SEPTEMBER 2016

STOPPING THE INSIDER THREAT

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

CONTENT:

INTRODUCTION

“Insider threat” is no longer just a security buzzword; it has become an enterprise concern commanding executive-level attention.

In government, devastating data disclosures by the likes of Edward Snowden and Chelsea (Bradley) Manning have brought attention to the reality that malicious actions by trusted employees within an organization can undermine that organization’s security and jeopardize national security. Insider attacks at private sector entities including Morgan Stanley, Monsanto, and Reuters have had consequences impacting those organizations’ customers, employees, operations, reputation, and bottom line.

At its core, insider threat is an Identity and Access Management (IAM) issue: malicious insiders, by definition, have been granted some level of authorized access and are therefore often harder to detect than bright-line cases of unauthorized access or intrusion. As addressed in this paper, many organizations’ vulnerability to insider attack stems from gaps in their IAM approach. These gaps can be mitigated by embracing a complete Identity and Access Management (IAM) strategy, rooted in governance, which can protect against the full range of insider attacks.

THREAT OVERVIEW

Disgruntled, malicious employees can have a variety of motivations for abusing access to steal and disclose data, including terrorism, retribution, thrill factor, personal gain, and intellectual property theft. But data theft or disclosure by malicious insiders does not reflect the full scope of the insider threat. A recent survey of IT professionals by Kaspersky Lab determined that 29 percent of all businesses interviewed reported accidental disclosures by insiders as their single largest source of lost data—bigger than either software vulnerabilities or outright theft. The sum of accidental disclosures and malicious cases of insider misuse captures the insider threat more fully. In 2015 alone, the Verizon Data Breach Investigations Report (DBIR) tallied 10,489 total incidents of insider misuse, whether malicious or accidental.

The number of annual incidents attributed to insiders is on the rise, and individual incidents are commanding more attention as their consequences become more damaging. The U.S. Government's focus on insider threat stems not only from the massive data breach perpetrated by Edward Snowden, but also from the fact that Snowden's disclosures came to light just three years after the Manning-WikiLeaks breach. Response measures have come from a number of agencies and leading officials, including the White House. President Obama released the Cybersecurity Strategy and Implementation Plan (CSIP) and later the Cybersecurity National Action Plan (CNAP), which placed heavy emphasis on securing employee and contractor accounts at federal agencies to protect against data loss in the wake of the OPM breach, which occurred after attackers stole the password of a contractor. Additionally, Director of National Intelligence James Clapper placed counterintelligence operations among his annual list of global threats to U.S. interests and the Department of Homeland Security expanded programs to monitor employee access levels through the Continuous Diagnostics and Mitigation (CDM) program. In May 2016, the Department of Defense published a change to the National Industrial Security Operating Manual (NISPOM) requiring any industrial, educational, commercial, or other entity with a facility security clearance (FCL) to establish and maintain an insider threat program to detect, deter, and mitigate insider threats.

Similar breaches have precipitated modest action in the private sector. A malicious insider at U.S. private wealth management firm Morgan Stanley stole the records of over 350,000 people, or 10% of Morgan Stanley's total client portfolio, and released over 900 of them online before discovery. In September 2013, Vodafone Germany reported that an attacker with insider knowledge had stolen the personal data of two million customers from a German server. Stolen data included customer names, addresses, genders, birth dates, bank account numbers, and bank routing numbers. According to *Security Week*, the company said in a statement that "This criminal attack appears to have been executed by an individual working inside Vodafone." Similarly, in March 2014, data including the bank account details of roughly 100,000 employees of British supermarket chain Morrison were published online by an inside hacker. In a fourth incident, a U.S. Monsanto employee is accused in an ongoing investigation of stealing data for use at a Chinese-based agriculture company. This particular attack reflects the national and industrial espionage implications of insider threats. In response to events of this type, private companies have begun taking initiative to mitigate insider threat. Though even the most advanced companies have struggled with the depth of the insider threat problem, most companies are starting to understand that if a threat is coming from the inside, an approach rooted in traditional perimeter defenses is insufficient.

STOPPING THE INSIDER THREAT: WHAT CAN BE DONE?

