Booz Allen®

NATIONAL CYBER

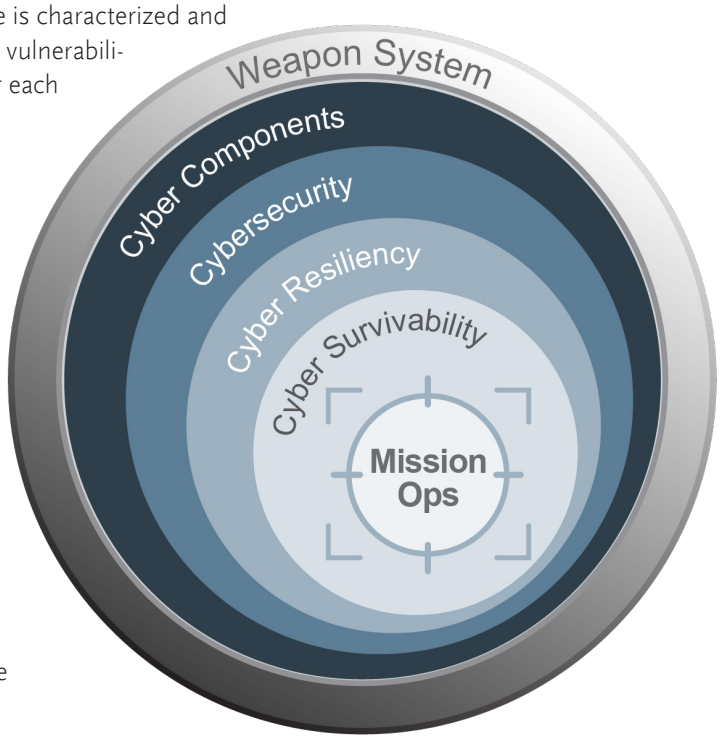
MISSION-BASED CYBER RISK ASSESSMENT

A mission-based cyber risk assessment (MBCRA) focuses on the assessment of a subset of mission-relevant components in order to heighten awareness of system-specific attacks from near-peer adversaries and to recommend mitigations to those mission-relevant threats.

Booz Allen's National Cyber Platform understands the challenges to cyber survivability that exist for weapon systems operating across the land, air, sea, space, and cyber domains. The Cyber-Physical Defense team at Booz Allen takes pride in helping to secure our nation's most advanced platforms with more than 200 credentialed operational technology (OT) cybersecurity professionals and experience across all 16 critical infrastructure sectors.

KEYS TO WEAPON SYSTEMS SURVIVABILITY

- **An MBCRA is the key to assessing cyber threats and impact to mission.**
  An MBCRA is an integrated and iterative methodology to identify potential cyber risks. Through the execution of a detailed functional thread analysis (FTA), the system's attack surface is characterized and mapped to missions, system functions, and potential cyber vulnerabilities. Cyber risk ratings and priority levels are determined for each point of entry into the system's cyber boundary.



- **Conducting MBCRAs is essential across the system lifecycle.**
  MBCRAs focus on highlighting potential mission impacts of vulnerability exploitation and help to inform program owners with generating cyber requirements. MBCRAs provide developers insight into the selection of security controls, relevant testing activities, programmatic decision making, and resource identification to reduce cyber risk and increase the system's overall cyber survivability. Further, an MBCRA enables operators to evaluate the impact of an always-changing cyber threat environment.

  MBCRAs allow the PM to apply assessment/mitigation resources to the right parts of the system by filtering mission-critical components and focusing on those with the highest threats based on cyber threat intelligence.

Department of Defense (DOD) Instruction 5000.89 requires all program managers (PMs) to conduct MBCRAs "to identify those elements and interfaces of the system that, based on criticality and vulnerability analysis, need specific attention in Test & Evaluation events."

MBCRA APPROACH AND IMPLEMENTATION

- **Tools and processes are vital to efficiently conduct complex and challenging MBCRAs.**
  MBCRAs require comprehensive understanding of the system from technical and mission perspectives. It takes a long time to collect and assemble the knowledge necessary for skilled weapon system cyber assessors to perform the assessment. This is valuable time that they could use to discover and mitigate vulnerabilities. As analysts conduct the MBCRA, another time-intensive aspect is mapping the mission onto the system to allow weapon system cyber professionals to focus on the parts of the system that matter most to mission impact.

