Designing an identity and access management program optimized for your business

Four key steps that can move you toward a more mature solution now

Highlights:

Taking a deliberate approach to identity and access management helps ensure that business objectives related to security, productivity or compliance can be met, both in the short term and as the organization continues to evolve in the future.

Contents

Introduction

In today's complex and distributed IT environments, identity and access management (IAM) programs do much more than simply manage user identities and grant access. They are at the core of achieving critical business objectives that are relevant to every high-performing organization. As a result, there are few IT or security initiatives that demand as much deliberation and scrutiny.

A mature IAM program optimized to a business's objectives and the unique circumstances surrounding it can reduce the risk of data breaches involving identities. It can help enable productivity and collaboration, delivering a real competitive advantage in the market. And, it can help ensure that regulatory compliance management is more systematically achieved and maintained, while reducing the costs to the business of performing audits.

But many organizations fail to meet one or more of these objectives due to fragmented, stagnant and incomplete IAM programs that have been developed over time using point-technology solutions. As a result, businesses are exposed to the risk of major losses and miss the competitive advantage of an agile and connected workforce.

Taking a deliberate approach to maturing an existing IAM program can lead to benefits that directly improve business performance and security posture. This approach can reduce costs through automation, improve operational efficiency through an integrated technology framework and help support more successful implementations through proper planning.

60% of all attacks were carried out by insiders

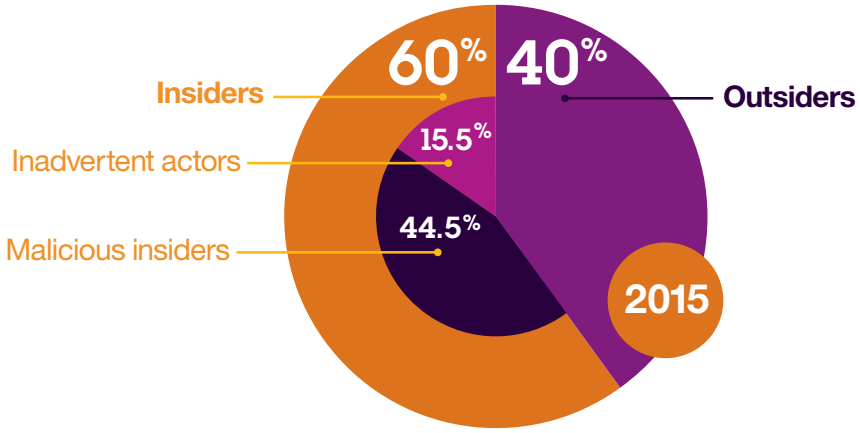

Figure 1: Who are the "bad guys"?

Going beyond "good guys versus bad guys"

Today's IAM solutions need to do more than just "let the good guys in and keep the bad guys out." That's because an increasing number of security breaches are the result of actions by insiders, whether malicious or inadvertent. When employees share passwords or lose corporate data—or third parties put information at risk with inadequate safeguards—even the "good guys" pose a security risk.

An IBM® X-Force® report found that insiders were responsible for 60 percent of attacks surveyed.[1] Of those, 15.5 percent were inadvertent actors. Often unwittingly "recruited" to aid the cause of others with malicious intent, they are becoming key players in carrying out highly damaging—and potentially prolonged—attacks. And because they're insiders, they manage to do so without arousing any suspicion, by logging onto a social media site from a corporate network-attached device or opening an email attachment sent by a legitimate-looking business contact.

Then there are the malicious insiders, making up the remaining 44.5 percent, whose actions are not at all innocent. The unsettling truth is that just because they're considered to be "insiders" doesn't mean they can be trusted. So it's important to remember that situations and relationships can change over time—and not always for the better.

1 IBM Cyber Security Intelligence Index 2016 http://www-03.ibm.com/security/data-breach/cyber-security-index.html

The pillars of a mature IAM program

An IAM program optimized to the needs and unique circumstances of an organization helps enhance regulatory compliance management capabilities, grant convenient access to authorized users and protect valuable data. Every organization will have different requirements in terms of technology maturity, and will have IAM programs in different conditions.