Although federal agencies and private companies are becoming increasingly aware of the depth of the threat posed by insiders, mitigation measures implemented in both sectors are immature. If traditional network defenses are insufficient to eliminate the threat posed by legitimately-credentialed insiders, what can be done? The first step towards addressing insider threat is recognizing that it cannot be fully eliminated, only mitigated. That said, a mature approach that integrates both people-centric and technology-centric approaches can help organizations mitigate the risk of insider attacks.

People-Centric Strategies

A people-centric approach to insider threat mitigation must start with the buy in of corporate leadership. Insider threat programs must have support, funding, and oversight from corporate leadership to ensure a culture of security and best practices to avoid data loss. The Chertoff Group typically recommends establishing an executive steering committee and an insider risk working group with representatives from human resources, legal, security, and other relevant departments to guide the insider threat program. This program should include a corporate communications plan to enable top-down messaging on core principles associated with an insider threat program, including safety, privacy, security, and IP protection.

Both people-centric and technology-centric approaches to insider threat should be understood and implemented across an employee’s time and service with an organization, which comprises hiring and onboarding, employment, and departure. This lifecycle framework can be used to assess the current level of protection provided by an organization’s overall security posture and to identify vulnerabilities in that system.

On the people-centric side, during the hiring and onboarding process, before employees are credentialed and given access to company networks using identity technologies, both enterprises and agencies should formalize thorough background investigations to identify and evaluate financial history, past misconduct, risky or criminal behavior, and relationships with potential bad actors. Though federal agencies already conduct background checks under HSPD-12, the private sector has yet to include them in onboarding procedures. Pre-employment screening of this sort is designed to identify employee risk levels before granting access to sensitive information.

Background checks are not infallible, however, and must be supplemented with ongoing mitigation measures throughout the course of employment. Enterprise-wide training and education programs should be offered at regular intervals and tailored to various roles within an organization including senior management, security staff, and general employees. Annual refresher training should be mandated, and reporting of suspicious behavior for investigation encouraged. Training courses can be particularly effective at inhibiting insider negligence by identifying best practices and encouraging vigilance and enhanced cyber hygiene. These measures create a culture of security without imposing significant costs on the organization.

Once employees are issued credentials, insider threat mitigation becomes an issue of risk management—accepting a certain degree of risk by granting employees access to confidential information, but limiting that access such that employees have access to only the materials they need to perform their professional obligations. Though this access is best governed by IAM solutions described in greater detail below, it is important to maintain a rigorous, continuous monitoring process on the people-side to ensure both physical and cybersecurity hygiene. This monitoring is particularly important for system administrators, who control the access of other employees and hold the “keys to the kingdom.” Additionally, organizations must also monitor employees who get transferred or promoted within an organization, known as “movers,” in order to ensure they have the appropriate access to align with their current and new roles.

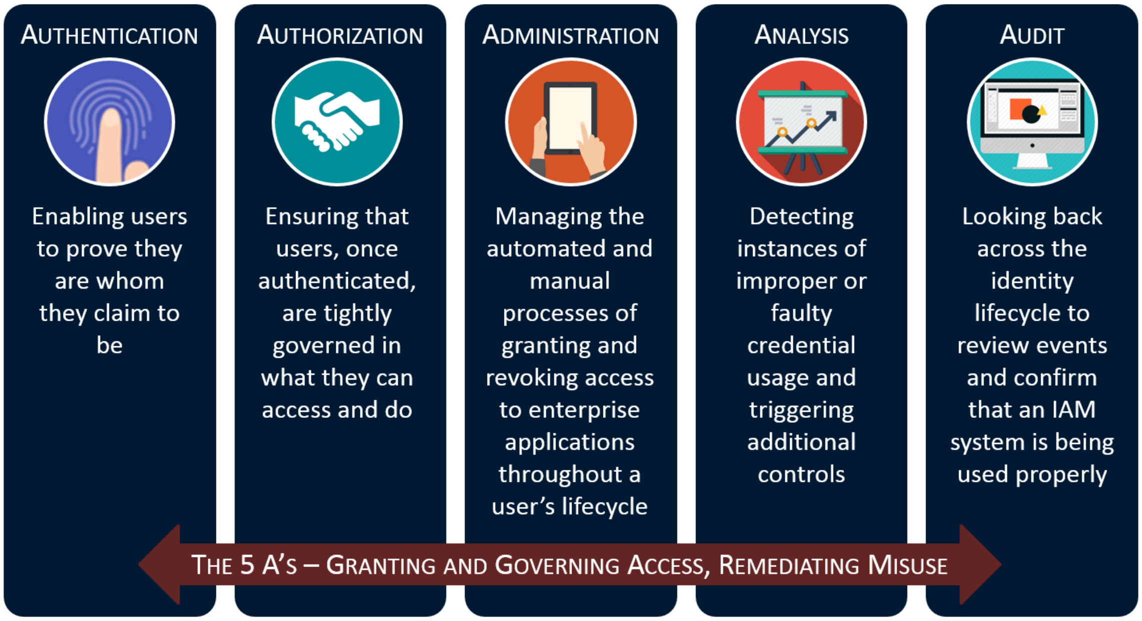
The final phase of the employee lifecycle is departure. When employees leave an organization, whether by choice or not, their access must be disabled. A proper IAM solution can handle the monitoring, logging, and de-provisioning of exiting employee accounts and credentials. This solution should be complemented by people-centric strategies including exit interviews to reaffirm existing agreements regarding IP and non-disclosure, as well as proper collection of organization-owned equipment to ensure a more complete offboarding process.

