RESILIENCY

Cyber Mission Assurance Engineering:
A Risk-Based, Threat-Informed Approach to Address Advanced Adversaries

MITRE

Advanced cyber threats present a challenge to established engineering and strategic analysis processes: Mitigation techniques vary widely in maturity; relevance to organizations, mission, and systems; and affordability, efficiency, and effectiveness. Cyber mission assurance engineering complements and extends established processes, to facilitate cost-effective risk management.

Introduction

Organizations and missions increasingly depend on cyber resources, ranging from general-purpose information and communications technology (ICT) to mission or business function-specific information systems to components of cyber-physical systems. Those resources are subject to persistent, stealthy, and sophisticated attack by advanced threat actors (also known as adversaries or as the advanced persistent threat [APT]). By establishing and maintaining an enduring presence on organizational systems, adversaries are able not only to exfiltrate sensitive information and/or collect intelligence on an ongoing basis, but also to corrupt mission data and to deny or degrade mission capabilities.

Advanced threats create concerns for mission assurance: How, and how well, can mission functions be performed when an adversary can compromise some of the cyber resources on which those functions depend, or create effective countermeasures to cyber defenses based on the unchecked intelligence being collected? Advanced threats also pose a challenge to existing processes: How can organizations acquire, and integrate into existing systems or systems-of-systems, capabilities to address adversaries that change tactics, techniques, and procedures (TTPs)?

This white paper describes MITRE's cyber mission assurance engineering (MAE) approach to these challenges. Cyber MAE consists of processes, consistent with a conceptual and analytic framework, realized via capabilities that include tools, knowledge bases, procedures, and worked examples. Cyber MAE is risk-based, focused on risks to missions due to dependence on cyber resources, and threat-informed, making use of threat information sharing and threat analysis.

Cyber MAE enables organizations, missions, and programs to identify and manage cyber risks, and to integrate cyber risk management into existing risk management processes. These processes include strategic planning, mission or business continuity planning, and – for systems or programs – processes for determining, implementing, evaluating, and monitoring the effectiveness of conventional security controls and capabilities[1], and for identifying how those controls can be augmented and/or complemented to address advanced threats. The goal of Cyber MAE is to enable missions and organizations that depend on cyberspace to achieve their objectives despite threats that exploit that dependence, particularly advanced threat actors.

1 As discussed below, these processes can be described using the Risk Management Framework (RMF) presented in NIST SP 800-37, *Guide to Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* NIST SP 800-53R4, *Security and Privacy Controls for Federal Information Systems and Organizations,* defines security controls, classes of security controls, and capabilities (i.e., combinations of as-implemented security controls or functionality).

Challenges to Existing Processes

Compliance is necessary but not sufficient. Compliance-oriented processes for systems security engineering, risk management, and strategic analysis focus on applying established security practices[2] effectively, in accordance with generally accepted standards of good practice. Security practices have been established for general-purpose ICT and adapted or extended to mission-specific information systems and, to a lesser extent, to cyber-physical systems. Standards of good practice arise from extensive experience with conventional threats (e.g., natural disaster, human error, insider threats, and unsophisticated external attackers such as hackers or cyber vandals), and with how to use security practices effectively to address such threats. However, established security practices are not sufficient against advanced and quickly evolving threats, nor are they characterized in terms of their risk-mitigating contribution to mission assurance. Existing information security risk management processes need to be extended or complemented to consider not only conventional threats, but also advanced threats which can exploit vulnerabilities in one system as part of a larger campaign involving other systems, can target missions rather than assets local to a system, can adapt their TTPs to defender actions, and/or have established a covert presence in systems for future exploitation.

