[OPPORTUNITIES FOR IMPACT]

Reducing Risk Through Collaboration

Cybersecurity: It’s About the Mission

The digital age is a double-edged sword for federal civilian government organizations. The increasing interconnectivity of our technologies enables government agencies to improve information and service delivery to the public. At the same time, the dependence on networked technologies for mission fulfillment places those very missions at risk. A cyber attack on an agency’s technology systems could prevent it from providing the services and protections its constituents depend upon.

Mission Execution and Cyber Risk Are Intertwined

“Mission breaches” have the potential for devastating consequences. They can expose confidential information, erode infrastructure reliability, damage public trust, endanger human safety, harm the economy, and even threaten our national security. The government must be able to sustain mission-essential services to the public despite cyber attacks and disruptions.

Securing data is not enough. Organizations must assure their missions by managing the risk inherent in the use of information systems.

To address the increasing risk that lies at this intersection, we recommend that agencies closely link their mission and cybersecurity strategies. This approach would call for agency leaders responsible for cybersecurity concerns to work with those responsible for mission operations, policy, and planning to address the perils—and promise—of networked technology. Through their collective insights and perspectives, cross-organizational teams can better outline a holistic picture of the agency’s cybersecurity risks and identify what can be done to mitigate them at all levels of the organization.

Background: Blocks to Build On

Over the past years, Congress and the executive branch have passed laws and enacted government-wide policies and programs to improve cyber risk management. These include:

- The Federal Information Security Management Act
- The 2015 Cybersecurity and Implementation Plan for the Federal Civilian Government
- The 2016 Cybersecurity National Action Plan
- Threat information sharing policies and practices as codified in the Cybersecurity Information Sharing Act of 2015
- Boundary protection and monitoring measures such as EINSTEIN and the Trusted Internet Connections
- Cross-government cybersecurity services efforts such as the Continuous Diagnostics and Mitigation program

These and other government-wide and individual agency initiatives have created a foundation for future cybersecurity efforts. But they will be incomplete without strengthening the connections between cybersecurity, mission execution, and enterprise risk management.

Discussion: Many Strategies, No Silver Bullet

No single action will bring mission execution and cybersecurity closer together. However, there are several elements of an overarching strategy that a new administration can promote. These include:

- **Adopting an Adaptive Defense:** Cyber defenders must anticipate and quickly adapt to threats in order to support ongoing mission performance. This requires greater focus on countering adversaries both before they enter networks and after they have breached them. It also necessitates using shared information to tailor defenses, and adopting resilience approaches that increase the likelihood of continued mission execution in the face of attack or disruption.
- **Addressing Holistic Risk:** Cybersecurity has often focused on risks to data confidentiality, availability, and integrity—such as theft of intellectual property. Changing technologies (e.g., Internet of Things, Cyber-Physical Systems) used in support of mission performance require cyber defenders to take a more holistic view of risk—one that also considers physical risks to human safety and infrastructure reliability.
- **Strengthening Trust in Technology and Users:** As networked devices play increasingly important roles in mission execution, the need for stronger trust in both the systems and the humans who use them increases. Organizations can increase the trustworthiness of their technologies by instituting strong security engineering at each stage of the system life cycle. Based on how a system will be used, agencies can assess the level of trust needed by a system or user and institute the appropriate protections.
- **Cultivating a Shared Mindset:** More than any technical issue, human attitudes are critical to address the risks that lie at the intersection of mission execution and cybersecurity. Cultivating a shared mindset requires greater focus on communicating the relationship between mission performance and cybersecurity. Agency leaders must send a clear message that cybersecurity is not just a static compliance exercise but requires ongoing evolution and continuous improvement in a collaborative manner.

Recommendation

The President direct the Office of Management and Budget (OMB), to work with federal departments and agencies to implement policies in support of adaptive defense, holistic risk, trust, and shared mindset. Further, direct the National Institute of Standards and Technology (NIST), working with the Department of Homeland Security (DHS), OMB, and industry, to review the Framework for Improving Critical Infrastructure Cybersecurity and Risk Management Framework to further encompass concepts of adaptive defense, holistic risk, trust, and shared mindset.

For further ideas about applying the guidance in this paper to your agency's particular needs, email cyber@mitre.org