GIGAOM RESEARCH

Identities management: an evolving landscape

Sal D'Agostino

January 8, 2014

This report is underwritten by Okta.

TABLE OF CONTENTS

Executive summary

Identity and access management (IAM) has traditionally focused on managing user information technology accounts in the enterprise. The rise of different types of accounts and identities such as cloud, mobile and other devices, e-commerce, and social networks has asymmetrically complicated things. Cloud, mobile, social, and personal networks have types of identities, platforms, services, and technologies not traditionally addressed by enterprise IAM. The result is fractured user authentication and authorization across applications and resources. There is not a single type of identity, identity token, or IAM that takes this into account. Identity management has very literally become identities management, and individuals and enterprises are struggling to keep up. In crafting IAM solutions to meet this evolving landscape, CIOs and those responsible for IAM deployments should take the following as given:

- User accounts exploding in number and type require identity and access management providers to offer flexible solutions. Even with this flexibility, the enterprise will likely deploy multiple IAM solutions.
- Multiple IAM solutions with multiple levels of identity assurance and attribute confidence mean that policy must adapt to the differences among identity types, and this will result in new and different procedures and workflows in order to manage users across these contexts.
- The same cloud and mobile services are being consumed internally and provided externally. This is creating a new and symbiotic dynamic between IT and development organizations in the enterprise. The management and synchronization of internal and external services will become a core competency of IAM solutions.
- Identity information — as widely defined here — is being generated and shared at astonishing rates. This creates extreme challenges for the protection of personal and corporate data and resources. In the enterprise, this drives a need for new ways to protect and share information while enabling a knowledge workforce.
- The explosion, leakage, and compromise of data will drive a demand for identity and other analytics at the edge in all types of devices, further driving distributed solution architectures and new requirements and programming interfaces.

- Personal data storage and clouds will become increasingly important systems of record and policy information, administration, and decision and enforcement points. IAM solutions will need to take this into account.

Identities management

Everyone wants everything, anywhere, anytime. Cloud and mobile – both devices and individuals – put these expectations in play, and there is no going back. The economics of cloud combined with accessibility, applications, and device support for the major mobile platforms continue strengthening these expectations. Today's norm is expecting an online interaction across devices and services, independent of the type of transaction. As a result, the number of user accounts is skyrocketing among a mash of identities services.

The mash ranges from zero trust to bonded transactions and includes device identities across PC, tablet, phone, homes, things, and facilities across platforms. These identity type and technology differences complicate what has become identities lifecycle management since each has a different:

- Policy
- Workflow
- Registration
- Attribute assignment
- Credentialing
- Validation and revocation

Traditionally, IAM has been offered as an on-premise solution that encompasses all of the previous steps. IAM solutions also have typically consolidated the onboarding of individuals into an enterprise-owned IT system and managed the means of identifying users as valid and having the rights to resources (data or facilities) and services (applications).

Through these consolidated systems, organizations and individuals adhere to a policy to gain what has traditionally been referred to as a level of identity assurance. Each level of assurance is embodied in a workflow (a series of well-defined steps, often with enforced controls) to enable the identity process described above. Traditionally this process enabled the use and management of IT systems owned by the enterprise.

Cloud and mobile have changed this and, as a result, the way IAM is delivered. For the CIO, cloud, mobile, and the related new identity types impact all of the policies, processes, procedures, and technologies of IAM services. Employees bring their own social and technical networks in addition to a range of devices. How to integrate these accounts, endpoints, and their associated applications and data is a tremendous challenge — as well as an opportunity — for information technology solution providers.

The same innovations that introduced the challenges – cloud and mobile devices – provide a means of delivering innovative identity services as well. In leveraging cloud and mobile, IAM solutions can be available at scale and, depending on the context, varyingly resilient. At the same time, most organizations are simply not ready to make this jump and provide the infrastructure and services to support all of these identities when they most need and can benefit from them.

As a result, a number of new identity solutions have come to the fore. Some of these have evolved from cloud offerings and the need to manage a cloud or mobile customer base. Others have come from companies specifically created to meet this need. And others yet come from the evolution of existing identity and federation service providers.

