MARCH 2016

SECURING IDENTITY DOES NOT STOP WITH STRONG AUTHENTICATION

The Importance of a Complete Identity and Access Management Strategy, Rooted in Governance

CONTENT:

INTRODUCTION

The “Cybersecurity Sprint” of July 2015 – launched by the White House in the wake of major breaches at the Office of Personnel Management (OPM) – was critical to efforts to improve the security of Federal IT systems. The root of the attack was identity – attackers stole the password of a contractor with access to OPM systems and used it as a vector through which to penetrate these systems and steal millions of records.

The “Cybersecurity Sprint” that followed the attack on OPM focused heavily on closing the vulnerabilities associated with passwords, pushing agencies to dramatically increase their use of two-factor authentication to mitigate the risk of stolen credentials. The results of the “Cybersecurity Sprint” showed that use of Personal Identity Verification (PIV) cards across civilian agencies jumped nearly 30 points – from 42.4% before the breach to 72.1% in the resulting sprint.

These results were impressive, especially given the length of the sprint (30 days). Further progress has been made since the sprint in pushing this number closer to 100%, with a particular focus on ensuring that two-factor authentication be prioritized for the accounts of privileged users with access to multiple systems and data stores. The Cybersecurity Strategy and Implementation Plan (CSIP) – released by the White House in October 2015 – places a heavy emphasis on the link between authentication and privileged users.

Amidst this progress, it is important that agencies do not simply check the two-factor authentication box and proclaim they have “solved” identity security. While authentication is a critical part of identity security, most agencies are dealing with a serious set of identity risks that extend far beyond passwords.

Many agencies:

- Struggle to inventory or govern who has access to what resources;
- Have too many “over-privileged” users – individuals who have been granted access to more resources than is appropriate for their job;
- Do not have a means to easily authorize individuals to access the right applications or revoke that access when it is no longer needed; and
- Struggle to govern “orphan” accounts that might have been left open long after a person has left the organization or moved on to another role.

No two breaches revealed these flaws more clearly than the cases of Bradley (Chelsea) Manning and Edward Snowden. Both Manning, an Army intelligence analyst, and Snowden, a NSA contractor, were legitimately-credentialed users. Neither breach resulted from insufficient authentication, but rather from a failure to properly govern authorization – what these users could do with legitimate credentials. Manning and Snowden are just two examples that illustrate the need for agencies to embrace a comprehensive approach to identity governance.

Now is the time for agencies to build on the momentum of the “Cybersecurity Sprint” and focus on a complete Identity and Access Management (IAM) strategy rooted in governance that can protect against the full range of identity-centered attacks.

This white paper will address the specific challenges associated with protecting Federal IT systems from identity-centric attacks and detail how agencies can lock down their identity security through a comprehensive strategy rooted in identity governance.

IDENTITY AND CYBER THREATS: MULTIPLE ATTACK VECTORS REQUIRE A MULTI-PRONGED APPROACH

In 2015, a record number of high-profile government leaks and data breaches resulted in the loss of tens of millions of personnel records and personally identifiable information. According to Verizon's 2015 Data Breach Investigations Report, 2,122 security incidents resulted in confirmed data loss. High-profile breaches of OPM and the Internal Revenue Service (IRS) commanded the attention of the nation and key decision makers in Washington, D.C. Attacks over the last few years on private-sector corporations, including Anthem, Premera, Target, Home Depot, and Experian/T-Mobile, drew similar attention from business and government. Though each breach occurred at the hand of a unique attacker with specific motives, they each shared a crucial commonality: attackers gained entry using compromised or stolen credentials.

While stolen credentials have always been a problem, the intensity of the problem increased in the past year as adversaries shied away from launching attacks on perimeter defenses or through malware in favor of using credentials to "walk through the front door." A September 2015 report from Dell SecureWorks discussed this trend, noting that in nearly all of the intrusions its incident response team responded to in the past year, "cyber criminals utilized the target's own system credentials and legitimate software administration tools to move freely throughout the company's networks infecting and collecting valuable data...these hackers don't employ malware in their operation."