While effective to an extent in their own right, people-centric mitigation strategies must be supplemented and enhanced with comprehensive technology solutions.

Technology-Centric Strategies

As demonstrated by the Snowden and Manning disclosures, people-centric approaches such as background checks and rigorous security training—though effective at thwarting some disclosures—are not themselves sufficient to prevent determined threat actors from executing an attack. Enterprises and agencies should utilize identity technology solutions, rooted in governance, to fully guard against insider threats.

While strong, multi-factor authentication is an essential first step to defending against external actors attempting to steal credentials and gain access to a network, using it as the only aspect of an identity security strategy is wholly insufficient to defend against malicious insiders, who are already credentialed to act within a network. Governance-based IAM approaches go beyond authentication, 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 associated with insider threat.



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 automated and manual processes of granting and revoking access to enterprise applications throughout a user’s lifecycle

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 and organizations to answer a number of critical questions regarding insider threat, including:

- Who within an organization has access to the most sensitive proprietary information?
- 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 strong 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, how are access and privilege consistently managed through a unified approach?
- Do you know who has access to what enterprise applications and data repositories?

The strongest identity governance solutions are capable of assigning risk profiles 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.

EXECUTING A FULL-LIFECYCLE, GOVERNANCE-BASED IAM APPROACH

In order to adopt a governance-based approach, enterprises and 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 - Administration" of the IAM lifecycle, but has far-reaching implications for the other four domains, as well. The basic act of provisioning for both manual and automated systems is 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 and enterprises should look to extend provisioning control models to all systems that provide access. Recent external breaches have shown that the exploitation of internal accounts for "lateral movement" is a key attack vector. Additionally, in a number of recent insider cases, malicious former employees have utilized their old accounts to siphon sensitive data once they have left the company. Managing the full lifecycle of all accounts is 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 identities. As users join, move within, or leave an organization, 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 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 or enterprise is much more effective for policy compliance and business productivity. When a user leaves an agency or enterprise 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 or enterprise 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 and enterprises can help create an umbrella of controls that can prevent, detect, and better manage privileged accounts and personnel.

The U.S. 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 and private enterprises 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 and enterprises should ensure that their identity governance solution is tightly integrated with PAM solutions. By configuring these systems to ensure that all access and privilege escalation requests originate within the identity governance solution, agencies and companies 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 is presenting many organizations 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. Most of the data that Edward Snowden stole were loose files from a SharePoint site. 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, organizations can identify risks, resolve compliance issues, and strengthen access controls. Data governance solutions offer the following benefits for federal agencies and private enterprises:

- Provide centralized visibility across structured and unstructured data in the organization – 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 and commercial IT leaders can address the full range of identity risks in their ecosystem.

CONCLUSION

Effective insider threat mitigation requires a strong IAM strategy rooted in governance. People-based controls and security processes are essential in building best practices and a culture of security within an organization. However, as people-centric strategies are not enough, agencies and enterprises must consider technology-centric strategies for a complete insider threat program. Organizations must deploy IAM solutions that address the "Five A's" – authentication, authorization, administration, analysis, and audit – to manage the full lifecycle of employees and contractors from onboarding to offboarding, determining access and privilege in order to mitigate the risk of malicious insiders.

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 advantage. 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.

© The Chertoff Group and SailPoint. All rights reserved.