The challenges of identities management in 2014

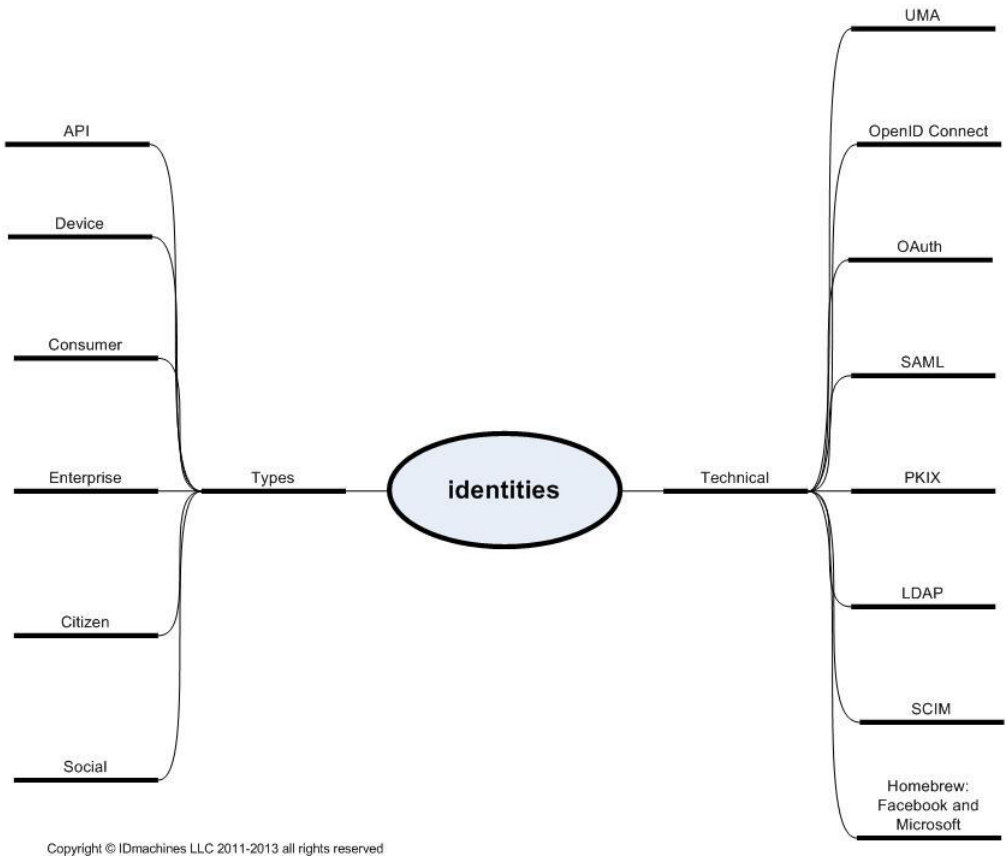
Privacy

Privacy, or how to address its absence, is the major challenge in managing the increasingly diverse world of identities. The privacy challenge is exacerbated by the extent to which identities, identifiers, and other attributes are shared across numerous social and business contexts. All the sharing has irrevocably leaked untold personally identifiable information (PII). Often this occurs in the process of commercializing the information. Over four billion email addresses flow to a billion Facebook accounts, half a billion iTunes accounts, 250 million Dropbox(es) or SkyDrives, and 200 million Pandora, eBay, Amazon, and Twitter accounts. The further sharing with third, fourth, and nth parties endangers the very idea of privacy. Numerous repositories of email addresses, usernames, and passwords along with other personal information have been compromised from individuals to companies and governments. Privacy protection across personal and corporate information needs to be a consideration for any IAM in 2014.

Multiple identity types and tech

Deploying identity, authentication, and authorization solutions requires identities management. Particularly in the United States, there is no one identity or technology solution. The challenge for the CIO and Jane Q. Citizen is the different types of identities and technical approaches to the protocols, tokens, languages, and hardware used to implement them. Each of the types of identities affords a mash of different functions. Putting some names on these combined identity types and technologies presents a picture for the CTO and CIO that looks like the figure below.