Use of PIV card strong authentication is a critical first step towards preventing these kinds of attacks. However, many agencies, even those using PIV cards, have thousands of employees whose accounts give them access to far more data and resources than they need, and often, this access is poorly governed. Some agencies also struggle to create a comprehensive inventory of who has access to what resources and ways to authorize individuals to access the right applications, revoke improper access privileges, and check for ghost accounts that might have been kept open long after employees left the organization or shifted roles internally.

The range of identity-centric attacks reveals a number of challenges associated with protecting Federal networks:

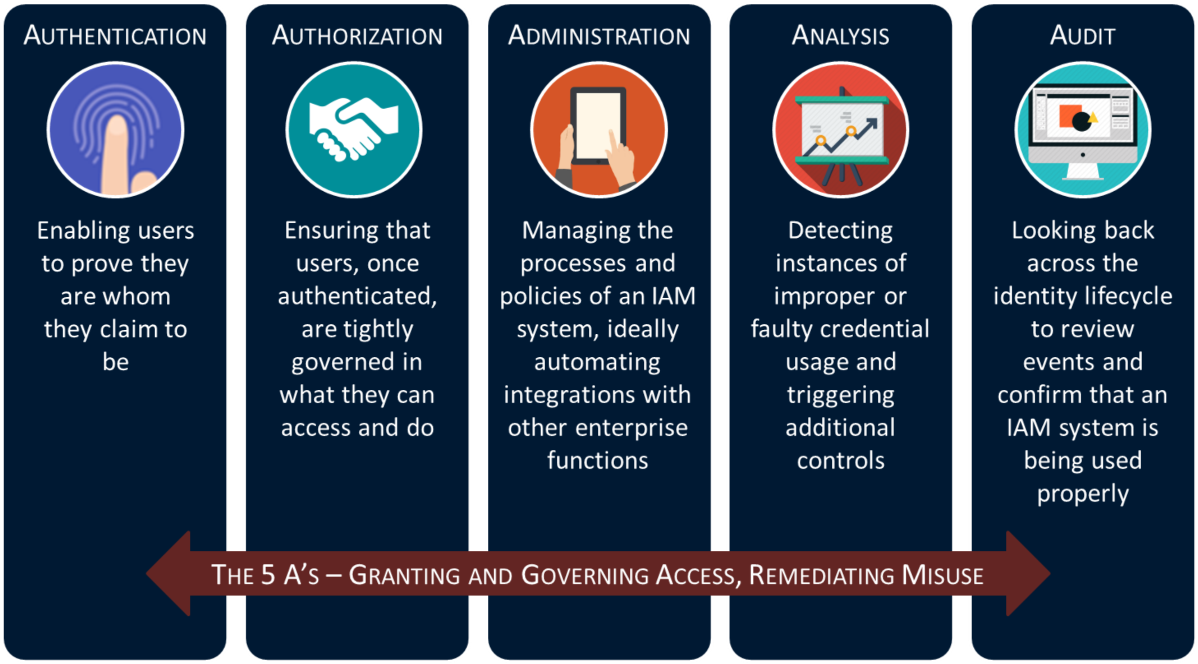
- Advanced attackers with evolving tactics, techniques, and procedures (TTPs);
- A complex, heterogeneous, and distributed network environment with an increasingly porous perimeter;
- Ineffective traditional perimeter-focused cybersecurity technologies that lack the ability to identify or prevent improper authorization and access;
- Large, transient contractor workforce with limited information sharing between or within agencies;
- Excess of privileged users with limited visibility into their actions;
- Manual operational and administrative onboarding procedures; lack of automation and monitoring capabilities; and
- Incomplete identity and access strategies for employees, administrators, and contractors that have made securing government resources more difficult.

By taking a holistic approach to identity – considering authentication, authorization, administration, analysis, and audit - agencies can close many of their most easily exploited holes and significantly improve their cybersecurity postures.

THE FIVE A's: ELEMENTS OF A COMPLETE IAM STRATEGY

To truly address the full range of risks to Federal systems tied to identity, agencies should take a holistic approach to identity security — one rooted in governance.