No one can do it all. New technologies, and novel uses of existing technologies, process and techniques, can improve mission assurance in the face of adversaries that cannot reliably be kept out of organizational systems. However, cyber risks (i.e., organizational and mission risks related to dependence on cyber resources) must be managed in a real-world context. Not every conceivable practice or new technology is applicable or can be applied to mitigate cyber risks; other organizational and mission risks must also be managed, and trade-offs must be made. Engineering and strategic analysis processes need to account for resource limitations and for different organizational strategies for technology adoption.

Risk is multidimensional. One of the challenges in systems security engineering is that risks must be managed and security needs to be addressed at multiple levels of abstraction or tiers. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, defines a general risk management process that organizations can apply consistently across three tiers: (i) the organizational tier, focused on risks to the organization, individuals, other organizations, and the Nation; (ii) the mission / business process tier, focused on risks to specific missions or business functions; and (iii) the information system or program tier, where information security risks are a component of programmatic risk and contribute to risks at the higher tiers. At each tier, the set of stakeholders – e.g., mission owners, program managers, individuals or groups affected by information or mission risks – adds another dimension, as different stakeholders have different equities, experience different risks, and assign different costs or impacts to possible risk mitigations.

2 The phrase "security practices" refers to processes, procedures, techniques, and methodologies for constructing and using security capabilities.

The Cyber Attack Lifecycle Framework

As illustrated in Figure 1, the cyber attack lifecycle[3] – the stages that an adversary goes through to achieve the objectives of establishing, using, and maintaining (or removing) a presence in an enterprise's information infrastructure – provides a framework for recognizing how attacks are structured. This framework supports analysis of how risk mitigation measures affect the adversary, and can be applied more effectively. Cyber MAE uses the cyber attack lifecycle as a framework for identifying adversary TTPs, and for characterizing how – and how well – different mitigations address adversary actions at different stages in the attack lifecycle.

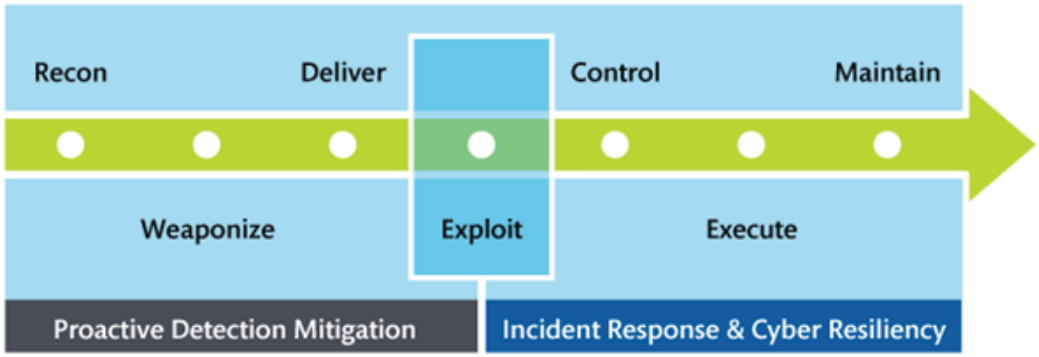

Figure 1. The Cyber Attack Lifecycle

General Methodology

Cyber MAE provides a risk-based methodology for identifying and evaluating alternatives for reducing cyber risks, with respect to the effectiveness, efficiency, and affordability of those alternatives. Alternatives can be evaluated at the enterprise, mission, and system tiers, and for programs which may acquire multiple related systems, services, or infrastructures. As illustrated in Figure 2, the Cyber MAE methodology consists of five component processes: (1) establishing mission priorities, (2) identifying mission dependencies on cyber resources, (3) performing a mission (or business) impact analysis, (4) performing a threat susceptibility analysis, and (5) analyzing alternative cyber risk remediation alternatives for effectiveness, efficiency, and affordability.

