



## Dynamic Defense

Building Enterprise-wide Cybersecurity that Learns, Adapts, and Proactively Combats Rapidly Changing Cyber Threats

**Ready for what's next.**

Booz | Allen | Hamilton

## Table of Contents

Executive Summary .....	1
The Growing Cyber Threat .....	2
The Dynamic Defense Approach to Cybersecurity .....	3
Conclusion .....	8
About the Authors .....	8
About Booz Allen .....	9
Principal Offices .....	Back Cover



# Dynamic Defense: Building Enterprise-wide Cybersecurity that Learns, Adapts, and Proactively Combats Rapidly Changing Cyber Threats

## Executive Summary

Traditional approaches to cybersecurity are proving to be inadequate against today's increasingly sophisticated cyber threats. Too often, governments and businesses find themselves one step behind attackers, reacting to rather than anticipating each new threat. Moreover, today's cyber attacks can strike at the very heart of an enterprise—its intellectual capital, its reputation and brand, and its ability to compete or carry out its mission. A new approach to cybersecurity is required, one that is proactive, dynamic, adaptive, and recognizes that cybersecurity has evolved beyond the realm of traditional IT management. Cybersecurity now resides in the executive boardroom, where cyber issues can be addressed from the perspective of enterprise risk management.

This broader view enables organizations to adopt a Dynamic Defense approach that incorporates a wide range of integrated cybersecurity activities to understand and mitigate enterprise risks. A Dynamic Defense focuses on four areas of cybersecurity:

- **Threat Vector Intelligence.** Actively scans networks and systems, constantly gathering information and intelligence from all sources to: (1) understand its own vulnerabilities; and (2) identify trends and develop insights into current and emerging threats.
- **Rapid Response.** Responds with network speed to breaches and attacks to eliminate threats, keep networks and systems operational, uncover and root out attackers through forensics analysis, measure the impact on brand, reputation, stakeholders, etc., and effect recovery.
- **Evolutionary Response.** Draws insights and identifies cybersecurity strengths and weaknesses through vulnerability assessments, after-action reports, and other organization-wide cyber diagnostics that drive a continuous evolution into a more mature cyber organization.

- **Integrated Remediation.** Implements the improvements, best practices, and lessons learned across all organizational components of an integrated cybersecurity mission framework—policy, people, management, technology, and operations—to address vulnerabilities and gaps, and strengthen overall security.

Dynamic Defense helps the enterprise integrate the major cybersecurity components to create multiple layers of defense within the organization, each layer serving to reduce cyber threats and mitigate overall enterprise risk. By linking operational activities with long-term remediation efforts, Dynamic Defense builds cybersecurity that is proactive, dynamic, and continuously adapting to changing threats and risks.

### Exhibit 1 | Cyber Mission Integration

Cybersecurity is a complex, multidisciplinary challenge that integrates and unites five major pillars of robust security: Management, Policy, Operations, People, and Technology. Cyber Operations supports each of the other functions as it anticipates threats and reduces risk.



Source: Booz Allen Hamilton

---

## The Growing Cyber Threat

The cyber revolution has transformed many nations' economies, societies, governments, and national security organizations. Every major private organization or business, public agency, and military organization relies heavily on digital technologies to carry out day-to-day functions and responsibilities. This includes running power grids, air transportation systems, financial markets, telecommunications, public utilities, and network-centric defense operations. Moreover, the reach and impact of cyberspace is accelerating across national boundaries among increasingly connected international partners in the private, public, and civil sectors. As cyberspace becomes critical to global operations within the enterprise, the potential damage from cyber attacks becomes more severe. As a result, cybersecurity has become essential to business and mission success.