Governance-based approaches go beyond authentication, instead addressing the full lifecycle of identity and access management. The Chertoff Group views the IAM lifecycle through the prism of "The Five As" – which, when tackled together, cover the full range of identity risks:



AUTHENTICATION

Enabling users to prove they are whom they claim to be

AUTHORIZATION

Ensuring that users, once authenticated, are tightly governed in what they can access and do

ADMINISTRATION

Managing the processes and policies of an IAM system, ideally automating integrations with other enterprise functions

ANALYSIS

Detecting instances of improper or faulty credential usage and triggering additional controls

AUDIT

Looking back across the identity lifecycle to review events and confirm that an IAM system is being used properly

THE 5 A'S – GRANTING AND GOVERNING ACCESS, REMEDIATING MISUSE

Properly implemented, this governance-based approach enables agencies to answer a number of critical questions around identity security, including:

- How is a credential provisioned?
- How are users authorized to access data or resources?
- How are those authorizations managed and updated as roles or attributes change?
- How is access to privileged systems provisioned and managed?
- Are Privileged Account Management (PAM) solutions tightly integrated with the rest of the IAM stack?
- Are firm controls in place to prevent the creation of new "phantom" accounts?
- How is access revoked when someone leaves an organization, ensuring that "orphan" accounts do not persist?
- With a blended workforce of employees and contractors – including some that may not have a PIV card – how are access and privilege consistently managed through a unified approach?

The strongest identity governance solutions are capable of assigning a risk profile for both employees and contractors, and automatically flagging privilege escalation requests to deter inadvertent or intentional access to restricted networks without proper authorization. A strong identity governance solution will also generate risk scores for all users based on their combined entitlements and historical performance.

WHERE FEDERAL AGENCIES SHOULD FOCUS

In most agencies, users' – or identities' – access to enterprise systems is tiered, encompassing the basic question of authentication and the more complex question of authorization – the first two areas of the IAM lifecycle. Considering the number of identities an enterprise may have across its employees, partners, and contractors as well as the multi-dimensional systems utilized, and the varying levels of access required, it is easy to see how an enterprise might have hundreds of thousands of access points into its systems. Every layer of access rights associated with an identity is a point of exposure for the organization.

Out of those hundreds of thousands of identity exposure points, it takes only one to be compromised. At a time when adversaries are increasingly targeting identities relative to other attack vectors, agencies need to increase their focus on identity security. Though the 2015 30-Day "Cybersecurity Sprint" jump-started many of the necessary changes needed to secure Federal networks, many government leaders have recognized the need for a more comprehensive identity and governance strategy that covers the entire organization, from contractor to administrator, providing controls and governance for the full lifecycle of the identity and the accounts and access it is afforded.

The Role of CDM

The Continuous Diagnostic and Mitigation (CDM) program run by the US Department of Homeland Security (DHS) will play an important role in the government's progress towards implementing a comprehensive identity governance solution complete with data governance and privilege management capabilities.

Phase II of the CDM program is heavily focused on raising the baseline IAM capabilities of all Federal agencies in order to continuously identify networked devices and systems, monitor users' statuses, and mitigate identified risk. Phase II requirements include:

1. **Trust** – Manage trust for those granted access
2. **Behave** – Manage security-related behavior
3. **Cred** – Manage credentials and authentication
4. **Priv** – Manage account access – manage privilege

The first requirement, **Trust**, serves to ensure that only properly-vetted users be provided credentials and granted access to facilities, systems, information, and privileged accounts. As employees and contractors move within an agency, they accrue access to different systems necessary to perform different roles. However, this access leads to entitlement creep, when employees have access to more systems than they need at a given time, and consequentially increasing the risk of a negligent or malicious insider attack and data loss. The first step towards achieving Trust is to implement a certification process for identifying who has access to what.

The second requirement, **Behave**, ensures that authorized users meet the security-related requirements for facilities, systems, information, and privileged accounts to prevent insider attacks. Agencies and organizations often find it difficult to holistically view a user's access across disparate systems. Visibility into all critical access-related activities can prevent behavior that could lead to insider attacks and data breaches. For example, security managers can identify a string of seemingly innocuous access requests as higher risk based on the nature or level of the user's job function.