The first three processes serve to determine which resources are most important, based on their mission criticality and on organizational priorities. The fourth process identifies threats, taking into consideration adversary charac-

3 The cyber attack lifecycle is frequently referred to as the "cyber kill chain." See http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Numerous variants of the cyber kill chain or cyber attack lifecycle have been defined. The version shown in Figure 1 is consistent with the organization of adversarial TTPs in NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments.*

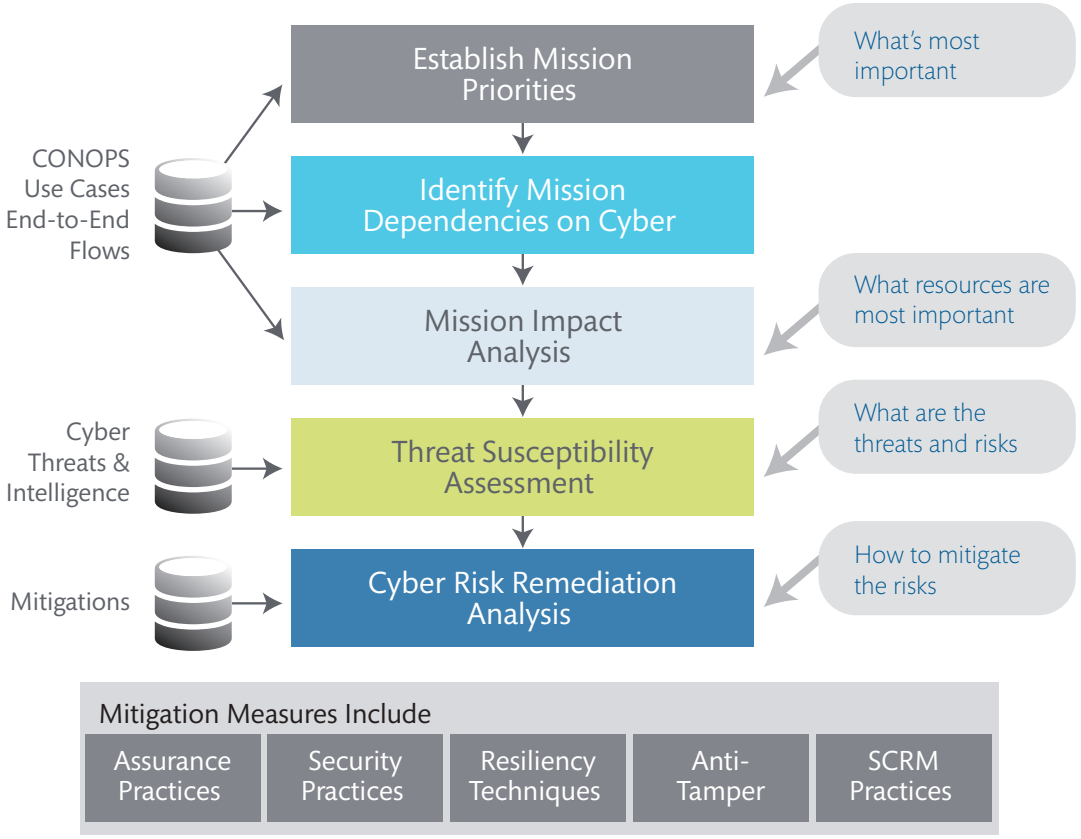

Figure 2. Cyber MAE Methodology

teristics such as capabilities, intent, and targeting as contributors to the likelihood that an adversary will use a given TTP or set of TTPs, together with information about vulnerabilities or weaknesses in as-built systems or components, in the operational environment, or inherent in information or communications technologies, in order to determine risks. The threat susceptibility assessment is informed by threat analysis and information sharing.[4]

Mitigations can be drawn from multiple disciplines, including assurance, security, resiliency[5], anti-tamper (AT), and supply chain risk management (SCRM). Practices and techniques in these areas counter or otherwise address the threats to the target system, program, or mission. Mitigations can vary in effectiveness, maturity, and cost. Thus, the risk remediation analysis takes these into consideration, as well as constraints imposed by organizational culture, policy, legal and contractual limitations, and commitments to technologies or standards. Cyber MAE supports the

