McKinsey&Company

Public Sector

The public sector’s cybersecurity imperative

May 2012

Tucker Bailey
Aamer Baig

The public sector's cybersecurity imperative

"Down the road, the cyberthreat will be the number one threat to the country."

—Robert Mueller, Director of the Federal Bureau of Investigation

On February 29, NASA's Inspector General reported that the organization had been the victim of over 5,000 cyber-incidents during the period from 2010 to 2011. In 2011, it experienced 47 attacks of such sophistication that the attackers had "full functional control over these networks."

On January 20, officials in the US Department of Commerce discovered evidence of a significant infiltration of the Economic Development Administration's (EDA) IT network. As a result of the attack, employees were prevented from accessing the Internet for more than a week. While the facts are still being determined, the severity of this attack likely points to a sophisticated adversary specifically targeting the EDA.

Although these attacks are significant in their own right, their true impact should be that of a catalyst for permanently improving government agencies' cybersecurity positions through changes in policies, processes, technology, and governance. These attacks are also a harbinger of a broader, systemic threat facing US government institutions.

NASA and the Department of Commerce are discovering what officials at the Department of Defense has known for some time—that they are the targets of systematic, sophisticated cyber-adversaries and that they must develop a new paradigm when it comes to protecting their sensitive information.

In this white paper, we discuss the emergence of this new threat, the approach for designing a next-generation cyberdefense, and testing and assessing agencies' ability to respond to emergent attacks in the future.

The emergence of advanced persistent threats

Hackers such as those that likely targeted NASA and the Department of Commerce fall under the category of Advanced Persistent Threat (APT). APTs, which often enjoy protection and support from state actors, possess the resources and patience to systematically probe organizations until they find a point of entry into the network. While APTs are highly proficient in leveraging technical vulnerabilities, they increasingly find their way into systems through social engineering—exploiting the behavioral vulnerabilities of an organization's employees or other stakeholders. Once inside a network, the APT's code may sit dormant for long periods of time or it may methodically expand its presence throughout the network. *An organization has typically been infiltrated long before the APT's actions are identified.*

APTs have differing motivations, but typically engage in hacking to obtain a financial or political advantage. Criminal syndicates routinely tunnel into financial accounts and siphon money into third-party accounts. State actors regularly target national-security systems to gain a military advantage and hack into commercial and government organizations to obtain intellectual property or insights into trade policy. *What is consistent is that APTs represent an enduring threat to critical systems across the US government and economy.* Defending against the APT threat has become the new reality for government security professionals. As a result, it is critical they share threat information and develop a more integrated response across civil government, the intelligence community, and the private sector.

Designing a next-generation cyberdefense

Undoubtedly, NASA and the Department of Commerce are drawing on the best resources in government to address the immediate issue, stabilize their systems, close the vulnerabilities identified by forensic analyses, and develop a playbook for responding to future breaches.

However, the greatest opportunity for government agencies comes from looking beyond recent breaches and building resilient security systems that will have the ability to detect, deter, and defend against the next generation of cyberattackers.

A comprehensive "mission back" cybersecurity strategy is an imperative for organizations with the depth and reach of our government's institutions. Such a strategy should be predicated on protecting the most important information assets from the most likely threats. It should include the following six elements:

- **Identify the most important information assets** across the organization. These assets—the agency's "crown jewels"—are those pieces of information that, if compromised, would prevent the agency from effectively executing its mission and may include categories such as intellectual property, control systems, predecisional economic indicators, foreign trade data, or citizens' and employees' Personally Identifiable Information (PII).

- **Categorize the highest priority threats.** An effective strategy defends against the most likely attackers. Rather than trying to defend against every contingency, agencies should focus their defenses against the attack patterns employed by its highest-priority threats. This will require developing a forward-looking analytical capability that assesses the evolving threat landscape and attunes the organization to changes in the threat environment. Developing such an intelligence function will allow agencies to anticipate potential adversarial activities based on real-world events. Cyberattacks are often precipitated by real-world actions, but the indicators are routinely missed, leaving organizations vulnerable.

