations or to corrupt its information products. Attacks are focused on specific high value organizations (e.g., IRS, Federal Reserve) or on specific employees of the organization (e.g., by targeting their home computer) thought to possess highly sensitive information with major national security or financial implications. Attacks may also focus on intercepting key supplies to the organization while in transit from the supplier to the organization, and replacing them with corrupted or defective components.
5	The adversary has been able to breach some combination of the organization's cyber, physical, personnel and supply perimeters, and establish persistent footholds within the enterprise. Sample attack methods include some combination of internally and externally based advanced cyber attacks (e.g., tailored zero-day attacks), corruption of the organization's supply chain, covert physical access (e.g., using an implanted insider), and physical attacks. The adversary attempts to prevent or disrupt high value organizations from carrying out key aspects of their mission (e.g., destroy or disrupt components governing portions of the electrical power grid causing wide scale blackouts, disabling IRS's ability to process tax returns) or take control of systems. Attacks are focused on specific organizations or on specific individuals thought to possess highly sensitive information with major national security or economic implications. In addition, the attacks may be more narrowly focused, targeting supporting components (e.g., key suppliers of the critical infrastructure component), or may be more broadly focused targeting a set of related organizations (e.g., multiple critical infrastructure providers).

Table 5: Sample Tactics, Techniques and Procedures (TTPs) Adversaries Might Use

Cyber Prep Level	Sample TTPs
1	• Discovering and accessing sensitive data/information stored on publicly accessible information systems; • Inserting known malware into organizational information systems (ISs), e.g., virus via email; • Performing brute force login attempts; • Defacing files on publicly accessible information systems; • Performing network reconnaissance; • Social engineering by outsiders to convince insiders to take harmful actions.
2	• Compromising critical organizational ISs via physical access by insiders; • Conducting phishing attacks; • Employing open source discovery of organizational information useful for later cyber attacks; • Hijacking information system sessions of data traffic between the organization and authorized external entities; • Opportunistically stealing or scavenging computer or data storage assets; • Sniffing external information systems and networks (e.g., hotel kiosk) to obtain organizational information; • Take advantage of split tunneling by authorized users to gain access to organization's ISs
3	• Compromising, and reintroducing to the internal environment, organizational ISs used externally; • Inserting malicious code into organizational information systems to facilitate exfiltration of data/information; • Installing general-purpose sniffers on organization-controlled (internal) networks; • Mapping and scanning organization-controlled (internal) networks from within (inside) the organization; • Performing reconnaissance and surveillance of information systems, facilities, and operations; • Successful compromise of widely used software; • Tailgating authorized employees to gain access to organizational facilities; • Use of non-targeted zero-day attacks.
4	• Inserting counterfeited hardware into supply chain; • Insider-based session hijacking; • Installing persistent and targeted sniffers on organizational information systems and networks; • Implanting subverted individuals into the organization; • Social engineering by (malicious) insiders to convince other (trusted) insiders to take harmful actions; • Targeting and compromising home computers of critical employees; • Targeting zero-day attacks on organizational information systems; • Using malware targeted at organizational ISs known to be used by the organization; • Using postal service or other delivery services to covertly insert wireless sniffers inside facilities.
5	• Causing destruction of critical information system components and functions; • Compromising design, manufacture, and/or distribution of IS components the organization is known to use; • Coordinating attacks on the organization using external , internal , and supply chain attack vectors; • Creating false-front organizations to inject malicious IS components into organization's supply chain; • Injecting false but believable data into organizational ISs; • Inserting specialized, non-detectable, malware into organizational ISs based on system configurations; • Jamming wireless communications; • Implanting subverted individuals into privileged positions within the organization.