However, successful IAM programs all share a common factor: they contain identity assurance, identity intelligence, and governance, working in an integrated fashion, consistently across an organization's IT landscape. As a result, organizations are able to achieve the appropriate levels of access controls and security without hurting productivity or constraining users to painful login experiences.

Enhancing identity assurance in a multi-perimeter world

Many organizations still rely on simple passwords as proof of identity. But passwords are static and inherently weak. Most users take the path of least resistance, using easy-to-remember passwords that can easily be stolen, cracked and compromised, exposing a system to fraudulent attacks. Once an attacker deciphers a static password, it becomes easy to impersonate the original user and gain access to many types of confidential data. Because many users benefit from single sign on or reuse the same password across many enterprise systems, data stored in applications far removed from the initial breach can also be compromised. And if that's not concerning enough, it's important to note that static passwords are also vulnerable to a wide variety of phishing and Trojan attacks.

To help prevent fraudulent access, users must be able to prove their identities within the context in which they're accessing corporate resources. That context could encompass the type of device they're using, their location or their patterns of activity. The latest security technologies can use this context information to determine whether a specific user is authorized for access.

Using contextual data analytics to analyze risk, organizations can grant access based on a dynamic assessment of both the transaction and the user in question. For example, if a North American worker suddenly uses her mobile device from Africa, the software notes an unusual change in context and may require the user to provide additional proof of identity, such as a one-time password. In some situations, the user may be denied access to certain IT resources because the security risk is deemed to be too high.

By requiring more than one form of authentication, organizations can help ensure that both the right user is granted access to protected resources, and that those resources are in fact protected from those who shouldn't be able to access them. In addition to increasing the security of an access request, leveraging its context also makes the experience smoother for the end user, increasing their productivity. In low-risk attempts, the user experience can be frictionless.

Enhancing end users' identity assurance can be done by combining a wide variety of authentication methods, from biometrics, to mobile-optimized push notification, to hard tokens, with a sophisticated policy engine, or, ideally, a risk engine. A policy engine enables administrators to set specific rules for each access request, and goes a long way toward achieving good identity assurance. A risk engine goes one step further –when a user requests access to a protected resource, the system calculates a risk score and determines whether access may be permitted, denied or permitted after a condition is met.

Integrating identity intelligence into the process

As security threats become more sophisticated and the pressures of risk and compliance continue to grow, so too does the demand for a new, proactive approach to identity management that weaves risk control into its very fabric. Today's most effective identity management solutions combine entitlement management with privilege control and "identity context aware" security intelligence.

Integration with privileged identity management

A privileged ID refers to any account that includes special or extra permissions for enterprise resources, such as servers, network appliances, database systems and enterprise resource planning applications. Of course the threat of attackers compromising a privileged ID poses an obvious risk. But the risks don't end there. An organization's authorized users with privileged accounts can also represent danger to the security of its IT infrastructure. At the same time, organizations are increasingly delegating specific administrative tasks to staff and contractors, opening the door to further risks associated with privileged accounts.

An organization's authorized users with privileged accounts can also represent danger to the security of its IT infrastructure.

That's why it's so important for organizations to:

- Prioritize the need for privileged identities
- Identify and monitor their highest risk users
- Know who has access to sensitive data and systems
- Develop baselines for normal behavior.

The most practical way to meet those requirements is with a sophisticated identity management system for allowing IT staff to share privileged IDs. It's critical that such a system includes the following:

- A credential vault to securely store the credentials to privileged IDs
- A check-out check-in mechanism that lets a privileged user check out an ID (with a password) for exclusive use and a limited time period, whenever necessary; and then check in the ID when finished, at which point the password changes automatically
- A means for centrally provisioning and managing IDs on various resources
- Roles and policies for dictating which users have access to which IDs
- A process for users to request access to IDs and for managers to approve the requests
- Integrated audit logs that feed into a security intelligence solution to record all check-out check-in activities and show which users had access to which IDs over a specific time period.

