With the adoption of distributed and remote infrastructures, the need for an identity and access management (IAM) solution has become paramount and is a top agenda item for most chief information officers (CIOs). The IAM market is also extremely competitive, with many technology heavyweights and exciting new talent battling it out for the top slot in this space. The options to choose from are many and it is important to have an IAM strategy and an underlying process in place to enable the tool. Effective governance along with automated role management, authentication, user profiling and integration are keys to establishing a holistic IAM solution.

An automated process that provides users with access to systems and revokes access when necessary forms the crux of IAM. Improved discovery, intrusion detection and monitoring technologies along with a rapid increase in the number of technology vendors offering IAM solutions may make it appear easy, but this is not the case. Companies can spend millions of dollars every year on security initiatives and still struggle to reach the right combination of confidentiality, integrity and availability (CIA). Lack of periodic entitlement reviews and nonexistent links among human resources (HR) systems, active directory and enterprise applications result in inaccurate employee identification and employment status. These are two of the major reasons why IT security regularly comes up short in IAM strategies.

Business process advancements fueled by technologies such as cloud, remote infrastructures, mobility and bring your own device (BYOD), along with changes in the way IT services are provided, such as multivendor outsourcing, Software as a Service (SaaS), multitenancy and virtual infrastructures, have made the IAM puzzle more interesting. The average consumer’s life has also changed for the better due to the above technology advancements, but these new technologies also introduced major risk factors to private data.1,2

According to an RSA survey inquiring about the status of IAM within UK businesses, 76 percent of IT directors concurred that IAM is a priority to their organization.3 Other countries in Europe also have a similar outlook. A survey of CIOs in the UK, France and Germany by Quest Software Inc. found that in 2013 IAM is a priority for more than three quarters of European organizations.4 Given the industry focus on this in the current milieu, it is important to consider the critical success factors in the IAM journey.

**USING A TOP-DOWN APPROACH**

As with any investment-centric IT initiative, it is extremely important to get business buy-in for IAM. In addition, IAM is a policy-driven initiative that should be communicated and mandated from the top business levels. This also helps to enforce the IAM policy at the employee level and to emphasize the consequences of noncompliance; it may also help with reducing instances of hacking via popular methods such as spear phishing.

In the RSA survey, respondents identified senior executives/board members as one of the biggest barriers to the implementation of IAM— one-third of IT directors declared cost and lack of funding and 27 percent stated buy-in from the board.5 The key to convincing the business is to discuss the pain points of system security, IT administration and compliance requirements that IAM would address. Articulation of business values should include improved lead time for new user access provisions, productivity improvements through enterprise single sign-on (SSO), cost cutting through reduced service desk use and improved compliance metrics during audits.

**USING A GOOD-BETTER-BEST PROGRESSIVE SOLUTION**

An IAM solution is a long-term investment and an evolving initiative. IAM has many components in role management, provisioning, password management and enterprise SSO. Thus, a good-better-best practice should be adopted.
While password management may be a quick win, automated provisioning may have security implications and federated identity systems and SSO may pose challenges in the form of complexity and diverse security architectures, particularly for legacy systems.

The best way to accomplish a good-better-best practice would be to understand the overall objective, break it down into smaller goals and come up with a road map (figure 1). Data security, regulatory compliance, competitive advantage, productivity benefits and reduced overhead are some of the goals that can be targeted during the road map phase. The road map should then be used as input for a plan—identifying quick, medium- and long-term wins with consideration for low-, medium- and high-priority goals targeted (figure 2).

**ESTABLISHING GOVERNANCE FOR CONTINUED BENEFITS REALIZATION**

It is important to outline what the IAM solution will enable—it helps if the right expectations are set at all levels and knowing what to measure. User profiling, authentication and rights management are key to kicking off the program. User profiles must be set up with role definitions, access rights, identity verification and user groups. Standard and core services provided, with access times, authentication procedures and approval workflows, should be included.