  Booz Allen's solutions speed up the process of data collection/management and conducting MBCRAs.
  - **Booz Allen's playbook to create a technical system baseline (TSB) does not require skilled subject matter experts (SMEs), freeing up the weapon system cyber SMEs to perform analysis.**
  - **Booz Allen's Modeling Cyber Analysis Tool (ModCAT) uses the TSB to identify mission-critical components and to visualize the vulnerabilities and threats to the system.**

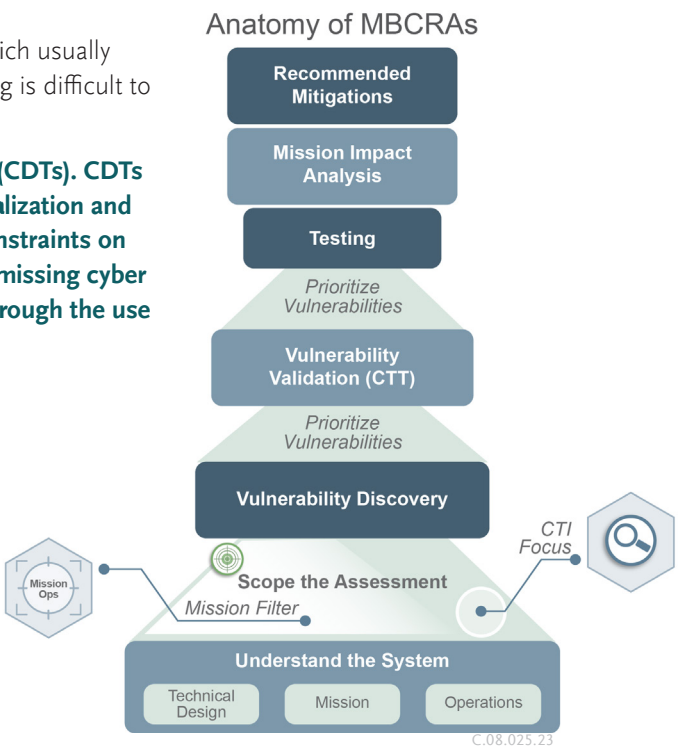
  The addition of the TSB and ModCAT significantly reduces the load of cyber assessors by migrating the data compilation and analysis to data scientists better skilled at data impact.

- **Technology reduces MBCRA assessment timelines.**
  It takes a long time to gather, digest, and understand systems documentation, and an even longer time to identify and prioritize all of the access vectors, possible mission impacts, vulnerabilities, and attack paths for a system.

  Booz Allen uses artificial intelligence (AI) and machine learning (ML) to analyze the system and present weapon system cyber assessors with probable answers, speeding up the process and providing a more complete analysis.

- **Digital engineering tools can validate MBCRA findings.**
  Testing must be performed on operationally relevant software, which usually requires trying to schedule time in a development lab where testing is difficult to schedule and is limited to non-destructive testing.

  Booz Allen addresses this problem by using Cyber Digital Twins (CDTs). CDTs allow us to use system simulation combined with software virtualization and hardware emulation to identify and test cyber effects without constraints on schedule and destructive testing. Booz Allen reduces the risk of missing cyber vulnerabilities while greatly increasing weapon system testing through the use of CDTs.



BOOZ ALLEN MBCRA SERVICES:

- Sponsored/Directed Research
- Full MBCRAs
- System understanding using Booz Allen AI/ML & TSB
- Mission decomposition using Booz Allen AI/ML & ModCAT
- Cyber table top (CTT) using KBSI's Assurant™
- Lead CTT
- Full opposing force team
- Opposing force lead
- Cyber effect development and testing using Booz Allen CDTs

CONTACT INFORMATION

DAVID FORBES
Principal
forbes_david@bah.com

ROBERT MILLER
Chief Engineer
miller_robert@bah.com

ABOUT BOOZ ALLEN

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining more than 100 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: **Empower People to Change the World®**.