Figure 1. Various identities types and technologies



(Source: IDmachines LLC, Gigaom Research)

Multiple identity services actors

Another challenge is managing the range of actors assuming these types and leveraging the different technical solutions. It is no longer just a single identity provider and a relying party. Today actors can range across identity provider, credential service provider, credential broker, attribute provider, attribute authority, attribute broker, attribute exchange, relying parties, and end users. The enterprise was traditionally the source of many of these services, but today this is changing. The personal data ecosystem is evolving rapidly, with individuals seeking to regain control of their identities, attributes, and their use. At the same time, external email and social networks act as identity providers, and others federate these accounts. For example, Canadian banks are now providing credentialing services, and a new class of credential broker is enabling this service. A similar pilot has just been funded by the U.S. Postal Service. Governments and third parties have long provided identity attributes, and now the success of social

networks in providing user attributes has led to the business of attribute exchange. Many of these actors are new to IAM.

These actors provide and consume identity services just as they provide and consume cloud and mobility services. And cloud-based service providers want to use cloud-based solutions, fostering collaboration and integration. Some have evolved specifically to meet this challenge. For example, brokers and exchanges are now registering, mapping, and maintaining services across identity types and technologies. Identity service providers can tailor different types of identities, technical authentication, and authorization services specific to the particular actor(s).

Standards

Identity standards remain a challenge. Standards are spread across organizations and uneven in usefulness and impact. In the meantime, proprietary solutions (e.g., initial clouds) remain widely deployed. Nonetheless, adoption of the latest round of identity standards is on the rise.

- OAuth has been leveraged by OpenID Connect and UMA (User Managed Access).
- SAML continues to be widely used (in various manners) by authentication and other service providers.
- New standards, such as SCIM, look to maintain support of legacy standards such as LDAP[1] while addressing the requirements of multi-tenancy and the need for complex user attributes.
- PKI remains a basis of much of the security for the internet and device authentication. PKI provides application programming interfaces (APIs), the often-required HTTPS, and TLS so its use is hard to ignore in an overall architecture.

The challenge of mobility

A number of identity challenges exist with mobile that add to the requirements of the identity and access management suite. Identity and credential lifecycle management was already complicated before bring-your-own-device (BYOD) and the ecosystems it created. At a minimum, the enterprise will need to support new device identities and multiple new user credentials. Most enterprises will jump at the option of implementing this as a service rather than trying to build out and support new mobile infrastructure.

[1] *See RFC 4510, 4511, 4512, and 4513*

Again, front and center are mobile lifecycles and their management. Devices, services, and apps each have their own and interrelated lifecycles. As the support required for a client computer is different from that required for a browser, mobile is also different and requires different IAM. Existing solutions are not built to support the workflow or features for mobile, so their integration with app stores and the provisioning associated with mobile is likely a new policy, process, infrastructure, and service for the enterprise. New is not necessarily good.

Remote access via VPN provides a controlled and secure method of connecting with enterprise infrastructure. Providing the same access via a range of mobile devices across a range of apps from multiple service providers is a different problem.

Combine this with the challenge of the new information set associated with the devices.

- Besides app usage and other user details normally associated with managing user accounts, there are vast new categories of information generated because the device is a mobile computer with a range of networks and sensors. Some examples are geographic position, device accelerometers, cameras, near field communications, and other short-range radios. And this is just for mobile devices, which are just the front of a wave of information from the internet of things. Enterprises with supervisory control and data acquisition (SCADA) systems are already generating and likely performing analytics on this as well. All generate data that grows into big data. In all cases, the information can be used to add context and finer grain to access control decisions and presents a challenge to IAM in terms of information that may be useful to or new benefits from IAM.

- Privacy and security concerns need to take the new device data into account. At the same time, they must safeguard traditional concerns such as user, device, and identifier leakage and association.