---

*A single successful breach has the potential to undermine a military operation, expose national secrets, drain a corporation's intellectual capital, shut down an enterprise, disrupt financial markets, or immobilize business and government.*

---

The cybersecurity function initially developed within the office of the Chief Information Officer (CIO), where it focused on protecting networks and machines with firewalls, anti-virus software, and other tools. As cyber threats grew in sophistication and size, the Chief Information Security Officer (CISO) emerged to manage the specialized cyber tools needed to counter new threats. The traditional CIO focused on the cost efficiencies of IT services that support the enterprise,

while the CISO focused on business (or mission) continuity and the effective management of risk. But today, as information and communications technologies (ICTs) have become indispensable elements of the modern enterprise, a cyber attack threatens more than networks and machines. A single successful breach has the potential to undermine a military operation, expose national secrets, drain a corporation's intellectual capital, shut down an enterprise, disrupt financial markets, or immobilize business and government. A cyber attack can damage an organization's reputation or brand and severely weaken its ability to compete or perform its mission. It can place the entire organization at risk. Consequently, cybersecurity has moved from the CIO's office to the boardroom, and from a narrow focus on network security, data security, and application security to the broader concern of minimizing corporate risk.

At the same time, cyber attacks and intrusions are also becoming increasingly difficult to stop. Attacks may come from "hacktivists" seeking to publicize political views, from criminal organizations seeking financial gain, from terrorists groups seeking to inflict economic or political damage, or from state-sponsored intelligence and security organizations advancing economic or national security aims. Emerging Advanced Persistent Threats (APTs) adopt extremely sophisticated technological and social engineering techniques; they target specific individuals or entities and then persist for months or even years in their efforts to uncover weaknesses and compromise networks and systems. However, low-tech penetrations—particularly insider threats—remain an extreme danger, as demonstrated by WikiLeaks disclosures. The growing connections within and among organizations, along with mobile computing, social media, and other emerging technologies, exacerbate the security challenge by creating more



opportunities for mischief. As a result, no organization, no matter how strong its defenses, can claim complete cyber invulnerability against today's determined, adaptive threats. The defender must guard all vulnerabilities; the attacker seeks to exploit only one. Because there is always a chance that a system will be compromised or a network will be breached, organizations must be prepared to respond.

## The Dynamic Defense Approach to Cybersecurity

Responding effectively to today's threats requires a cybersecurity program that address threats from an enterprise risk perspective. The CIO, of course, cares intensely about cybersecurity; but the CIO focuses on protecting network and systems in relation to business and operational needs. The enterprise requires a more expansive and holistic view of cyber risks. By addressing cybersecurity from an enterprise risk perspective, the organization can tackle not only the risks to business operations but also to reputation, intellectual capital

and competitiveness, financial viability, and other potential business and mission risks. This broader risk perspective supports a Dynamic Defense approach to cybersecurity that tailors defenses to each organization's unique requirements and risks, based on such factors as its industry or mission, organizational culture, work processes, employee composition, and networks and systems.

In addition to reflecting an enterprise risk perspective, the Dynamic Defense approach is characterized by two other important features. First, it recognizes that no network is impenetrable and so, rather than placing all bets on stopping every attack at the perimeter, it creates a system of layered defenses and rapid response capabilities that minimize overall enterprise risk. A rapid response enables organizations to "stop the bleeding" through triage efforts and to assess, plan, respond, and recover networks and systems to a secure operational state that minimizes business impact, brand, and reputation.

---

Second, the Dynamic Defense approach integrates the Cyber Mission Integration Framework that encompasses five major organizational components and activities: policy, people, management, technology, and operations. Although a robust Dynamic Defense relies heavily on strong operational components—such as threat intelligence and incident response operations—it also requires the right policies, skilled cyber staff and properly trained employees, effective cyber technologies, and a capable management structure overseeing a wide range of cyber-related activities. At the same time, the analyses, insights, and lessons learned generated by Dynamic Defense operations and enterprise-wide assessments provide valuable feedback that enable organizations to refine and improve all five cyber mission components. In this way, the Dynamic Defense approach builds deep layers of defense that not only support the broad spectrum of operational activities—deter, prevent, detect, respond, and recover—but also enable the organization to stay one step ahead of constantly changing APTs and other threats through continuous improvements to its integrated cybersecurity mission framework.