Cred identifies if and when agency authentication, reissuance, and revocation policies are incurring more risk than acceptable. This management ensures that authorized users can be authenticated appropriately for access to facilities, systems, and information. Employee password management can be complicated, confusing, and insecure for an agency with many disparate systems. Outdated, common passwords can be used to grant legitimate access to malicious users. Agencies should seek one solution that can sync credentials across applications according to government policy. This capability also helps reduce account lockouts and password resets. Automated provisioning, discussed in further detail below, is key to securing and automatically altering privileges throughout employee lifecycles.

Priv ensures that privileges for both physical and logical access are assigned only to authorized people or accounts that require that access to perform authorized job responsibilities. Similar to entitlement creep, granting too much access to users at the administrator and/or system level unnecessarily increases risk to an agency. Enforcing a least-privilege model, in which employees have the minimum amount of access to applications and information necessary to perform their job function, curtails this issue. Governance solutions can define and enforce a least-privileged model that limits risk to agencies.

The CDM program will deliver some important building blocks to Federal agencies to help improve identity governance. These building blocks, however, will not in and of themselves cover the full gamut of the "Five A's" of the IAM lifecycle. Components will need to be integrated and additional functionality will be needed to deliver a full lifecycle approach to IAM that is rooted in strong identity governance.

Toward a Full-Lifecycle, Governance-Based IAM Approach

In order to adopt a governance-based approach, Federal agencies need to focus on the provisioning lifecycle, detailed management of privileged accounts and users, and inventorying and managing access to unstructured data. A comprehensive identity governance solution helps secure the overall systems access lifecycle by addressing all three of these functions.

Provisioning Lifecycle

Defining and managing a controlled provisioning lifecycle falls primarily into the domain of the "Third A," of the IAM lifecycle, Administration, but has far-reaching implications for the other four domains, as well. The basic act of provisioning for both manual and automated systems is fundamentally the process of administering systems of authentication and authorization. Fine-grained administration is the basic process of defining and managing who has access to what. Agencies should look to extend provisioning control models to all systems that provide access. Recent breaches have shown that the exploitation of internal accounts for “lateral movement” is a key attack vector. Managing the full lifecycle of all accounts is now critical to security.

A significant obstacle in current Federal identity strategy is overreliance on manual provisioning. Many legacy provisioning solutions were adopted in the early years of identity management, upwards of two decades ago, and are inadequate to address today’s requirements. The number of users, devices, and databases has grown such that legacy systems are no longer capable of managing the security and compliance demands of a modern government agency.

Successful provisioning solutions use automation to streamline and secure Federal agency identities. As users join, move within, or leave an agency, automation reduces the burden of manually provisioning those users, and provides the ability to embed preventive policy controls that help implement functions like separation-of-duty. This automation capability is particularly useful in the management of contractor credentials, as contractors’ transience within the Federal government can make their credentials particularly difficult to monitor. A provisioning solution that responds automatically with access to the appropriate resources when an employee or contractor joins a Federal agency is much more effective for policy compliance and business productivity. When a user leaves an agency or a contractor’s period of work ends, those same automated processes can be used to de-provision the user immediately, helping to ensure the security of sensitive information by eliminating phantom accounts. Without lifecycle automation and embedded policy controls, an agency may be blind to the types of ongoing lifecycle changes that directly lead to abuse of privilege and privileged account escalation attacks.

Managing Privileged Users

Managing privileged users touches several of the five domains of IAM previously outlined. Based on the level of privilege afforded a given user or account, changes need to be made to the authentication, authorization, and audit processes. It is now a recognized best practice to change the way enterprises and agencies manage and monitor systems access based on the level of privilege that access affords. By taking a holistic approach to governing all five IAM domains, agencies can help create an umbrella of controls that can prevent, detect, and better manage privileged accounts and personnel.

The Federal government recognized the importance of privileged access management (PAM) in the wake of the OPM breach. Given that malicious actors were able to elevate their privileges from contractor to system administrator over the course of the breach, there has been a renewed focus on the need to identify and secure privileged accounts. Indeed, the Cybersecurity Strategy and Implementation Plan (CSIP), published by the Office of Management and Budget (OMB) on October 30, 2015 requires that Federal agencies use Personal Identity Verification (PIV) credentials for authenticating privileged users.