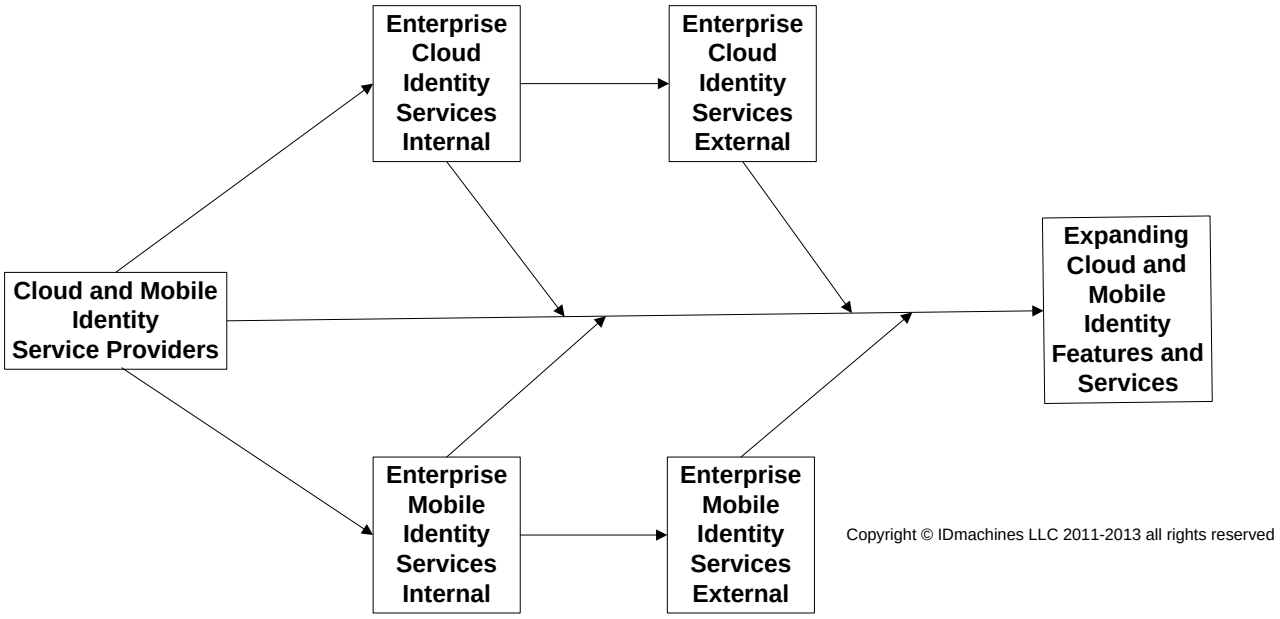
The challenge of cloud

Cloud-based information technology infrastructure, platforms, and services are attractive to a wide range of enterprises for a variety of reasons. Cloud and mobile attract and feed off each other in multiple ways and combine to accelerate their use and uses.

Research for this report – which included conversations with cloud service providers across finance, technology, and life sciences whose IT departments were also consumers of cloud-based identity and

access management – uncovered an interesting and productive back-and-forth between service providers and service consumers. These were fast-growing enterprises with a need to onboard multiple cloud service providers from Salesforce, Google Apps, WebEx, Office 365, etc. – typically in the dozens. They are also service providers of applications to their customers via devices and the web. For the cloud-committed, this has evolved into partnering with their cloud identity and other service providers to deliver other customer and partner cloud services. Amazon is the most prominent example, but there are many others, including a number of IAM providers.

Figure 2. Internal services become external services



(Source: IDmachines LLC, Gigaom Research)

The differences in the identities of the internal and external service accounts result in a desire to consolidate their management and expand the solutions in the market. Over time, the differences between internal and external will drive a convergence of features. This creates less of a distinction between large enterprise and small-to-medium business solutions and greater "co-opetition" among IAM cloud and mobile vendors.

While building external services based on their use internal to the enterprise is extremely healthy from a market development perspective, it also represents challenges. As more services are put into play, their synchronization needs to be addressed. This is particularly true as new service features (e.g., multi-factor authentication, single sign-on, or federation) are built into other services. As the relationships increase,

the challenge of synchronizations does as well. Providing mail, calendars, and authentication and authorization services no longer requires just synching devices, operating systems, and applications but also synchronizing APIs. The service provider that integrates services must be able to sandbox its multiple services and test new API releases. And synchronization of services and their related APIs furthers the requirement for back-and-forth between provider and consumer. The consumer/provider internal/external relationship creates new classes of services in the API economy of the enterprise cloud and mobile ecosystem.