The Dynamic Defense approach to cybersecurity focuses on four major areas:

**Threat Vector Intelligence.** The vigilant enterprise understands its cyber environment, vulnerabilities, and threats, particularly its adversaries and their capabilities and intent. An adversary can be a competitor company, a nation state, a terrorist group, criminal enterprise, or individual actor, such as a hacker. Some may represent sophisticated APTs that will persist and adapt to cyber defenses. Some may intend to steal a company's proprietary software design, a bank's financial data, or a federal agency's sensitive data; or they may want to embarrass an organization by defacing its website or disrupting its services. But their capabilities—the time, money, and skilled resources they can bring to the task—will vary significantly.

Adversaries' capabilities and intent must be evaluated within the context of the organization's mission and vulnerabilities. For example, a healthcare organization may be concerned with the threat of cyber criminals who seek to obtain customer personally identifiable information (PII). Consequently, intelligence activities



---

might be geared towards analyzing criminal organizations and the underground PII market. By understanding how criminals generate value from the theft and sale of PII, the healthcare organization can adopt measures to ensure that any compromise of PII is of little or no value to criminals. Similarly, intelligence collection on adversary attack vectors might reveal that targeted spear-phishing is a favored tactic. This intelligence would inform corporate-wide e-mail security policies and guide personnel training on how to handle suspicious e-mails.

---

*An in-depth understanding of potential adversaries' capabilities and intent enables the organization to build the most effective I&W triggers and the strongest operational response to cyber attacks.*

---

With this understanding of its vulnerabilities and potential adversaries, the organization can better anticipate each adversary's strategy and techniques used for attack. The organization can be proactive in establishing indication and warning (I&W) triggers that know where to look and what to look for—the likely signatures and footprints—in an adversary's attacks. Automated monitoring tools continuously scan networks and systems, gathering information from all sources not only to defend against known threats but also to identify trends and develop insights into new and emerging threats. When a breach or attack is detected, the enterprise must take immediate action, and so the I&W triggers are programmed to automatically respond. An in-depth understanding of potential adversaries' capabilities and intent enables the organization to build the most effective I&W triggers and the strongest operational response to cyber attacks.

**Rapid Response.** When I&W triggers or other information signals a potential incident or attack, the enterprise responds with the upmost speed to contain the threat, eradicate it, facilitate a rapid recovery, and investigate the potential long-term damage beyond the company's networks and systems. This latter objective is extremely important. Many organizations focus their response activities on getting networks, databases, and applications restored so that normal operations can be resumed as quickly as possible. Restoring operations quickly is important, but the enterprise also needs to know how its business or mission capabilities may have been impacted by the attack. The enterprise could suffer serious harm if its leaders do not know, for example, what data has been stolen and who may have taken it.

Consequently, while the cyber response team is repairing networks and getting systems up and running, responders must also investigate what the attackers may have gained. Did they steal sensitive data, such as a proprietary design for new software, the formula for a new drug, the Social Security numbers of customers, or classified intelligence data? Did they implant malware that can spy on networks or trigger a shutdown of power grids? These types of investigations require more sophisticated forensics capabilities than needed to restore operations, such as reverse engineering of the attack to uncover a Trojan virus or identify precisely which data was exfiltrated and, potentially, by whom. Obtaining this information is absolutely critical to minimizing enterprise risk.

Rapid response represents more than protecting information and networks. When it includes deep-dive forensics to uncover what happened, rapid response not only enables the enterprise to respond quickly to eliminate threats and keep networks and

---

systems operational, it also provides boardroom executives with the information they need to respond effectively to the strategic implications of an attack. In addition, an organization that seeks to improve its cybersecurity maturity will have response plans, policies, management structures, trained cyber personnel, and the technologies needed to effectively respond and minimize overall impact.