4 See A New Cyber Defense Playbook, http://www.mitre.org/work/cybersecurity/pdf/cyber_defense_playbook.pdf.

5 For more on cyber resiliency techniques and their assessment, see D. Bodeau and R. Graubart, *Cyber Resiliency Engineering Framework*, MTR 110237, http://www.mitre.org/work/tech_papers/2012/11_4436/11_4436.pdf and *Cyber Resiliency Assessment: Enabling Architectural Improvement*, MTR 120407, http://www.mitre.org/work/tech_papers/2013/12_3795/12_3795.pdf.

overarching goal of providing the right level of mitigations for the organizational or operational environment, providing recommendations that can be used by strategic planners, architects, and systems security engineers.

These component processes can all be exercised as part of mission assurance engineering. Alternately, the results of some processes can be assumed (e.g., all cyber resources can – unrealistically – be assumed to be equally important to mission objectives). Component processes can be also be exercised in different ways, and can leverage (or even be subsumed by) existing processes. For example, a Business Impact Analysis (BIA) performed as part of contingency or continuity of operations (COOP) planning can be expected to identify and determine the criticality of cyber resources. The last two processes are often performed together, and can make use of the cyber attack lifecycle framework.

The methodology can be applied with different scopes (e.g., system, mission or business segment, system-of-systems, enterprise), and with varying levels of detail and effort. The methodology can use existing information (e.g., cyber threat knowledge bases, the results of a BIA) or entail collecting or developing specific information. For systems and acquisition programs, the methodology can be applied (with different data sources and degrees of detail) throughout the life-cycle. MITRE has applied the methodology to multiple systems and programs, with varying levels of effort, degrees of detail, and knowledge bases, and at various points in the integrated life cycle (ILC).

Relationship to Other Processes

As a risk-based engineering methodology, Cyber MAE complements and can be integrated with existing processes. These include processes following a system development life-cycle (SCLC) or integrated life-cycle (ILC) framework as well as those that are part of the Risk Management Framework (RMF)[6]. Figure 3 illustrates how activities from Cyber MAE fit into the DoD ILC[7]; the mapping to other life-cycle models is similar. In Figure 3 (and later, in Figure 4), cyber resiliency techniques are highlighted as a class of mitigation measures.

In the DoD ILC, mission priorities are established at the strategic level. Based on the initial system concept, mission dependencies on cyber resources and an initial mission impact analysis or Crown Jewels Analysis result in identification of critical resources. This identification serves as input to the threat susceptibility analysis, which also takes into consideration the system's environment of operations. The risk remediation analysis considers the affordability as well as the effectiveness of possible mitigation alternatives. As noted above, mitigations can be drawn from multiple

6 The RMF, as defined in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions with Tiers 1 and 2.

7 See DoD Instruction 5000.2, *Operation of the Defense Acquisition System*. In the figure, O&S refers to Operations and Sustainment. Alternatively, NIST SP 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle*, presents a five-phase conceptual view: initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal. T he GSA system development life cycle consists of nine phases: System Concept Development, Planning, Requirements Analysis, Design, Development, Integration and Testing, Implementation, Operations and Maintenance (O&M), and Disposal.