IAMs that operate in this environment must add managing APIs to the types of devices and service identities that need to be addressed in the enterprise. Users authenticate to APIs, but APIs also connect to APIs. The ability to manage identity and access of the service provider APIs depends on their user interface, functionality, and documentation. This explains why OAuth is so attractive; it provides a standard for connecting to the APIs. And while this is often referred to as authorizing an API, in reality it is more akin to authentication. And given the wide acceptance of OAuth with its limited authorization capabilities also explains why JOSE, OpenID Connect, and UMA become important as the desire grows with the feature sets to do more fine-grained authorization of the access to the APIs. This set of evolving technology standards does not tie access to policy; as a result, they are better able to deal with the different identities that need to be managed (e.g., XACML, which can be powerful in a specific context, has challenges across them).

The challenge of scale

The largest enterprises have hundreds of thousands of employees and contractors, resulting in millions of accounts under their IAM while internet scale runs into the billions. In order to leverage social, citizen, devices, and other identities, IAM must interact with large and growing populations. Access control at these scales creates a challenge for centralized approaches and will push for the further development of solutions that can deliver IAM services in a distributed manner.

The challenges of scale have multiple and secondary aspects – considerations other than sheer numbers. In particular are the related challenges of diversity. For example, diversity in geography enforces diversity in the solutions to a global market. Even smaller enterprises have global workforces that include field and development operations. As a result, scale implies diversity, and diversity impacts the requirements around privacy and compliance.

The challenge of uncertainty

Another challenge providers and consumers face is the uncertainty associated with the deployment environment. Synchronization and other challenges get more difficult in the context of uncertain infrastructure and platforms, so solution providers must be capable of working across enterprises and their service provider networks, authentication technologies, and devices. While standards may help, you still need to understand the network plumbing and the wide range of features and functionality that still exist.

Uncertainty also exists in the legacy and custom applications remaining in a customer environment. Even in the case of known legacy silos, the way these components are used may vary from organization to organization. A system of record for one IAM deployment may be a relying part in another. This makes it all the more difficult to sandbox a potential deployment. Most cloud and mobile identity and access solutions introduce new components and endpoints into the enterprise, making it at best a learning experience.

Cloud and mobile exert another kind of uncertainty. IT networks have long used IP addresses as a possible indication of where a transaction is taking place, but this is much less deterministic in a service-based architecture. Device geographic position or other information potentially mined from big data or social networks may well be leveraged by IAM solutions to reduce this aspect of uncertainty.

Bridging the gaps

As more cloud and mobile solutions come online, the enterprise will increase its demands to add them. Security and other gaps exist in enterprise implementations of cloud and mobile, but they have not slowed their adoption. Lack of multifactor or strong authentication and lack of fine administrative or fine-grain access controls are some examples. These gaps set the challenges and requirements and imply a wider solution set than typically deployed in the enterprise identity suite.

Identity and access management has focused on managing user accounts; it seldom is actually involved in managing identities, let alone multiple types. The impact of cloud and mobile has put the focus on managing these types of accounts. Solutions that bridge the acute authentication gap may not bridge the wider IAM needs around authorization and broader and finer controls. Tomorrow's needs have little impact on purchasing medicine for today's pain. Even so, having an understanding of these is a step in cloud and mobile enabling. Understanding these gaps and needs can be helpful in defining requirements for solutions that can bridge requirements over time.

The enterprise must not just focus on the multiple types of identities and technologies; it must also focus on the policies and procedures to be put in place to meet the business goals that IAM looks to support. One way to do this is to identify the critical use cases and related IAM requirements. Often the use case is the desire to consolidate login across enterprise cloud and mobile service solutions that in many cases live outside of the enterprise directories and access management systems.

Other use cases for IAM to address include managing apps via the creation and management of an enterprise app store. Along earlier lines, enterprises can thus help determine the features they need in the APIs of their external application service providers. High on the list of features is the ability to provide users with self-service and automation in the provisioning and de-provisioning process. Just as initial IAMs provided value as a means to centralize this so too must an IAM solution look to provide these features for cloud and mobile solutions.