It's a solution that allows organizations to:

- Avoid the proliferation of privileged IDs linked to its resources
- Allow privileged users to access a privileged ID if, when and on the condition they need it—for only as long as they need it
- Make privileged users accountable for the IDs that they've owned or checked out
- Delegate management of IDs and access policies to the respective resource owners
- Collect identity attributes and use that data in conjunction with log events and network flow data rules to provide "identity context aware' security intelligence.

Integration with identity intelligence

Several security intelligence solutions—including security information and event management systems—can provide usable log files and metrics that help identify anomalies, highlight risky or inappropriate behavior and assist in compliance reporting. By integrating identity and access management with these solutions, organizations can combine that output with log events and network flow data to develop "identity context aware" security intelligence. With an expanded view of activities across different security domains throughout the enterprise—and by correlating identity and access management data with other important security events—organizations can more quickly uncover inappropriate or suspicious user behavior (including insider threats) and significantly decrease threat response times.

Addressing compliance mandates with identity and access governance

Virtually every industry faces compliance mandates at some level. Countless government regulations around the world stress the importance of visibility and control for individuals' entitlements and access privileges.

Thanks to escalating security and privacy concerns—along with a renewed focus on corporate oversight and governance— risk management and compliance measures are now being driven to the business forefront. As a result, organizations must prove that they have strong and consistent access controls to meet both their own compliance requirements and those of their business partners.

It's far more likely that security breaches and compliance issues will occur when users have outdated or inappropriate levels of access, driving up the potential for insider threat activity. Outside attackers often look for the "easy prey" that poorly controlled and managed user access programs offer. It's simply not enough to develop a solid identity and access management program. You also need to keep it functioning properly.

Case study: A global leader in customer management streamlines and improves its identity and access management program

Recent merger and acquisition activity—compounded by disruptions from organizational changes—highlighted this company's need for a more robust, agile and consistently implemented identity and access management solution.

IBM assessed their business priorities, identified their identity and access management-related strengths and weaknesses, and evaluated them against industry standards and best practices to develop a clear business-driven strategic roadmap for improving the company's identity and access management capabilities.

With the help of IBM Identity and Access Management Services, the organization consolidated its administrative identity and access management silos into a common framework designed to reduce costs and complexity through the use of common, reusable standards-based components, technologies and services. And as a result, the company was better positioned to avoid and mitigate compliance risks.

Reducing risks through governance

Identity and access governance provides guidelines on how user roles are defined and access is provisioned, managed and enforced throughout the lifecycles of users.

Solutions designed for managing user access requirements with greater accountability and transparency helps you govern and enforce user access more effectively. These tools can help administrators ensure that user accounts and privileges are updated and appropriate to their roles. In addition, identity and access governance can help organizations implement more thorough and consistently enforced control over who can do what with which resources.

A policy-driven approach for an identity and access governance program should include:

- Planning for an identity and access governance strategy
- Defining standards, processes, and controls for identity and access governance
- Enabling the implementation of identity and access governance
- Monitoring, measuring, and reporting on the effectiveness of the identity and access governance program.

When the system breaks down

Most enterprises have a long history of legacy IAM investments, followed by pointed efforts to modernize with varying degrees of success. While these substantial implementations are a great foundation and often times have elements of the pillars described above, over time they generally fail to keep up with organizations' evolving IT landscape. As a result, they are no longer able to protect against insider threat or identity fraud, they fail to enable the lines of business or they struggle to achieve compliance.

Several factors contribute to this phenomenon. The adoption of cloud applications by various business functions is often done in silos, with access managed in parallel (and sometimes even without IT's knowledge). As a result, they aren't automatically included in a central policy management system. As organizations become more and more complex due to mergers and acquisitions (M&As), reorganizations or simply organic growth, the scale of these problems expands rapidly. To compound these issues, users are becoming varied sets of individuals with very different access needs. The end-user groups managed by an IAM program can include employees, partners, contractors and even customers—sometimes bringing along their own devices or even identities through social media accounts.

Most companies attempt to keep up with these changes using point solutions as a logical response to each rising need and challenge. But over time, the end result is a fragmented IAM system that no longer meets objectives. By contrast, taking the time to deliberately design an IAM program optimized for specific goals has many benefits.