The National Institute of Standards and Technology (NIST) published draft guidance on Privileged PIV User Authentication in February 2016, which contains important best practices for agencies to secure privileged accounts. A core issue of today's identity governance is not how privileged users are authenticated, but rather the way that privileged accounts are created, enabled, modified, disabled, and removed, as well as the specific privileges given to each account.

In practice, many privileged accounts are created outside an organization's core IAM processes. Amidst a rush to install PAM solutions, organizations often do not integrate them with the systems that provision and govern identity accounts – creating potentially serious gaps in the visibility and control of the overall identity security model. Agencies should realize that PAM solutions themselves are now a significant attack vector. PAM infrastructure should be tracked, monitored, audited, and controlled with an increased focus on state change and authorization. All systems of centralization inevitably become a focus for attack and therefore require an increased level of diligence and control over the provisioning and verification of these systems.

Agencies should ensure that their identity governance solution is tightly integrated with PAM solutions. By configuring these systems to ensure all access and privilege escalation requests originate within the identity governance solution, agencies not only ensure the integrity of the broader solution, but also enable the creation of more granular access permissions for privileged accounts. Moreover, this integration grants administrators total visibility into all accounts, both regular and privileged.

Unstructured Data

Unstructured data refers to items such as files and shared data content that are authorized via a model that permits indirect access, such as a document on a file share that is protected by an Active Directory group authorization model. Managing these access models is complex and inevitably touches all five of the IAM domains. The authorization, administration, analysis, and audit of these models are complex tasks.

The growing volume of data generated in organizations is presenting many agencies with a new challenge: how to inventory and classify this data, as well as manage who is authorized to access it. With a majority of all data falling into the "unstructured" category, it is important to discover what data exists, who can access it and how, and apply appropriate policies to protect it. Authorization is a key component of data governance, and a complete identity strategy must include controls and visibility into access.

By augmenting IAM data from structured systems with permission data from unstructured data targets, agencies can identify risks, resolve compliance issues, and strengthen access controls. Data governance solutions offer the following benefits for Federal agencies:

- Provide centralized visibility across structured and unstructured data in the agency – all applications, all data, and all users;
- Add unstructured data targets to preventive and detective controls, such as access certifications and separation-of-duty policy enforcement;
- Automate provisioning of access to unstructured data repositories and revocation of inappropriate access; and

- Inform the IAM system with real-time activity data to improve risk mitigation and understand appropriate use.

By embracing identity governance, which integrates all facets of an IAM system together – including provisioning, privileged users, and data governance – into the IAM platform, Federal IT leaders can address the full range of identity risks in their ecosystem.

CONCLUSION

Multi-factor authentication is an essential first step in securing identities. A complete identity strategy, however, includes an additional four elements beyond authentication: authorization, administration, analysis, and audit.

Together, the “Five A’s” of a complete IAM strategy secure identities through appropriate governance of employees, contractors, and system administrators from onboarding to off boarding, determining access and privilege escalations along the way in order to mitigate the risk of stolen credentials or malicious insiders. Governance-based approaches go beyond authentication to address the full lifecycle of identity and access management, managing the provisioning lifecycle, privileged accounts, and unstructured data.

Federal agencies should leverage the “Five A’s” to build on the good progress made on strong authentication during the “Cybersecurity Sprint” and ensuing CSIP, embracing a holistic approach to identity security.

ABOUT THE CHERTOFF GROUP

The Chertoff Group is a premier global advisory firm focused on security and risk management. Founded in 2009, The Chertoff Group helps clients grow and secure their enterprise through business strategy, mergers and acquisitions, and risk management security services.

With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantages. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations.

Headquartered in Washington D.C., The Chertoff Group maintains offices in Houston, London, Menlo Park, and New York City. For more information about The Chertoff Group, visit www.chertoffgroup.com.

ABOUT SAILPOINT

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of global organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information, visit www.sailpoint.com.