Balancing Identity and Access Management for Risk versus Speed

At a Glance

Identity access management is the cornerstone of security. To arrive at programs that balance speed, risk and usability, CIOs must collaborate with the C-suite to:

- Target incremental progress over perfection
- Aim for infrastructure with governance
- Gain visibility into customer profiles
- Choose smart partners and effective products
- Address pain points to gain buy-in

Identity and access management (IAM) is the cornerstone of security. As such, it is important to balance IAM to ensure maximum speed of user access while managing risk. Proper IAM enables legitimate internal and external users to access the right data at the right time from the right devices. While IAM may seem like a check box in the journey to technology transformation, its role is much larger.

IAM is — quite literally — a key to a desired, secure and modernized state. Identity and access issues such as duplicate and stale user accounts, excessive user access and suboptimal automation can slow user access and erode security and should be resolved. Technology transformation is an opportune time to clean up old habits. "Lifting and shifting" obsolete identity and access processes to modernized technology is equivalent to using a defunct motor in a new Ferrari. Solid IAM programs clean up data, increase speed for a wide range of internal and external users, and look to reengineer and automate processes within the framework of a governance and policy program.

CIOs identify and focus on current strengths and weaknesses to arrive at a best-of-breed IAM solution that is structurally sound and integrates well in the organizational technology ecosystem. They implement IAM programs that enable efficiency and trim duplicative or overlapping technologies so that organizations are not over-licensed for capabilities that will not be utilized.

IAM brings value

IAM must be balanced for three things — speed, risk, and usability. IAM can enable enterprise transformation projects through automation that enables quicker access. It allows for movement of workloads into the cloud seamlessly and enables companies to externalize applications that are on-premises. However, speed must be balanced with each organization's unique risks. While the right IAM structure can reduce risk, insufficient IAM can increase risk.

Usability is also an important factor in an IAM program. Whether the solution is single sign-on or multifactor, a simplified, well-designed solution that is easy to use and understand can improve the user experience, make employee onboarding seamless and reduce help-desk calls. Conversely, a poorly designed solution can create friction in a user's experience depending on what choices are made in the technologies and processes that are put in place, and can negatively impact user adoption.

With far-reaching implications *across* the organization, it is crucial that CIOs are exceedingly thoughtful about their IAM strategy.

It takes time to build the right identity infrastructure. Upfront investment costs with an eye toward scalability are essential as the organization grows in people, processes, data, performance and cloud capability. Once a robust IAM foundation is established, organizations can move faster into future states.

Target incremental progress over perfection

It is critical to understand that IAM is not a project — it is an ongoing program that must span and align with the life of the organization. CIOs should aim for incremental progress over delayed perfection. IAM must be maintained, keeping pace with growth and dynamic business needs. IAM cannot be an afterthought of technology transformation, as afterthoughts lead to failure and newsworthy security breach disasters.

Aim for infrastructure with governance

Beyond choosing the right technology, strong IAM requires a solid infrastructure, with a strategy and a roadmap. CIOs should build out a strong IAM infrastructure with ongoing maintenance and improvement that aligns with business needs. Maintaining IAM is a never-ending marathon because once the infrastructure is rolled out, there are additional capabilities, integrations and (sometimes) business units that impact IAM programs.

While a strategy and a roadmap are instrumental, they must be accompanied by a governance model led by a steering committee that champions the voice of the customer. The steering committee serves to inform C-suite decision-making with an empowered understanding of business pain points, risks and security challenges. It is then that informed decisions about trained staff can be made to ensure that the organization's crawl-walk-run strategy leads to the stated vision.

Gain visibility into all identity profile types

An effective IAM program creates a consolidated record for each person as one identity. For a comprehensive view of each user's accessibility and associated risk, IAM must be able to form a single identity for each user. While many organizations are focused on employees (e.g., segregation of duties), client identities across the various business units are just as important, particularly in the case of corporate mergers and acquisitions, where a customer might have access across several business units. A strong IAM program addresses disparate identity issues by developing a consolidated profile for each person across a unified user experience when they interact with the organization.

Robust IAM demands smart partners and effective products

Put bluntly, effective IAM is not a do-it-yourself program. To prevent user access breach disasters, CIOs must recognize that they need smart partners and best-in-class products. IT departments that attempt to build and maintain their own IAM program are left with failed frameworks, or they crash along the transformation journey. Experienced IAM partners enable flexible frameworks that control risk while leveraging customized technology such as intelligent process automation (IPA) and artificial intelligence (AI).

Address pain points to gain buy-in

IAM touches every aspect of the organization, making implementation and adoption very challenging. When new controls are implemented, users often find a way around them. To gain user buy-in, CIOs must collaborate with other C-suite leaders to solve for user pain points such as automating tedious functions. Offering value propositions to C-suite members is key to effective implementation and acceptance. The sooner users are vested in the controls, the more successful the program will be. Issues unique to C-suite members include:

- **Chief risk officer (CRO) and chief administrative officer (CAO)** — Access governance models, monitoring, prevention and remediation strategies and identity risk scores (of internal and external users, including vendors) are top concerns. It is important to demonstrate value by providing traceability for faster, more accurate audits. Implementing IAM controls to address access and permission for risk reduction offers value propositions to CROs and CAOs.
- **Chief financial officer (CFO)** — Preventing and mitigating data breaches, protecting assets, and demonstrating return on investment are critical to CFOs. They look for increased production, efficiency and value, while protecting sensitive assets with privileged access management programs.
- **Chief data officer (CDO)** — Protecting data from hackers is the critical task of CDOs. IAM offers the data protection, monitoring, privacy policies and classifications that CDOs want while also applying analytics for enriched, contextualized data from protected data lakes. A collaborative partnership between the CIO and CDO is crucial for building an IAM strategy that considers the who, when, why and how of data access.
- **Chief marketing officer (CMO)** — CMOs are interested in privileged user management, which is the activity of users who have privileged access. They are concerned with controlling proper usage of social media accounts and other external-facing communications to secure brand value. And they appreciate the ability to rapidly capture customer information, protect customer identity and enable quick authentication.

Where do companies go from here?

IAM brings significant ROI to enterprise transformation by:

- Supporting compliance
- Elevating security
- Increasing operational efficiency

While the most significant benefits of IAM cannot be numerically quantified, the value of an effective IAM program is undeniable, because access breaches come with severe consequences and intolerable monetary and reputational costs.

To acquire the greatest benefit from IAM during enterprise transformation, companies should undertake the following, with each step centered on IAM:

- Understand the organization's current processes, users and technologies
- Know the organization's transformation infrastructure goals
- Understand the drivers for transformation
- Assess how IAM fits into enterprise transformation
- Lay out an IAM strategy with subject matter experts
- Evaluate gaps and opportunities and discuss pain points with business centers
- Create a roadmap that delivers iterative and consistent improvements to security, risk reduction and the user experience

Identity and access management is difficult and ongoing. CIOs should aim for progress over perfection. IAM programs that scale for growth are essential to bringing a future IAM state endowed with security, speed and visibility.

AUTHORS

ASHRAF MOTIWALA, Managing Director, Security and Privacy, Dallas
DUSTY ANDERSON, Director, Security and Privacy, Phoenix
CHAD WOLCOTT, Director, Security and Privacy, Boston

*Managing Director **ENRICO FERRETTI**, Milan, also contributed to this article.*

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

For more information, please contact us at TechnologyConsulting@protiviti.com.