**Evolutionary Response.** The enterprise works continuously to better understand the threat environment and develop more effective response strategies. It gathers information as it scans networks, conducts vulnerability assessments, initiates after-action reports following attacks, and examines proven best practices. This holistic diagnostic is particularly useful in helping enterprise leaders identify ways to strengthen the depth and breadth of cyber defenses beyond network monitoring, examining how all integrated components of the cybersecurity mission—policy, people, management, technology, and operations—can be improved. For example, this may include diagnosing the ability of the organization to train cyber personnel; establish effective governance or access rights; implement the most appropriate identity and access management controls; or to forecast the technological innovations that will best suit business needs. The analysis also provides ongoing insight into adversaries’ capabilities and intentions, while discovering cyber weaknesses and offering lessons learned to strengthen cybersecurity.

---

*As new solutions are rolled out across the organization, the enterprise works to ensure that cyber operations are integrated with policy, people, management, and technology, so that all components are operating effectively together.*

---

Assessments across the organizational components—policy, people, management, technology, and operations—are essential to evaluating the cybersecurity maturity of the organization. The diagnostic information and analyses enable executives to develop a strategic roadmap for achieving greater levels of cyber maturity and reducing enterprise risk.

**Integrated Remediation.** The enterprise strengthens its defense posture by implementing the remediation strategies and cyber solutions prescribed by the assessments and diagnostics conducted as part of Evolutionary Response. The new “in-depth” defense solutions might include:

- Implementing supply chain asset management to minimize the risk of software vulnerabilities, counterfeit products, or malware entering the firm through supply chain partners;
- Developing policies about employees’ use of Twitter and social media sites, training employees on the safe use of social media, and implementing technology to monitor social media activities;



- Compartmentalizing business- and mission-critical data, and applying tighter identity management controls to protect the data;
- Implementing application security layers that are separate and distinct from data security;
- Implementing security safeguards that prevent the unauthorized printing or downloading of sensitive documents;
- Reprogramming I&W triggers to incorporate intelligence about new APTs;
- Introducing a new training program to ensure that cybersecurity professionals possess the most up-to-date knowledge and skills.

As these examples show, the feedback and remediation solutions generated by a Dynamic Defense pertain not just to cyber operations but to all five components of the Cyber Mission Integration Framework. As new solutions are rolled out across the organization, the enterprise works to ensure that cyber operations are integrated with policy, people, management, and technology, so that all components are operating effectively together. At the same time, an enterprise-wide perspective enables executives to adopt a remediation strategy that most effectively addresses the organization's security requirements and risk profile, creating enterprise-wide cybersecurity that is proactive, dynamic, and continually adapting to changing threats.

# Conclusion

---

Businesses and government agencies are under constant attack from adversaries looking to disrupt their operations or gain an advantage by stealing valuable information, such as intellectual capital, strategic plans, financial data, public records, or military secrets. Many large organizations are attacked more than a thousand times every day. Today's APTs probe, phish, feint, dodge, and deceive as they attempt every stratagem to exploit weaknesses and circumvent barriers. Their tactics grow increasingly sophisticated and change constantly in response to the defensive systems they encounter. Countering such threats requires a Dynamic Defense that evolves with the changing threat. By focusing on the four major areas of Dynamic Defense, the enterprise can create in-depth cyber defenses that are continuously improved—across people, policy, management, technology, and operations—to build an enterprise that excels at reactive and proactive cybersecurity. The enterprise can react with maximum speed and effectiveness to attacks because it has been proactive in anticipating and preparing for those very attacks.

Each organization will adopt Dynamic Defenses that best fit its unique circumstances and needs, and the best way to accomplish this is to approach cybersecurity from an enterprise risk perspective. This will allow executives to allocate cyber resources and build layered defenses aimed at not just protecting networks and data but also at minimizing overall risk to their business or mission objectives.