A deliberate journey to maturity

Taking a deliberate approach to identity and access management helps ensure that business objectives related to security, productivity or compliance can be met, both in the short term and as the organization continues to evolve in the future. Organizations can watch their IAM investments grow from providing them the bare minimum function to creating real value for their users as well as their bottom line.

A deliberate approach also allows organization to prioritize their roadmaps to address their most pressing issues. In the long term, costs can be reduced by breaking teams out of reactive spending cycles.

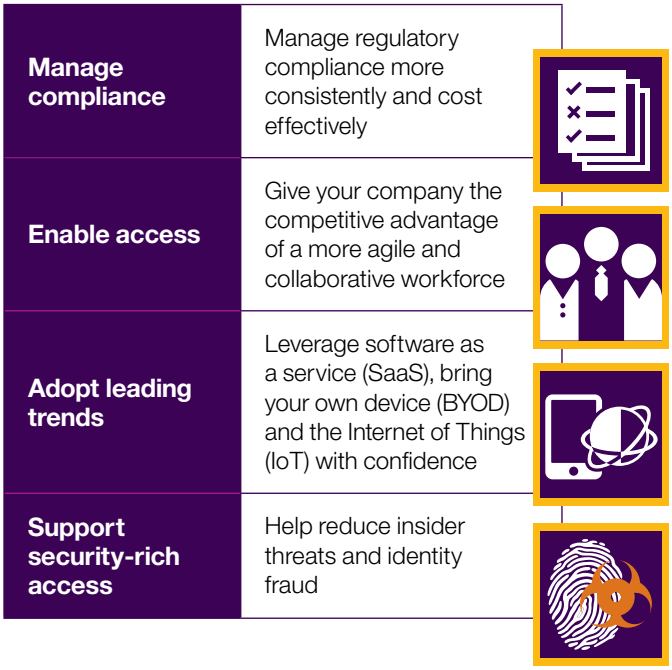

Figure 2: An IAM program tailored to your organization supports your business objectives

Figure 3: The benefits of taking a deliberate approach to identity and access management

Additionally, this method can help organizations avoid the costly mistake of jumping to vendor selection prematurely. IAM projects involve a fair amount of business reengineering. Focusing on technology selection too early distracts from core activities that align IAM solutions closely to business goals.

A deliberate approach includes three steps. The first is to **evaluate** the health of the current program, assessing key IAM gaps along with their impact on the organization and its ability to reach its business and IT goals. The second step is to **design** an executable IAM strategy to support long-term business needs, and a prioritized IAM roadmap, timeline and budget requirements to execute on that strategy within the context of the business. Once this strategic work is concluded, it can be used as a solid foundation upon which to complete the third step: **executing** on the plan to bring together the products, processes, and people necessary to bring the strategy to life.

Step 1: Evaluate

Starting with an evaluation of a current IAM program has many benefits. First, it allows organizations to perform a health check, truly identifying most pressing vulnerabilities and pain points, rather than simply the issues getting the most attention. While most organizations stop there, taking this approach means going one step further: these vulnerabilities are not taken by themselves, but rather within the context of the greater business goals—generally, some balance of security, compliance and productivity requirements. This focuses efforts and prioritization on the most important pain points while helping to ensure solutions that will work toward meeting business goals get deployed, in addition to solving current, pressing challenges.

Additionally, taking the time to develop a vision for the future can move an organization from a reactionary stance to a more strategic position, ensuring a system that does more than simply avoid issues. Instead of playing catch up and scrambling to patch up the IAM program anytime a pain point becomes impossible to avoid, it becomes possible to better anticipate future challenges and remain in control.

Oftentimes, a side benefit of this exercise is the ability to clearly articulate the connection between the budget allocated to an IAM program and a clear return on the investment in the form of the business objectives that will be met. An increase in end-user productivity can reduce costs and boost revenues and a reduced risk of breaches can be quantified, as can compliance efforts.

When developing this future vision, it is important to take into consideration the specific circumstances surrounding an organization. Needs will vary depending on the types of users who demand access, how much variability there is in their access requirements, in who they are and where their identities are stored. Compliance pressures are also vastly different depending on the industry and country (or countries) of operation. Risk factors for data breaches also vary depending on the information protected, affecting security obligations.

