Governance, Standards, and Shared Services Can Drive Effective Implementation of Zero Trust Strategies

By Margaret Graves

Federal agencies and their partners are engaged in a continuous and ongoing dialog about improvements to our cybersecurity posture. I am heartened by the fact that there is such continued focus on the topic and accelerated momentum in implementing improvements.

With the January 26th release of OMB Memorandum M-22-09, and the release of the National Security Network Advisory Committee (NSTAC) draft, Report to the President: Zero Trust and Trusted Identity Management, I want to take the opportunity to emphasize certain recommendations from the draft report and to share what I am hearing from my colleagues in industry and government as to the challenges and opportunities associated with the implementation of zero trust.

The NSTAC draft report contains twenty-four recommendations and identifies nine of those as a priority for agency

> *Governance . . . is key to a successful long-term federal enterprise implementation of zero trust.*

Margaret Graves *is a Senior Fellow with the IBM Center for The Business of Government.*

implementation. The nine priority recommendations, from my perspective, fall into three categories: governance, standards, and shared services.

Keys to Zero Trust

It is important to address governance at the outset, as it is key to a successful long-term federal enterprise implementation of zero trust. The NSTAC draft report states the need to establish a whole-of-government approach and to manage implementation at an enterprise level, complete with all the expected governance elements. Those elements include, at a minimum, an enterprise program management office (PMO), a reporting and accountability structure, a unified plan, and oversight from appropriate stakeholders. If this structure is not in place, we risk the real possibility of agencies pursuing individual transactional improvements without the benefit of a clear vision.

In a conversation regarding this topic with Francis Rose on The Daily Scoop, I referred to the fact that there is already precedent for this enterprise model. The Continuous Diagnostics and Mitigation (CDM) program and its PMO were established within the Department of Homeland Security/CISA to ensure a set of cybersecurity improvements were met from a governmentwide perspective. The program was legislated by Congress, with appropriated centralized funding and a mandate to build an enterprise implementation plan inclusive of all agency activity.

In addition, the CDM PMO executed a centralized acquisition strategy and established shared services for agencies to use. OMB and DHS held periodic progress reviews with agencies and reported to Congressional stakeholders as required. There is already a baseline of cyber reporting and what is added should indeed be minimal.

Both the Federal Information Security Modernization Act (FISMA) and the Federal Information Technology Acquisition Reform Act (FITARA) have recently been the subject of legislative revisions, so there is a very real and timely opportunity to rationalize all cyber reporting requirements, avoiding any additional burden and ensuring that all measures are congruent. Finally, all this activity must be underpinned by best practice frameworks, maturity models and playbooks, and ultimately codified in National Institute of Standards and Technology (NIST) standards.

A Long-Term Vision

Establishing governance, standards, and shared services will focus us on the long-term vision, but agencies are already in the throes of implementing the short-term requirements of zero trust. The DHS/CISA Zero Trust Maturity Model establishes pillars or areas of focus for zero trust implementations. Those pillars are identity, device, network/environment, application workload and data.