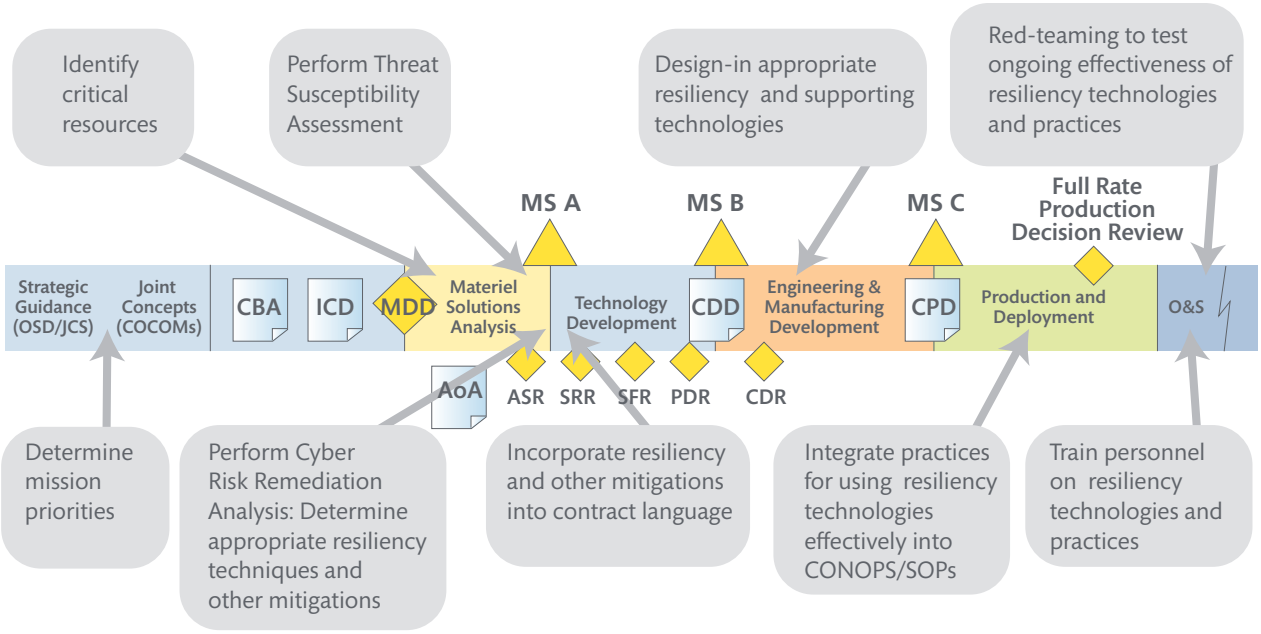

Figure 3. Cyber Mission Assurance Engineering in the ILC

areas, including security, assurance, AT, SCRM, and cyber resiliency. Some existing performance, reliability, and security mechanisms support (or can be modified to support) cyber resiliency. However, other cyber resiliency technologies are transitional or novel, which can entail programmatic risk. The risk remediation analysis includes consideration of risk-risk trade-offs.

While one aspect of the Cyber MAE methodology supports the initial determination of mitigation requirements, mission assurance engineering continues throughout the life-cycle. Selected mitigations are designed for seamless integration into the system architecture, and they are implemented and integrated with conventional security controls, as well as with performance, reliability, and management mechanisms. The concept of operations for the system and the mission capabilities it provides, and standard operating procedures for users, administrators, and cyber defenders must include processes and procedures for making effective use of resiliency technologies and other mitigations, and training is vital to both effectiveness and efficiency. Depending on mission criticality, Initial Operational Test and Evaluation (IOT&E), exercise of contingency plans, or other activities can include Red Teaming to test the effectiveness of the technologies and practices intended to address advanced threats.

Figure 4 illustrates how mission assurance engineering activities fit in with the steps in the Risk Management Framework. This overlay, like the mapping to the ILC above, illustrates how activities correspond to the steps in the RMF starting with the inception of a new system or program, and is simplified to show a linear process flow. However, Cyber MAE (like the RMF) can be applied to an existing system or program, and to programs using agile development. In such cases, the determination of appropriate cyber risk mitigations and security controls takes into consideration existing implementations and dependencies.