![Figure 2—IAM Target Goals](image)

![Figure 1—Benefits Realization Through a Phased Road Map](image)
The user life cycle should be documented with procedures for access provisioning, temporary suspension and permanent revocation. Exception procedures should also be documented in accordance with security policies and implemented through IAM. A steering committee should be established to review the progress on a periodic basis. The effectiveness and efficiency of the solution should be tracked and measured using formal metrics. The metrics help the business to understand how the IAM solution has improved security and enabled business benefits in the form of productivity improvements, better compliance numbers and return on investment (ROI). Oracle’s functional strategy of categorizing key requirements (such as provisioning, authentication, authorization, self-service and audit/compliance), understanding the current state and building a shared vision of the target state with the business stakeholders is a best practice in this area.6

SECURITY AND AUTHENTICATION NEEDS
Additional authentication for critical systems and system life cycle monitoring are two important aspects of IAM. Authentication must be strong enough to prevent hacking while not encouraging bypass attempts with excess security. Some business-critical legacy systems may still be in production but may not have expert support due to outdated technology. Access provision to such systems should be minimal and based on a business case to reduce the risk of extended outages. Other legacy systems may not be supported at all, but may be accessible by users and, therefore, require audits if not decommissioned. In application environments with continuous integration, production data are used for testing as an exception—quite frequently due to data creation and data dependencies. In addition to data masking and the anonymity of personally identifiable information (PII) and sensitive PII (SPII), access control and provisioning of such environments need to be controlled, as hackers might target such nonproduction environments due to their reduced security measures.

Mobile and home users should have an extra layer of authentication such as biometrics and geotagging for location identification. No other breach emphasizes the need for multilayer authentication more than the RSA SecurID intrusion of 2011. It was a wake-up call for IAM vendors and customers alike as it showed the meteoric rise in hacking capabilities, emphasized that reputation in the security industry did not guarantee safety, and paved the way for research on new and improved authentication measures.7 Service request management (SRM) and standard change models can be used for requesting access, but for systems hosting product know-how and finance details, an extra level of security such as biometrics, government ID verification or manager approval may be required. IAM is also accountable for compliance data provisions, providing a record of access during forensic investigations and complying with user information data protection legislation.

INTEGRATION CONSIDERATIONS
In addition to its affiliation with change management and SRM, IAM is a process with multiple interfaces that are integral to vendor tool offerings and can be achieved through partnerships. The policies executed in IAM are defined in availability and security management. Unauthorized access is detected by intrusion detection (ID) and event management (EM) tools and handled as part of security incident and event management (SIEM). Hence, EM and ID parameters for filtering and triggering responses should be defined accordingly. Integration with HR systems ensures entitlement verification and configuration management record changes to user access in the configuration management database (CMDB).

CONCLUSION
There are significant financial and reputational risk factors associated with losing corporate data, particularly customer data and other sensitive business information. Among organizations that have experienced these data breaches, 33 percent agreed that the enterprise had lost customer trust and 32 percent believed its corporate reputation had been damaged.8
The recent hacking of security firm Bit9 is a case in point. Although the full impact of the hack on Bit9’s business is yet to be determined, the negative publicity and customer angst expressed after the incident imply severe damage to the firm’s reputation.9

A must-have for any IAM solution provider is a disaster recovery plan that gives the organization a head start in minimizing damages in case of a hack. Recent security attacks have proven that no amount of preparedness is sufficient in such a situation. For example, after spending US $63 million on a massive outreach program involving more than 60,000 customers, disgruntled clients and industry experts still questioned RSA’s response to its security breach.10

At the corporate, consumer and government levels, there are major opportunities for improving how to protect private data. The potential for further advancements in the field of technology is enormous, and as with every opportunity, there is an associated risk.

In a world where business processes are increasingly being delivered over social and collaborative platforms, IAM is not only a compliance mandate, but a key differentiator over competitors. It is past the time to question the value of an IAM solution; instead, it is time to protect and differentiate the enterprise by continually increasing the knowledge and understanding of the risk in the enterprise. While unauthorized access and security breaches can be reduced to a great extent with a capable IAM tool, it is the implementation strategy and the underlying processes that can enable the technology to secure the enterprise.

REFERENCES


ENDNOTES


5 Op cit, RSA Security


7 Savage, Marcia; Michael S. Mimoso; Robert Westervelt; “The RSA Breach: One Year Later,” TechTarget, http://searchsecurity.techtarget.com/magazineContent/The-RSA-breach-One-year-later

8 Op cit, Quest Software Inc.


10 Op cit, Savage, et al.