Lessons Learned from Maturing Zero Trust

Highlights from an April 2022 Roundtable

The transition to Zero Trust across the Federal Government is in full swing due to M-22-09. Agencies are racing to meet those guidelines to drastically improve cybersecurity Government-wide and learn how to manage and mature Zero Trust initiatives.

To assist agencies in moving beyond the planning and initial deployment of Zero Trust, the Advanced Technology Academic Research Center (ATARC) recently hosted a roundtable in partnership with **Swish** and **Zscaler** to discuss the shifting scenario of Zero Trust in light of the new requirements.

Roundtable participants were experts in agencies that have already begun their ZTA initiatives. They shared their experiences and the lessons learned through the process. Zero Trust shouldn't be a siloed effort in the Federal Government: cross-collaboration will be essential.

New Day, Same Issues

While the Zero Trust mandate has garnered most of the attention lately, the idea of cybersecurity as a priority is nothing new. Since 1997, The General Accounting Office (GAO) has listed information security a high-risk area for the Federal Government.

More recent GAO reviews have identified weaknesses regarding:

- Access controls
- Configuration management
- Protection of data shared with external entities.

GAO has made numerous recommendations to address these.

GAO has made more than 3,700 recommendations on cybersecurity issues since 2010, with over three-quarters of those implemented by the end of 2021.

Obviously significant issues remain. While the GAO has made cybersecurity a priority in audits for 25 years, and the Federal Information Security Modernization Act of 2014 (FISMA) has improved information security program effectiveness Government-wide, there's still work to do.

Participants in the roundtable shared that many of the initial GAO findings in 1997 still apply today. While overall understanding of government cybersecurity risks has improved, that progress is not even across all agencies. Some organizations are still not compliant with previous cybersecurity mandates.

"Technical debt" in the Federal Government is real, making the transition to better security processes difficult. Those issues must be addressed before there can be meaningful transition towards ZTA, as compliance is not possible if vulnerabilities exist due to legacy code or network infrastructure.

Participants noted that there is a critical need for change in organizational structure (i.e., "who owns what," etc.) and in organizational culture. ZTA is a Government-wide effort, and with a continuing shortage of qualified experts and the workforce in general, agencies must pool their resources.

Insights from Zero Trust Planning

Per M-22-09, agencies were expected to submit their Zero Trust plans by March of this year. In the Roundtable discussion, similar challenges in the planning process and insights on how best to tackle ZTA emerged.

Understand where you are and where you want to be

Participants repeatedly mentioned that a clear understanding of current architecture is critical to meeting M-22-09 mandates. This involves fundamental levels of how agencies conduct work, address risk, and grant access. Only then can solutions be found to solve the existing shortcomings. Notably – software is only part of the solution.

Break down barriers

While cross-collaboration between agencies is critical, they must also strive for internal harmony. Many participants had seen great success in breaking up ZTA initiatives into smaller chunks with specifically designated project assignments. Regular reconvening is vital to ensure the transition is not resulting in new issues, however.

Participants suggested building teams around the pillars in M-22-09: **Identity; Devices; Networks; Applications and Workloads; and Data**. This way, work can happen simultaneously across all aspects of ZT making it easier for agencies to meet the short deadlines set by the Zero Trust memo.

CISA's Five Zero Trust Pillars

1. **Identity:** Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.
2. **Devices:** The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.
3. **Networks:** Agencies encrypt all DNS requests and HTTP traffic within their environment and begin executing a plan to break down their perimeters into isolated environments.
4. **Applications and Workloads:** Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.
5. **Data:** Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data and have implemented enterprise-wide

Get Buy-In

Participants admitted struggles with finding funding given the speed of technology evolution. The appropriations process is often arduous but securing funding can be easier when supported by plain-and-simple descriptions of desired outcomes and reasoning for their importance. The IT side of the Federal Government has already bought into Zero Trust. Of the three challenges broadly discussed, the financial side of it is perhaps the most difficult for agencies to manage.

Underfunded and Unfunded Mandates

While the Federal Government is budgeting for Zero Trust, most participants agreed that, by and large, it is not enough to implement ZTA. The challenge of stretching agencies' limited funds to cover Zero Trust initiatives is similar to any other program subject to taxpayer funding.

Participants laid some blame on the inability of Congress to pass a full budget regularly, instead relying on continuing resolutions that are meant to fund essential government functions while lawmakers work towards a full budget. But even when passed, those budgets are often insufficient.

Participants suggested that if agencies work within the assumed constraints of inadequate funding, it might lead to reprioritizing Zero Trust above other concurrent modernization initiatives and pool resources between ZT teams across agencies.

As revealed by insights above, concrete plans to transition to ZTA can further promote its reprioritization. Less than two years remain before agencies are expected to adopt Zero Trust fully – and budget battles are to be expected.

One participant noted that while the deadline is approaching, Zero Trust does not have a finite endpoint. Balancing time, money, and scope will be critical to ensure agencies get to the Administration's prescribed expectations.

Where To Find Help

Swish provides the expertise to guide and implement the transition to ZTA quickly and effectively, employing a **Zscaler** cloud platform.

Contact ATARC today to learn more and get involved in ATARC's Cybersecurity Working Group, or attend our many security-themed events.