In regulated industry, the need for strong multifactor authentication (MFA) also continues to rise in parallel with the need to enable zero trust identities. IAM solutions that have the flexibility to address a range of authentication assurance will much better match the range of enterprise use cases. In addition to fixed identities and levels of assurance, the notion also exists of being able to step up the level of identity assurance or authentication. Enterprises must understand the difference. The former involves the nature of onboarding in the enterprise and the extent to which there is a separation of roles in enrollment,

background investigation, adjudication, and provisioning components of the process. Separately stepping up the level of authentication can be accomplished with the requirement for additional or different authentication tokens and factors.

The recently updated National Institute of Standards Special Publication 800-63-2 addressed the level of assurance for identity-proofing and authentication. While not a be-all document, it does provide a table (3) that examines identity-proofing requirements by assurance level and a table (6) with different token levels of assurance based on their four levels. It also provides a table (7) that shows the combination of the potential combination of tokens. The token tables are of interest not only in establishing the level of assurance but also in how they can vary within a type. So not only do IAM solutions need to manage multiple identities but they also need to do so over a range (9) of token types that can be associated with them. The token types – all of which cover the range of something you know, something you have, and something you are – include:

- Memorized secret token
- Pre-registered knowledge token
- Look-up secret token
- Out-of-band token
- Single-factor one-time password device
- Single-factor cryptographic device
- Multi-factor software cryptographic token
- Multi-factor one-time password device
- Multi-factor cryptographic device

The number of solutions for MFA, in particular, continues to climb, with more than 100 vendors identified in related research. Some standards for one-time passwords (e.g., OATH) or the use of a short message service (SMS) have an ability to leverage mobile devices and push MFA use.

In addition, biometrics continue to creep their way into the enterprise. While only narrowly implemented as a means of achieving MFA, picture-tagging and low-cost fingerprint sensors are making biometrics

part of the social or device package. Contextual biometrics based on user behavior have also begun to weave their way into the enterprise – a new class of "something you are" based on what you do, thanks to big data. Enterprises must understand that a biometric is more like a username than a password, but unlike a username, a biometric should not be shared. While we did not run into any IAM solutions that specifically address the challenges of biometrics during the course of researching this report, most of those interviewed did include accommodations for MFA.

Longer-term approaches are also important. In a number of cases, the easy provisioning, user authentication, and administrative dashboards for managing cloud-based applications contrasted with the overhead associated with using and managing them with traditional enterprise directory tools (e.g., Active Directory or LDAP). This was a driving factor in the adoption of new solutions on top of the existing IAM stack. While many of the solutions being deployed enable tying directories with applications as a service, a clear preference would be a solution that could consolidate them.

Enterprises might begin to bridge this gap by analyzing, cleaning up, and centralizing user data and looking to establish enterprise identifiers apart from email addresses. One example of the need for unique identifiers is granting electronic physical access to individuals who are enterprise employees but who may not need logical access. Having access to a building for the purpose of maintaining it does not necessarily imply a need to be provisioned in the enterprise directory. Yet the employee will likely want to gain access to portals with information about their benefits. Combined these requirements suggest a need to manage multiple identities in the enterprise with innovative solutions.

The operative word is investment; these are not sunk costs with no return. All of these cases demonstrate a clear requirement for investment in the infrastructure, platforms, and applications that support these identities and their related use cases. Those investments that support identity and access across the types and technologies – and, if possible, standards – provide a greater return than those that are one-time fixes that address a silo of identity or technology. And with a nod to the yin and yang of cloud and mobile-service consumer and service provider, the investment might yield a return on the enterprise products and solutions and even top-line revenue.

Implications for the CIO

The growth of identity types and technologies that directly impact the CIO is in direct proportion to the size, age, and type of organization. The CIO at a cloud startup, at a 20-year-old business, at a Global 1000 enterprise, and for a federal, state, or local government all have different requirements even though they may have the same number of employees. Even with a clean slate, many organizations still pursue stove-piped solutions as long as they meet an acute need, even when these are in the cloud. So in some way, this is simply a matter of degree. The big difference for the new enterprise is that it does not have to worry about moving to the cloud; it can simply start there.