The decision whether to adopt new trends, and at what pace, will also be unique to each organization. Software-as-a-Service (SaaS) apps, the Internet of Things (IoT), Bring your Own Device and Bring your Own Identity (BYOD and BYOI) programs, among others, offer a nearly infinite set of options for customization, allowing organizations to optimize their choices to their own business needs and circumstances.

Step 2: Design

Once there is a clear understanding of the current state of an IAM program and a well-defined vision of a target, future state, it is possible to design a roadmap to fit a reasonable timeline and budget to move from one state to the next.

Within that framework, existing assets can be evaluated to optimize their value, reduce inefficiencies and become more cost-effective. A plan to roll out new solutions can be put in place with integration in mind, so controls are consistently enforced and silos of IAM are eliminated. Key criteria can be identified to make vendor and technology selections for future purchases.

The end result is a prioritized roadmap and a clear timing plan that help ensure existing technologies are leveraged and new ones are implemented in the right order. This can mean higher rates of project implementation successes and a positive return on investment.

Step 3: Execute

In this stage, the time and care expanded to evaluate the current IAM program and design a future state to fit business requirements show their value. Project and spending proposals can be more quickly and easily approved, because there is structure and purpose to the requests, tying them to overarching business imperatives. This also helps gives clear, quantifiable measures of success for each deployment and implementation. Finally, IAM product deployment costs can be dramatically reduced, because requirements and business processes are fully understood and simplified ahead of time.

With appropriate buy-in, expectations and preparedness, bringing the necessary people, processes and technologies together to execute on the strategy can be done methodically and with great success.

Step 4: Take action now

While there are plenty of organizations today with long-standing strategies designed to help them protect their systems, applications and data from unauthorized access, the need for a truly comprehensive identity and access management strategy often continues to go unmet. But now that identity has clearly emerged as a new security perimeter— requiring controls to manage, enforce and monitor user entitlements and access activities—it's time to take action.

IBM Identity and Access Management Services can help you, with a holistic approach that provides the services and technology that have gained IBM recognition as a leader in developing and delivering security solutions. Our identity and access management services focus on the key security challenges facing enterprise IT and line-of-business managers today, helping them to:

- Safeguard mobile, cloud and social interactions
- Prevent insider threat and identity fraud
- Simplify identity silos and cloud integrations
- Deliver intelligent identity and access assurance

We offer professional and managed services that include:

- ***Identity and Access Strategy and Assessment Services***—Business and technology consulting to help clients design an IAM program to fit their business needs. The offering is designed to provide an achievable plan to enhance regulatory compliance management capabilities, grant convenient access to authorized users and help protect valuable data.

  This approach, using a systematic and robust maturity model, helps clients optimize their IAM program with a prioritized list of projects to execute on a reasonable timeline, within their budget requirements.

- ***Identity and Access Management Design and Implementation Services***—Time-tested, best-practice framework and methodology for designing and implementing solutions to help maintain security control over mobile devices, mitigate internal and external threats, reduce security risks in cloud environments and automate compliance management.

- ***Identity and Access Management Managed Services***—On-premises, hosted or cloud-based delivery models offering a full array of capabilities, including user provisioning, lifecycle governance, single sign-on, enterprise user registry services, federation and multi-factor authentication.

Figure 4: IBM can offer end-to-end solutions to support your IAM needs from evaluation and design of an IAM strategy to its execution

IBM has long been recognized as a security solutions thought leader—and is one of the few service providers offering these kinds of end-to-end identity and access management solutions, from strategy development, to design, building and management. Our security specialists work with you to address your specific needs and provide the solutions that are designed to fit with your business goals.

For more information

To learn more about how IBM Security Services can help you reduce costs and increase your protection against sophisticated threats, please contact your IBM representative or IBM Business Partner, and visit the following website: ibm.com/services/security

© Copyright IBM Corporation 2016

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
July, 2016
All Rights Reserved

IBM, the IBM logo, ibm.com and X-Force are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing

improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle

SEW03038-USEN-01