Booz | Allen | Hamilton

IMPROVING CYBER READINESS BY MANAGING RISK AND BUILDING RESILIENCE

Rafiq Jamaldinian
Principal
jamaldinian_rafiq@bah.com

Jonathan Chiu
Principal
chiu_jonathan@bah.com

IMPROVING CYBER READINESS BY MANAGING RISK AND BUILDING RESILIENCE

READINESS ASSESSMENTS CANNOT IGNORE CYBER RISK

The United States' ability to take full advantage of information technology across all aspects of warfighting has helped secure its global military dominance. But given the highly-contested nature of cyberspace, this extensive dependency on IT networks and systems also poses critical vulnerabilities to U.S. military readiness and effectiveness that must be addressed. As Defense Secretary Jim Mattis put it in his confirmation hearing: "We find ourselves embracing the dual reality of seeking engagement and cooperation where we can, yet defending our interests where we must. While our military maintains capable land, air, and sea forces, the cyber and space domains now demand an increasing share of our attention and investment."[1]

Traditional approaches to cybersecurity are comprised of compliance regimes around security controls, perimeter protections, and assessing and managing risk — tasks under the purview of CISOs, CIOs, and IGs. But such approaches, while necessary, are not well understood within the context of the mission – particularly in an age where continued innovation is intensifying the military's reliance on IT and cyber threats steadily advance in scale, speed, and sophistication.

Boundaries between the physical and virtual worlds have evaporated — incursions in the virtual realm can yield disastrous physical effects, making traditional military missions every bit as reliant on secure networks as on the platforms and warfighters carrying them out. Recognizing that the platforms and warfighters too are networks and networked, Lt. Gen. Paul Nakasone, commanding general of U.S. Army Cyber Command, recently said: "Network readiness is a component of Army readiness."[2]

Today's defense leaders are under great pressure to monitor, manage, and be accountable for their mission readiness. Readiness is typically measured and assessed across well-established institutional standards, such as personnel, training, equipment, and supply. But commanders increasingly recognize that their operational readiness is significantly impacted by their cyber posture, and are hungry for data and metrics to inform them of how cyber risk-management initiatives are impacting their abilities to carry out missions.

Yet, while there is progress advancing cybersecurity efforts in some quarters, there remains a big challenge for operational commanders across DoD: Gaining command-level visibility into how cyber risks affect mission readiness. The problem they face is that existing methods and tools typically provide only technical, low-level detail on cyber resources and cybersecurity compliance. Organizational leaders need more, and they are increasingly dissatisfied with aggregating tactical-level information as a substitute for strategic understanding and comprehensive situational awareness of their cyber risks to mission.

The next logical focus for Department of Defense planners is cyber readiness: the ability to deliver to organizational leaders, combatant commanders, and mission and business owners the visibility they need to understand and manage their own operational mission readiness from a cyber risk and resilience perspective.

CYBER READINESS BEGINS WITH RISK MANAGEMENT

A key foundation of military readiness today is cyber risk management, a discipline that has been in practice across DoD for many years with mixed results. Today, numerous risk-management initiatives are under way with a collective focus on reducing the network intrusion attack surface. These initiatives are generally compliance-based and intended to: improve organizational cyber

hygiene; strengthen supply chain and network security controls; monitor and mitigate network vulnerabilities; improve compliance with configuration standards; add rigor to system certifications and accreditations; consolidate and modernize IT infrastructures; and improve workforce responses to network risk.

Data from these initiatives are collected in various repositories across the department, including the Enterprise Mission Assurance Support Service (eMASS), the Mission Assurance Decision Support System (MADSS), the Continuous Monitoring and Risk Scoring (CMRS) system, the Assured Compliance Assessment Solution (ACAS), and the Host Based Security System (HBSS). These repositories perform automated collection and analytics of software inventory and asset compliance data and serve as authoritative sources for vulnerability information, informing enterprise-level cyber risk assessments such as the DoD Cyber Scorecard, DISA's Command Cyber Readiness Inspections (CCRIs), and OMB's Federal Information Security Management Act (FISMA) Scorecards.