All cases have a need to implement IAM best practices that take risk into account and that leverage standards to the extent possible – all the while balancing privacy, security, and usability. CIOs need to keep these IAM best practices in mind as they address today's needs. In any of these cases, the goal is:

- Reaching a single system of record
- Having an IAM with flexibility in supporting identity types and technology
- Doing all of it on a budget

Cloud and mobile have made the CIO a key business partner. In technology companies, IT is the delivery mechanism for the enterprise value proposition. Even in traditional manufacturing, critical infrastructure, and natural resource industries, technology plays an increasing role. In smaller concerns, titles such as vice president of sales enablement accurately reflect the evolution of the CIO role. It is indicative of a wider than expected outcome for an IT investment – namely adding to the top line in addition to the more traditional focus on the bottom one.

IT can become a partner of the development team in ways that go beyond simply providing IT services. This goes to the point raised earlier in which internal use provides experience with technology and partners that might benefit the external offerings being developed. While only hinted at in the course of this research, it seems to be another area where the modern CIO and his or her organization can bring additional business value to the enterprise.

At the same time, identity threats in terms of fraud, espionage, or continuity of business are all real and growing. As a result, the CIO must not only enable the workforce but also protect it.

Given all the above, it is no wonder that IT jumps at service-based solutions that can progress goals with a minimum of capital investment, software deployment, or maintenance. And there remains the CIO challenge of enabling an increasingly knowledge-based workforce while measuring against protecting corporate and personal assets and privacy in a world where it's share first and considerations later.

Big data

IAM traditionally used static information stored in directories or databases. The growth of big data and analytics in the enterprise means that user data is not just static; it can be different and evolve over time. This has created a new requirement for IAM to be able to connect and even be a new type of dynamic data store with ongoing requirements for synchronization and updating of data. Big data is not simply driven by the ability to process data; it is also driven by the creation of more data from sensors, mobile devices, and apps. This is combined with an expansion of the computational capabilities to process it and a need to feed those capabilities. The ability to collect, store, and analyze increasing amounts of data increases the amount of information and the richness of context that identity and access management systems can use in managing people and resources. The cloud is an enabler here because it can leverage Moore's Law by pushing data collection, storage, and processing into areas not yet realized.

Personal data stores

Another important trend for the CIO to recognize and leverage is the growth of personal data stores, which are different from the release of personal data to social sites with users effectively handing over control of their data and being made the product of the social service. It is also different from the way the enterprise controls identity-related information. While the enterprise primarily controls all of its information, the growth of personal data stores and personal clouds are on the rise and a useful source and approach to data.

These consumer and personal identities represent a different workflow for the creation and registration of these identities, and they also represent the use and need for new workflows with increased user control over the release of personal identity attributes. This is part of the promise of UMA, which puts the user in control, as well as its ability to distribute and isolate the access control decision based on the user (owner) requirements for protecting and sharing their information. This can enable other types of identity exchanges and registration services that look to do the identity business of Facebook and the like. In this case, it is a more transparent commercial model in which the identity information acquired and sold recognizes the value and owner as opposed to data obtained via an obfuscated end-user agreement.