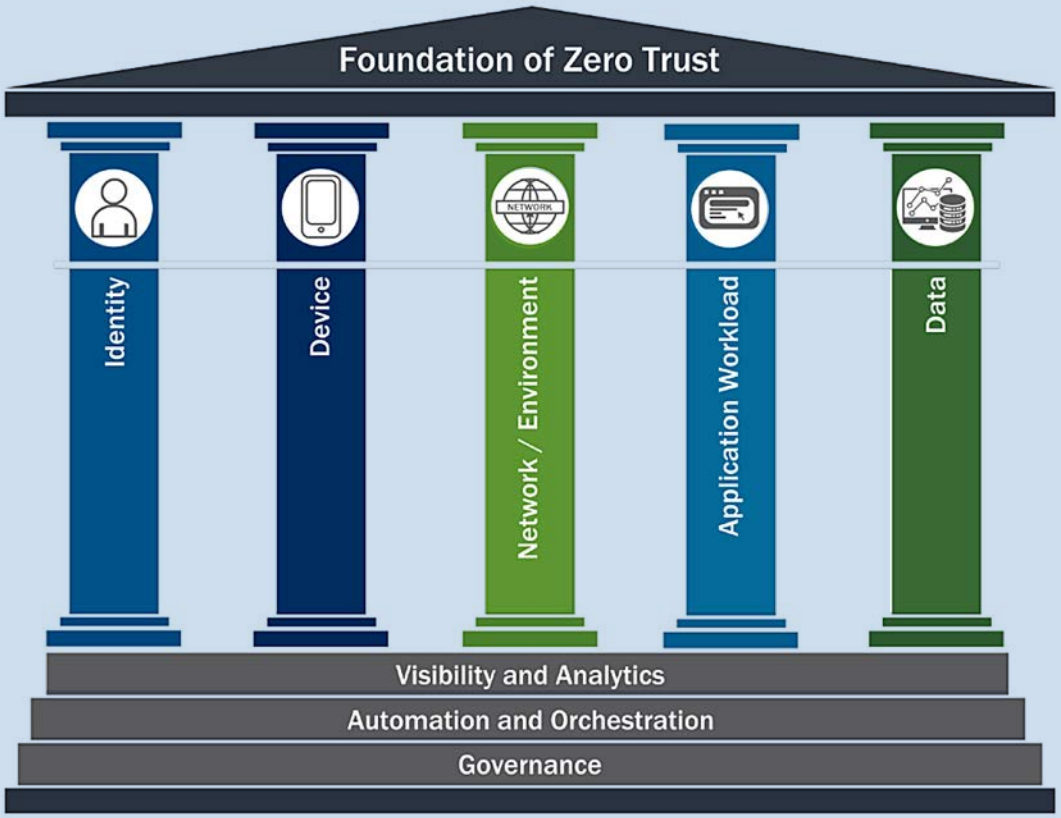
CISA Zero Trust Maturity Model does not prescript a starting point, and indeed every agency will be developing a roadmap based on its legacy environment and a risk-based assessment of opportunities to rapidly improve cyber posture. In addition, the maturity model does not imply that these pillars should be addressed in a stove-piped manner. Agencies should take advantage of ongoing cyber initiatives where investments have already been made while augmenting that activity with complementary projects that could enhance outcomes. Agencies can integrate cyber improvement initiatives across all the pillars by borrowing from the agile methodology and driving implementation across the domains through the application of use cases or user stories.

When you study the graphic representation of the CISA Zero Trust Maturity Model, you notice that the two pillars that "bookend" the model are "identity" and "data." In discussions with my government and industry colleagues, a common theme emerges of identity, data, and the intersection of the two elements being key.

The Bottom Line

Zero trust has at its center the concepts of data architecture and identity and access management. The incorporation of the principle of "least privilege access" requires that agencies understand their data and data flows, and how employees, external partners and customers interact with that data. This fundamental foundation must be established to correctly classify the protection level required for data and to develop appropriate fine-grained permissions for access. This foundation is also necessary to take full advantage of the tools and analytics that can accelerate and augment the implementation of zero trust.

Most importantly, establishing an effective data architecture and identity and access management ruleset is work within the purview of the agency personnel who best understand the mission and data within their portfolios. My observation is that most agencies have not completed this work in its entirety, but must do so to move forward with speed. The good news is that the Foundations for Evidenced-Based Policy Act has already established the imperative for CIOs, CDOs,



Source: *This illustration was inspired by Figure 1 of the American Council for Technology (ACT) and Industry Advisory Council (IAC) "Zero Trust Cybersecurity Current Trends," (2019). https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf.*

and program executives to work together to understand and make best use of their data for policy making, mission execution, and program performance/management. In parallel to establishing a data and access baseline, agencies can take best advantage of technologies and toolsets to improve operational cybersecurity.

Effective Implementation

Some examples of technical approaches and tools available to agencies to enable implementation include:

Data discovery and classification tools and technology that assist with establishing data provenance and tracking data flows. Dynamic, automated data discovery and tracking highlights the behavior and flow of data and allows agencies to understand how the data is accessed and used by agency personnel and customers/citizens. Data tracking uncovers areas of vulnerability that should be addressed to enhance data loss prevention programs, and prevent inappropriate access and improper data exposure. The study of data use patterns also gives agencies visibility into how the data is morphed and changed through use in mission processes and identifies areas where multiple data stores of the same data can be reduced.

Identity proofing that incorporates biometrics and behavior. Companies and government entities are increasingly turning to algorithms and artificial intelligence/machine learning to curate digital footprint data from multiple sources—i.e., multifactor authentication (MFA) to result in a confidence factor score of an individual's identity. These tools gather multiple data points based on biometrics and behavior. For example, online behavior follows patterns based on an individual's professional activities. If that behavior changes, that identity may have been compromised.

Conclusion

Federal agencies can start with the basics of understanding their data portfolio and integrating that data with appropriate access. It is the most cost-effective way to gain traction. This is not glamorous work, but it is key to success. At the same time, an overarching governance approach needs to be established to integrate and guide all agency activities for long-term success.