The stakes are growing higher. Responsibility for cybersecurity has risen to the boardroom because the impact of a cyber attack can reverberate throughout the enterprise and, increasingly, threaten its profitability or public mission. Unprincipled foreign governments, terrorist groups, and cyber criminals are stealing ideas and secrets—and are using them to bolster their own financial, technological, and national security capabilities at the expense of nations and businesses that play by the rules. We can never declare victory in cybersecurity, but a Dynamic Defense approach can turn the advantage decisively in our favor.

# About the Authors

---

**Robert J. Lamb**, a Booz Allen Hamilton Senior Vice President, leads the firm's cyber operations business, providing support across the cyber operations mission area. His major clients include the US Cyber Command along with several of the National Cyber Centers. Before joining Booz Allen, he served as a Signal Officer in the US Army. He concluded his military career as the Chief of Staff for the Joint Task Force for Computer Network Defense.

**Christopher Ling**, a Booz Allen Hamilton Senior Vice President, leads the firm's business in military intelligence which includes the Defense Intelligence Agency (DIA), Service Intelligence Components, and Combatant Command Intelligence Directorates (J2s). He specializes in developing high-level strategies to

innovate and improve intelligence support to operations. He has 20 years of experience managing intelligence and information technology system concept definition, trade analyses, requirements, modeling, and simulations.

**Randy Hayes** is a Booz Allen Hamilton Vice President who leads the firm's Army Military intelligence business. He also provides specialized Strategy Development and Change Management leadership across the Military Intelligence Community, spanning all military services within the Department of Defense. He is also a leader in Booz Allen Hamilton's Strategy Development and Change Management Center of Excellence, focusing on developing strategies for clients across the federal government.

# About Booz Allen Hamilton

---

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, Booz Allen is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients in the Middle East. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

The firm's management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant's problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm's many client relationships

that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 25,000 people, and had revenue of \$5.59 billion for the 12 months ended March 31, 2011. *Fortune* has named Booz Allen one of its "100 Best Companies to Work For" for seven consecutive years. *Working Mother* has ranked the firm among its "100 Best Companies for Working Mothers" annually since 1999. More information is available at [www.boozallen.com](http://www.boozallen.com). (NYSE: BAH)

## Contacts

### **Robert J. Lamb**

Senior Vice President  
[lamb\\_robert@bah.com](mailto:lamb_robert@bah.com)  
703-984-0742

### **Randy Hayes**

Vice President  
[hayes\\_randy@bah.com](mailto:hayes_randy@bah.com)  
703-377-5501

### **Christopher Ling**

Senior Vice President  
[ling\\_christopher@bah.com](mailto:ling_christopher@bah.com)  
703-902-5679



## Principal Offices

---

Huntsville, Alabama

Sierra Vista, Arizona

Los Angeles, California

San Diego, California

San Francisco, California

Colorado Springs, Colorado

Denver, Colorado

District of Columbia

Orlando, Florida

Pensacola, Florida

Sarasota, Florida

Tampa, Florida

Atlanta, Georgia

Honolulu, Hawaii

O'Fallon, Illinois

Indianapolis, Indiana

Leavenworth, Kansas

Aberdeen, Maryland

Annapolis Junction, Maryland

Hanover, Maryland

Lexington Park, Maryland

Linthicum, Maryland

Rockville, Maryland

Troy, Michigan

Kansas City, Missouri

Omaha, Nebraska

Red Bank, New Jersey

New York, New York

Rome, New York

Dayton, Ohio

Philadelphia, Pennsylvania

Charleston, South Carolina

Houston, Texas

San Antonio, Texas

Abu Dhabi, United Arab Emirates

Alexandria, Virginia

Arlington, Virginia

Chantilly, Virginia

Charlottesville, Virginia

Falls Church, Virginia

Herndon, Virginia

McLean, Virginia

Norfolk, Virginia

Stafford, Virginia

Seattle, Washington

*The most complete, recent list of offices and their addresses and telephone numbers can be found on [www.boozallen.com](http://www.boozallen.com).*

Booz | Allen | Hamilton

---

delivering results that endure