Advancing Information Sharing Using Zero Trust Principles

In the 20 years after 9/11, we've seen a remarkable increase in the level of information and data that is shared within Agencies, across Agencies, and with partners across all levels of jurisdictions. Such significant progress had been made that, in February 2017, the Government Accountability Office (GAO) removed "Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland" from the high-risk list. Unfortunately, modernization of the Department of Homeland Security's (DHS) information sharing technology platforms has lagged as both internal and external focus has moved to other, more immediate, problems.

Given the increase in the level, scope, and importance of cybersecurity programs to the business goals of an organization, not to mention the high financial and reputational costs of a cyberattack, business leaders rely on Guidehouse to act as their trusted advisor in their cyber program efforts. Guidehouse's Cybersecurity consultants have experience working across multiple platforms and service capabilities to build integrated solutions, not standalone objects. We understand the burden too many cyber tools in an environment place on both system architectures and the people and processes that support them.

The goal of Zero Trust is to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible. It is an approach, not a tool. The Office of Management and Budget's (OMB) January 26, 2022 Memo (M-22-09), "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," sets forth a strategy for all agencies to achieve major progress by the end of fiscal year 2024, with many of the same goals set forth in Section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 as amended, which established the attributes of the Information Sharing Environment (ISE) that applied to the Departments of Homeland Security, Justice, State, Defense, and the Director of National Intelligence.

Much of the approach for the current information-sharing technology platforms was based on this common goal, to provide approaches that enabled a network of heterogeneous users across federal, state, local, tribal, and territorial users within trusted platforms, using strong identity authentication and policy-based access control for sensitive data and information.

As an example, the current Homeland Security Information Network (HSIN) platform satisfies many of the information-sharing requirements of homeland security mission operators. The information-sharing model is a network of trusted users working in trusted communities with access to cross-mission functions to share information related to national security events, natural or man-made disasters, and ensure the daily exchange of information for law enforcement and intelligence functions.

While HSIN successfully facilitates community-based collaboration, some challenges and limitations remain:

1. The burden of community-based sharing is placed on the administrator of each community of interest to act as a gatekeeper to evaluate the identity and purpose of individuals that should be authorized to work within the community, thus limiting the ability to scale at the speed required to support a natural disaster or other urgent operation need. The number of communities, now in the hundreds, creates a significant threat surface to monitor for data loss and compliance and makes it impossible to clear users not yet identified before the event.

2. Agencies and entities that produce and disseminate information must be cognizant of the users and communities with whom they share, and understand their risks and responsibilities. The major communities such as the National Network of Fusion Centers, and federal agencies that disseminate information and analysis, such as DHS's intelligence, need to duplicate their information into many places, making it a laborious process to get the information out, to ensure it remains up-to-date, and to remove it when it is no longer relevant.
3. The community-based collaboration model has resulted in highly customized commercial off-the-shelf software, with many code adjustments specific to single communities. This has added untenable complexity during upgrades with major software releases and tools, including Spark on AWS Elastic MapReduce, Hadoop's MapReduce, and other technologies.

The last HSIN modernization effort wasn't able to achieve the entire original vision of the ISE as stated in the Intelligence Reform and Terrorism Prevention Act of 2004 in large part because the commercially available technologies were not ready for the complexity of implementing policy base access mechanisms at scale. Given the focus of the Biden administration on increased cyber protection and Zero Trust, as well as advances in technologies over the past 10 years, it is time to overcome these constraints, and to address the alignment to administration shared service priorities such as the use of Login.gov for increased strong authentication procedures, and encryption of data through the entire lifecycle: in transit, at rest, and at access.

It is now possible to shift from a community-based model where users sign in to multiple systems to pull information, to a content-based model, and reimagine a new model that pushes information based on user access rules and published data attributes, as originally envisioned after 9/11 and now in Zero Trust Principles.

Considerations for a New Information-Sharing Model in a Zero-Trust Environment

In the future, platforms such as HSIN should enable content producers to provide access to an integrated set of trusted authoritative content, replacing the content silos of today.

Access to content would no longer be based on whom you know or which community you were a member of, but rather by the verified information about you, or attributes you possess, as confirmed in a trusted identity management capability. When combined with an effective system of information/data governance, policy enforcement, and standard operating procedures, users will be able to get the information they need pushed to them and content producers will be able to trust the information they are providing is being disseminated to the right users.

A new model will require the following shifts, in addition to technology solutions:

1. **Strengthening the role of the data/information steward:**
   Aligning to the Zero Trust principles published by the OMB, technology platforms can provide information/data producers with the capability for a "virtual place" for one trusted source of information for sharing. Each publisher of information signing up to use a "virtual library or trusted source" will categorize the information and data with keywords (aka tagging their data) to describe the types of users that should have access, retention, or expiration dates for content to be managed or removed, as well as attributes such as a level of trust of the device, and location of the device or user, operating system, or network used to secure sensitive information.

2. **Rethink the boundary for governing data and information:**
Consider moving the boundary of data governance by empowering every user of an information-sharing platform with the ability to flag information that is inappropriately tagged, allow suggested updates to the tagging, and crowdsource the ability to increase trust in data and information as well as trust in a process across the system for safe and secure sharing.

3. **Customer experience and data-driven production:**
Deploy features allowing insight into the usefulness of information based on the number of downloads, time spent on content, and/or member-based recommendations for sharing content. This would serve to continue to build trust in data and information by providing a feedback loop to information stewards, while also allowing the virtualized libraries to develop and implement a comprehensive and routine program effectiveness assessment process.

Considerations for Modernization of Information-Sharing Platforms

Assess against the Zero Trust pillars, as well as customer experience goals, such as:

Identity

Device

Network/
Environment

Application
Workload

Data

How do I assess, architect, engineer, implement, and manage solutions to achieve advanced Zero Trust Principles?

- **Is the user and/or end point trusted?**
- **How does the system authenticate users?**
- **What attributes are available to set access policies?**

- **Is the device managed and trusted?**
- **Has this device been allowed previously?**
- **Show the system remembers the device?**

- **Is the connection/ transmission managed and trusted?**
- **What is the location of the network? Is it encrypted?**

- **Is the platform managed and trusted?**
- **Does the platform provide single source of information/data?**

- **Is the data trusted, and who can it be used by and for which purpose?**
- **Has it expired or is it beyond its retention period?**

How does implementing Zero Trust impact the customer experience?
Is the solution causing unnecessary friction for the use of data?

As organizations manage their Zero Trust journeys, finding the best way to architect their information-sharing platforms while modernizing them is critical for mission success. Organizations that approach their architecting strategically and infuse their implementing roadmaps with those goals will see the benefits in improved efficiency, effectiveness, and a better customer experience.