Understanding cyber readiness requires assessing and managing risks not only to networks and end points, but also to DoD's many missions. But cyber data is typically isolated from the context of the mission, obscuring its real impact on operations.

An important first step toward fixing this problem is the Defense Information Systems Agency's new Command Cyber Operational Readiness Inspection (CCORI) program. The CCORI moves cybersecurity inspections from a compliance-based systems inspection to a risk-based operational commander's mission-focused inspection. CCORIs employ software tools at selected sites to simulate internal and external attacks against a commander's mission critical systems to assess threats and vulnerabilities. The result is a measurement of operational risk to each of the organization's mission-critical tasks and a system to assist commanders in prioritizing cybersecurity resources.

CCORIs are a critical step in the evolution of DoD's cybersecurity approach because they explicitly link cybersecurity assessments to operational mission readiness. But CCORIs present only a snapshot in time. They cannot substitute for a near real-time, enterprise-wide dashboard view of the risk environment – including those operational risks that cross organizational boundaries – that commanders need to properly manage their mission readiness postures.

The lack of an advanced analytical framework limits the ability of existing repositories to measure and assess mission dependency and, therefore, readiness. Enterprise-wide risk-based situational awareness requires an aggregation of data from cyber, mission assurance, and readiness systems across a multi-stakeholder ecosystem for a given mission. By applying new technologies, such as data analytics, and new system architectures that consolidate capabilities, synchronize data models, and facilitate data sharing, DoD planners can fully realize the potential of comprehensive, near real-time, risk-based situational awareness. Powerful analytic tools can convert combined pools of structured, semi-structured, and unstructured data — comprising vulnerability, compliance, threat, and mission data — into actionable intelligence that leaders can use to effectively manage their cyber environments to increase mission success.

THE CRITICAL ROLE OF CYBER RESILIENCE

To achieve a cyber readiness capability, system and network owners, as well as the mission commanders they support, should embrace a complimentary philosophy of resilience—the capacity of systems to withstand disruption and continue operating without impact on output or function. Resiliency lies at the heart of the

Department of Defense's strategic IT goal of "ensuring successful mission execution in the face of a persistent cyber threat."[3]

While risk management looks at how to assess threats, vulnerabilities, and impact to prioritize and mitigate risks to the organization and the mission, resilience looks at mission execution and begins with an acceptance that some disruptions will succeed and some functioning will be lost. Understanding that networks are comprised of many individual nodes that may operate independently and relatively autonomously, resilient design recognizes weaknesses that exist within the network structure and leverages its strengths. The primary strength enabling resilient deign is the interconnectedness of the nodes within a network and their ability to provide needed functionality in the event other nodes are disabled. So, while there may be many paths to vulnerability and many ways to fail, there are also multiple ways for a network to quickly heal itself to achieve functionality.

Building resilience requires balancing two approaches:

- Architecting a system or network to absorb disruption through redundancy, backups and fail-safes.
- Designing rapid responses to return a system or network to operating capacity as quickly as possible.

The optimum mix of these approaches should be managed to achieve a balance between mission criticality and the best price point to achieve security in the cyber systems. Examples of this within DoD are the targeted use of backup systems and contingency planning around computer centers or the use of cloud-based systems.

In addition, building resiliency requires the testing of that resiliency in simulated environments to ensure networks, systems, and operations staff are responding to stress and disruption as expected.

MEASURING THE IMPACT OF CYBER ON READINESS

By managing cyber risk and building cyber resilience, leaders can better understand and actively manage their cyber readiness. In bringing relevant data and visibility to decision-makers at all levels they can become more aware of how cyber risk and resilient design impact their mission readiness through dashboard views of the organization's ability to operate and achieve mission goals. Getting to that insight requires three key components: tools, data enhanced by applied analytics, and a ready workforce.

Tools

The Defense Department has plenty of tools deployed, but their deployment over the years has taken a piecemeal approach without the benefit of a unifying goal. The result is understandably an uneven mix of isolated capabilities to report and analyze cyber vulnerabilities, threats, and potential impact of attacks on IT assets. Moreover, as discussed earlier, there is little linkage established between cyber tools and mission execution tools. The problem is not unknown, as the DOD CIO noted in his strategic vision, "The unnecessary complexity of the network and computing environment limits visibility and impedes the capability to securely share information and globally execute Joint operations."[4]

The tools in use today must be optimized, aligned, and aggregated to produce a more coherent and measurable broad view of cyber readiness that leaders can use to make resource and operational decisions.