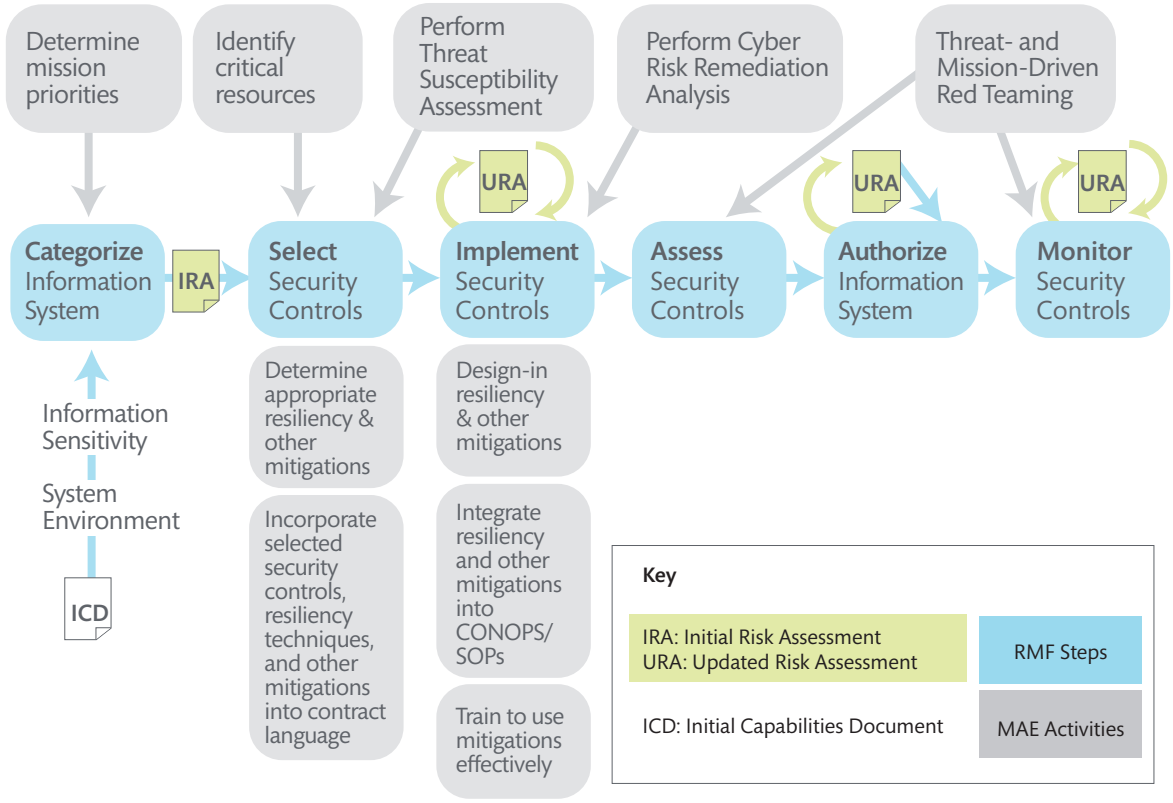

Figure 4. Cyber Mission Assurance Engineering and the Risk Management Framework (RMF)

Cyber MAE Capabilities

MITRE has developed specific capabilities (e.g., tools, knowledge bases, procedures) to realize the general Cyber MAE methodology in practice. As illustrated in Figure 5, these include Map-the-Mission (for identifying mission dependencies on cyber resources, particularly in operational environments) and Crown Jewels Analysis (for establishing mission priorities, identifying mission dependencies on cyber resources, and performing a mission impact analysis), each of which identifies high-value (e.g., mission-critical, mission-essential) cyber resources and each of which is tool-supported. Capabilities for identifying and evaluating cyber risk remediation alternatives include the Threat Assessment and Remediation Analysis (TARA) process, structured using the cyber attack lifecycle framework and/or supported by catalogs of threats and remediation alternatives and a tool that uses those catalogs; the Cyber Prep methodology; and the cyber resiliency metrics and assessment methods that are part of cyber resiliency engineering.