Table 6: Sample Safeguards per Cyber Prep Level

Level	Existing Solutions[2]	Emerging Solutions[3]	Future Solutions[4]
1	• Perimeter firewalls and intrusion detection. • Strong identification and authentication (I&A) for remote privileged access. • Anti-virus and anti-spyware on email servers and client systems. • Audit-log monitoring of external-facing and perimeter systems (non-real-time).	Not required	Not required or none identified
2	• Strong I&A for all remote access. • Encrypted external transmissions (e.g., SSL, VPNs) between internal systems and trusted external systems. • Segregated Demilitarized Zone (DMZ) at the edge of the enterprise network. • Scanning of portable systems (laptops, thumb drives, etc.) prior to re-connection to internal network. • Strong physical security for critical systems to deter malicious insiders. • Periodic open source searches and defensive adjustments for information.	• Use virtualization on desktops to better segregate production environment from risky user behavior • Improve design/architecture for additional security software.	Not required or none identified
3	• Strong I&A for all privileged access (remote and local). • Deploy sensors at critical points to detect exfiltration. • Monitor and analyze network traffic for abnormal conditions and unusual patterns. • Honeypots.	• Deploy insider monitoring. • Rootkit detection. • Correlate/analyze physical and cyber access. • Monitor control channels through perimeter for illicit data transfer. • Honeyclients.	Not required or none identified

[2] Solutions are commercially available and in widespread use.
[3] Solutions require application of existing technology in a new manner or early adoption of emerging technology.
[4] Solutions require further Research & Development.

Table 6: Sample Safeguards per Cyber Prep Level (concluded)

Level	Existing Solutions	Emerging Solutions	Future Solutions
4	• Use strong I&A for all access to critical information systems. • Partition internal information infrastructure into sub-networks, using rapidly reconfigurable boundary control solutions. • Minimize time between placing an order and requested delivery date to stress any supply chain intercept attempt. • Penetration testing of physical security on the organization's facilities.	• Analyze systems to see which critical components should be (re-)implemented to avoid risk of serious COTS failure/ malware. • Use trusted foundries. • Use a heterogeneous code base for key infrastructure components. • Acquire spare parts during initial system procurement. • Use trusted shipping with physical protection and continuous accountability.	• Make frequent small changes to software configurations to thwart offensive TTPs.
5	• Strong I&A for all access. • Use multiple trusted suppliers for key components. • Trusted cutouts to support shipping – acquiring critical components through trusted intermediaries that purchase them on the organization's behalf.	• Integration of cyber and physical penetration testing. • Virtualization to reconstitute services. Periodically conduct reconstitution of critical functions to reduce persistence of ad to gain and maintain a foothold. • Employ out of band control – to maintain or reconstitute operation of critical services.	• Contingency reserve – critical capabilities or operating modes that are maintained offline and used when production capabilities are no longer available or trusted, or simply to confuse the adversary. • Near-real-time forensics and response to cyber attacks; investigate root-cause analysis of attack. • Use trusted components for critical organizational functions.

Summary

The application of the Cyber Prep methodology requires focusing on the anticipated threats and TTPs. Different organizations, even at the same Cyber Prep level, are likely to have differences in their threat environments as well as in their risk management strategies and enterprise architectures, which will determine which TTPs are relevant to them and which safeguards best suit them. As a consequence, it is very likely that different organizations (even at the same Cyber Prep level) will employ different mixtures of safeguards. "Achieving a given Cyber Prep level" is based on the degree to which an organization has taken action to address as many as possible of the TTPs it has identified as relevant. Reaching a particular Cyber Prep level is accomplished by selecting those safeguards which partially or fully counter the identified TTPs[5]. Within the Cyber Prep framework, there is no additional benefit from expanding the potential set of safeguards to the maximum associated with a particular level. Nor is there additional benefit from selecting safeguards that do not address the organization's threat environment. Successful application of Cyber Prep requires prioritization and an explicit understanding of the tradeoffs being made. Ultimately it should be used to improve risk management of cyber assets and the environments in which they reside and the cost effectiveness of safeguard investments.

[5] At MITRE we are applying Cyber Prep in just this manner, first selecting a target Cyber Prep level, then identifying which of the TTPs we need to address, and then deploying appropriate safeguards to counter those TTPs.