"...while there may be many paths to vulnerability and many ways to fail, there are also multiple ways for a network to quickly heal itself to achieve functionality."

Data and Data Analytics

The data sets generated by these cyber and mission tools also must be optimized so they can be aggregated and analyzed. This task begins with a framework for how to compile, standardize, ingest, apply analytics, and then display data that will produce needed situational awareness.

Another important piece of this data challenge is assembling effective diagnostic — and, eventually, predictive — readiness models. These rely on a multi-disciplinary approach that includes both data scientists and domain experts. Data science consists of a variety of disciplines, including mathematics, probability and statistics, information science, data mining, data warehousing, advanced and predictive analytics, and machine learning. The domain experts are those with military cyber and mission readiness experience, people who understand the factors that determine readiness and how those factors interact to create different levels of readiness.

Military readiness systems already contain data for descriptive analytics, such as equipment levels, maintenance schedules, spare parts inventories, supply chains, procurement pipelines, personnel levels, training, and other readiness-related factors. The goal is to include cyber metrics around mission-critical systems and networks into those algorithms and eventually to create diagnostic analytics — and even predictive analytics — that can model the extremely complex relationships among these variables.

Workforce

A workforce that can dependably respond to attacks and disruptions is also critical to readiness. Leaders must know whether staffs possess not only the requisite certifications, but also the necessary skillsets to minimize disruptions and apply creative engineering solutions in response to various scenarios. Moving toward Persistent Cyber Training Environments (PCTEs), which employ automation to establish and maintain persistent and scalable training environments, will enable cyber mission forces to train in emulated network environments while utilizing current cyber tool suites. PCTEs will enable full spectrum training from individual competencies to the team, unit, group and force training. It can also enable – in a human resource management sense or formal request for forces – improved understanding of who has been trained and in what environments.

TOWARD MISSION SUCCESS

Enabling defense leaders to navigate the trade-space between cyber risk / resilience and mission readiness relies on the realization of DoD's strategic IT vision of building a "seamless, transparent infrastructure that transforms data into actionable information and ensures dependable mission execution in the face of the persistent cyber threat."[5]

But achieving this requires that those leaders have visibility into the relationships between cyber risk and mission readiness. Conversely, a mission readiness assessment that fails to account fully for cyber risk holds limited value in today's IT-driven operational environment, resulting in reduced situational awareness and higher risk of failure.

Developing a cyber readiness capability would not only improve the accuracy of readiness assessments, but dramatically improve readiness visibility and management, and optimize resource management and risk trade-off decisions at all levels in an organization where IT spending is decentralized. These benefits ultimately translate into an ability of today's leaders to more readily understand, manage, and be held accountable for their own risk postures and mission readiness.

NOTES

1. *James N. Mattis, Senate Armed Services Committee Nomination Hearing Statement, January 12, 2017. http://www.armed-services.senate.gov/imo/media/doc/Mattis_01-12-17.pdf*
2. *Statement of Lt. Gen. Paul Nakasone, commanding general of U.S. Army Cyber Command, before the Subcommittee on Cybersecurity, Committee on Armed Services, U. S. Senate, May 23. 2017. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf*
3. *"Department of Defense Information Technology Environment: Way Forward to Tomorrow's Strategic Landscape," DoD CIO, August 2016. http://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf*
4. *"Department of Defense Information Technology Environment: Way Forward to Tomorrow's Strategic Landscape," DoD CIO, August 2016. http://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf*
5. *"Department of Defense Information Technology Environment: Way Forward to Tomorrow's Strategic Landscape," DoD CIO, August 2016. http://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf*

OUR AUTHORS

Rafiq Jamaldinian, *Principal*
jamaldinian_rafiq@bah.com

Jonathan Chiu, *Principal*
Chiu_Jonathan@bah.com

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

© 2017 Booz Allen Hamilton, Inc. |