As illustrated in Figure 6 below, the emphasis varies, depending on the tier in the Risk Management Hierarchy at which it is applied. To reflect this difference in emphasis, several variants have been identified:

MAE for cyber-aware enterprise transformations, which focuses on transforming governance and identifying enterprise-wide risk remediation practices so that the enterprise can standardize approaches to addressing threats to mission and organizational dependence on cyberspace. At the organizational tier, MAE enables cyber risks to be

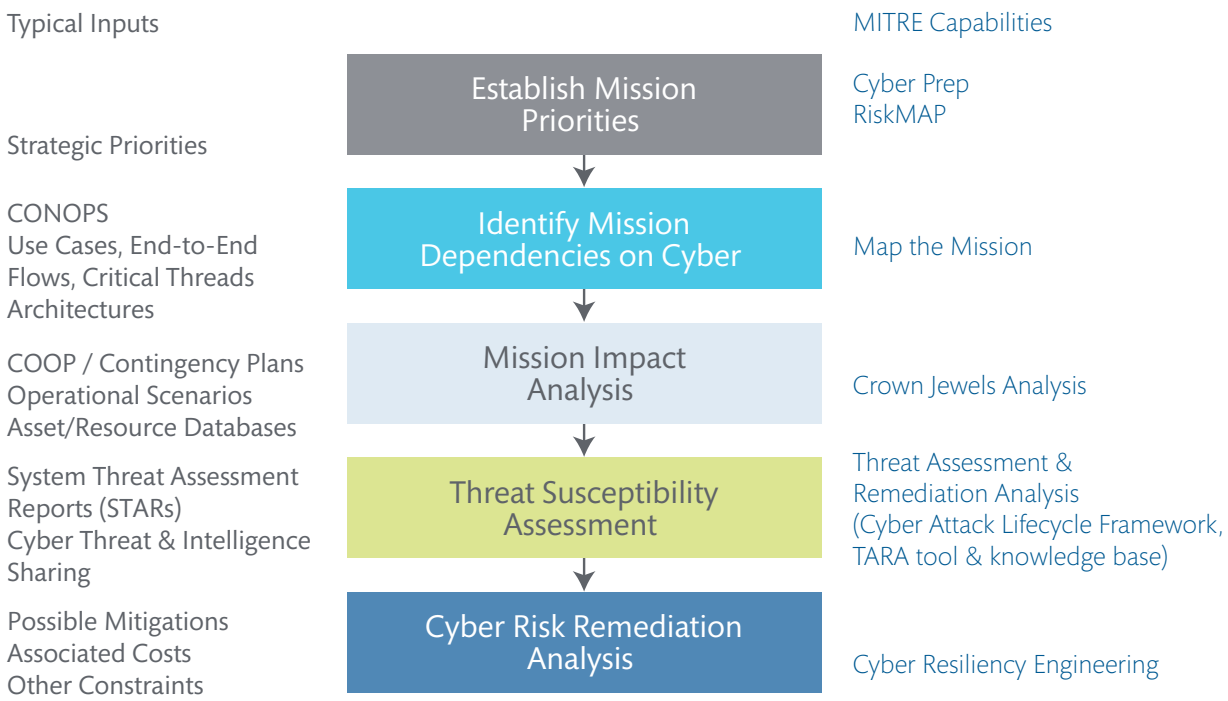

Figure 5. Cyber Mission Assurance Engineering Capabilities

considered as part of strategic analysis and planning. While MITRE's Cyber Prep methodology focuses on strategic planning for cyber-aware enterprise transformations, it has been applied at the system tier as well as at the organizational and mission tiers.

Cyber resiliency engineering, which focuses on an evolving set of resilience techniques (e.g., deception, unpredictability, dynamic positioning, diversity) to improve mission resilience in the face of advanced threats. These techniques can be applied (in different ways) at all tiers of the Risk Management Hierarchy, and are also relevant to systems-of-systems that span organizations to support trans-organizational missions. MITRE is performing investigatory implementation and integration of cyber resiliency technologies, applying cyber resiliency engineering to sponsor programs, and integrating resiliency into a cybersecurity roadmap.