- **Assess existing capabilities** and the ability to defend highest-priority assets. Conducting an asset and threat-based review of government agencies' cybersecurity infrastructure will highlight areas for improvement. Many organizations assess their cybersecurity in terms of perimeter vulnerabilities rather than how well it defends their most important information assets.

- **Design an in-depth approach to defense** that uses multiple levers to protect each high-priority asset. These levers include technical tools such as robust data-loss prevention and encryption, process changes, such as limiting access to the most critical assets, and behavioral shifts that reinforce sound security procedures. Our public-sector institutions can no longer rely solely on network-perimeter defense and must put additional internal protections in place under the assumption that the adversary is already inside the castle walls.

- **Develop an internal counter-APT campaign** to detect and "fingerprint" APT actors. Best-in-class organizations have created dedicated cyberintelligence teams that conduct forensic analyses of historical events and share and collect cyberthreat information from peer organizations and federal agencies. While civil government agencies have been undoubtedly coordinating with the "three letter agencies" to remediate recent attacks, it will become imperative to formalize and systematize these relationships. Investing in this capability will sensitize agencies' detection and monitoring team to APT patterns and modus operandi, helping to identify APT activity before the APT is able to extract data.

- **Shift mind-sets, educate, and establish governance** to strengthen cybersecurity posture. While technology investments are critical to developing a next-generation defensive capability, perhaps the most important factor will be creating a security mind-set within the organization. This mind-set shift is required to enlist all employees of an agency in the fight against cyberattackers. Effective governance will guarantee personnel are adhering to appropriate security protocols. A concerted awareness-building campaign will ensure they understand the severity of the threat facing them, and their role in protecting their agency.

While advanced threats cannot be wholly defeated, invasive actions can be detected earlier and countermeasures can be put in place before APTs can access high-priority information assets. While the enemy may be inside the castle walls, it can be kept out of the throne room. It is this ability to operate in a degraded environment that will separate the next-generation cybersecurity leaders from the pack.

Testing and assessing government agencies' ability to respond in the future

As an organization develops its next-generation capabilities, it will need to routinely test its security posture to assess its ability to respond to emergent threat situations. These tests should stress agencies' ability to recognize and react to the most likely threat scenarios in real time.

Best-in-class organizations routinely assess their ability to respond to threat scenarios by conducting enterprise-wide "war games" of cyberevents. These war games simulate a cyberattack scenario and test not only the IT defenses but also the operational response to the breach.

War-game exercises offer three significant benefits to an organization. First, they align the organization and raise awareness of the highest-impact cyberthreats. Second, they assess the organization's ability to respond in real time to an emergent attack. Third, they build institutional muscle memory to respond in the event of an actual attack. Cybersimulations allow government organizations to "practice like they'd play" in the event of an actual breach.

Cyberwar games often surface insights that may not be identified in audits or traditional diagnostics. For example, one organization realized they had inconsistent messages in prepared communications aimed at different stakeholder groups that would have generated a significant media outcry if they were issued. Similarly, another organization discovered that its contingency communication plans were based on a system that would have been rendered inoperable by a potential attack. Identifying failure modes such as these—in the "no fault" environment of a war game—will ensure government agencies retain a robust ability to respond to future threats.

The mandate for government institutions

The recent attacks on NASA and the Department of Commerce are representative of a broader, systemic threat posed to critical systems inside and outside government agencies. Such a pervasive threat has implications writ large for the US economy. The theft of intellectual property, corporate espionage, financial fraud, and the latent threat of critical national infrastructure all imperil the free flow of commerce.

While the recent cyberattacks caused significant harm, they also provided an opportunity to learn from historical shortcomings. Government institutions can recognize this as a call to action and design a robust next-generation cybersecurity strategy to safeguard their most important assets, ensuring the ability to operate even in the face of increasingly sophisticated cyberthreats.

●●●

Tucker Bailey is an expert associate principal in McKinsey's Washington, DC, office. **Aamer Baig** is a principal in the Chicago office.

Contact for distribution: Shannon Kelly
Phone: 1 (202) 662-3288
E-mail: Shannon_Kelly@mckinsey.com

Public Sector
May 2012

Designed by Editorial Shared Services design team