System / acquisition mission assurance engineering, which focuses on Threat Assessment and Remediation Analysis. MITRE has successfully applied its TARA methodology[8] to multiple sponsor programs, making specific recommendations for phased integration of security measures and for architectural changes.

Cyber mission assurance engineering complements compliance- or best-practices-oriented engineering and strategic analysis processes with a focus on mission needs and on advanced threats that exploit mission dependence on

8 See *Cyber Risk Remediation,* MITRE Systems Engineering Guide, http://www.mitre.org/work/systems_engineering/guide/enterprise_engineering/se_for_mission_assurance/cyberrisk_remediation.html.

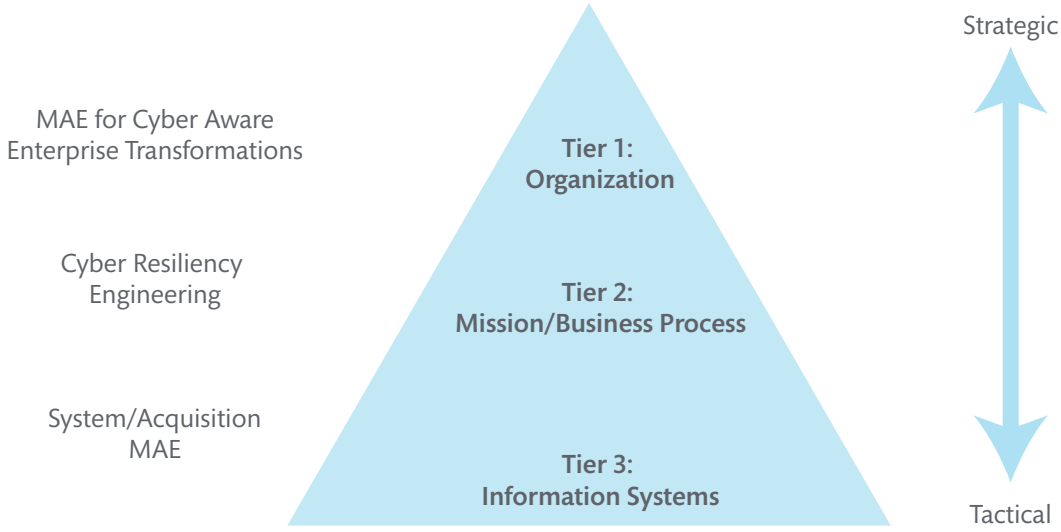

Figure 6. Cyber MAE in the Risk Management Hierarchy

cyberspace. Over time, organizations will transition to the multi-tiered approach to risk management, making the need for engineering analysis at the organizational and mission/business tiers more evident. MITRE will continue to apply the Cyber MAE methodology – and the tools and knowledge bases that support it – to support analyses of alternatives and selection of risk mitigations that are affordable, effective, and efficient.

Getting Started

Organizational senior executives, mission owners, program managers, and systems engineers can make use of Cyber MAE capabilities in multiple ways, depending on the decisions they need to make or the concerns they need to address. For a mission or business process, a cyber resiliency assessment or an effort to identify mission dependencies on cyber resources could inform and improve existing continuity of operations planning (COOP) with an understanding of the APT. For a system-of-systems or a common infrastructure such as a network, a threat assessment and remediation analysis using the cyber attack lifecycle framework identify existing mitigations, potential mitigations that could be integrated in the near term, and possible long-term architectural evolution toward greater mission assurance. For a planned system undergoing requirements analysis, application of the TARA methodology can help prioritize requirements based on expected cybersecurity benefits. In any situation, a quick and high-level application of Cyber MAE can help focus attention on areas that merit further attention, to ensure that missions and organizations are aware of – and can cost-effectively mitigate – the risks of depending on cyber resources.

MITRE