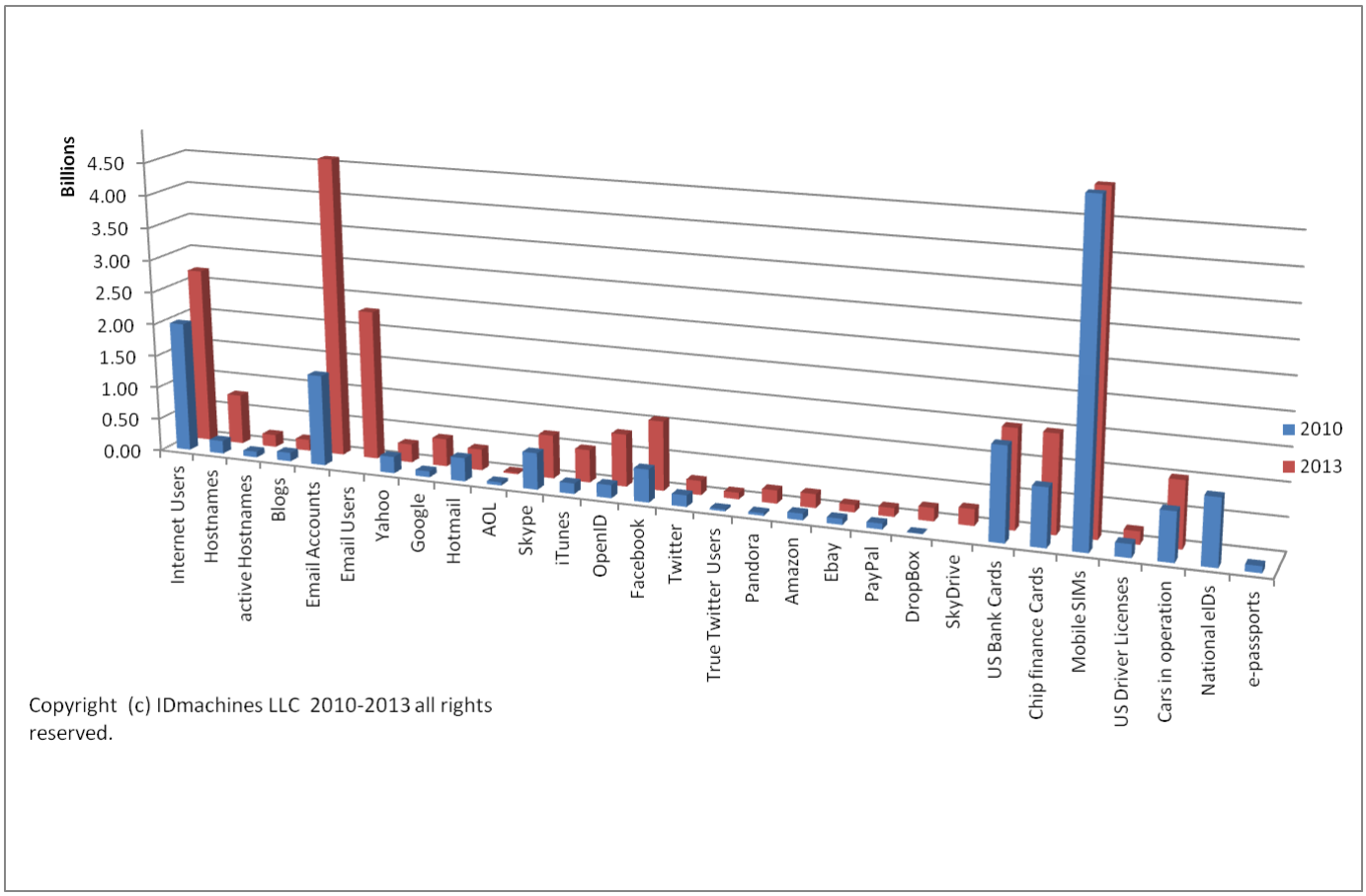
How many of those identities?

The types and technology of identity will continue to expand. In related research, IDmachines looked at the growth of the number of identities and related accounts in 2010 and again in 2013. The figure below shows the selected online identities across user types and accounts along with some other types of identity credentials and devices. These categories represent the actual numbers reported from a variety of sources associated with each of the different types of identities and devices. Note that some of these categories overlap.

The following highlight some of the numbers with implications for the future:

- Across categories, user accounts continue to explode. While the number of accounts for email and social are in the billions so are a number of other categories.
- The number of OpenID accounts is approaching a billion as the protocol becomes adopted by major sites such as Google+, Yahoo (Japan), AOL, and others. It shows how attractive identity standards that address the desires of development communities can be. This number also shows the demand for easy-to-use identities regardless of their level of assurance. The transition from OpenID to OpenID Connect has allowed it to maintain this footprint.
- The number of chip finance cards exceeds the number of Facebook accounts. This large number of strong identity credentials demonstrates the potential for banks to be in the identity business. This report mentioned Canada, where banks have been incorporated into the national scheme for delivering citizen identity credentials that provide higher levels of assurance and that hold the potential to be leveraged across identity types. High-assurance user credentials have yet to have a significant impact on the internet or enterprise network.
- The number of mobile devices as represented by the number of subscriber identity modules (SIMs) produced in a year exceeds the total number of email accounts and is five times the number of Facebook accounts, giving a stark example of the breadth of mobile devices and the market for mobile services. This number is also a stark example of the magnitude of device identities that currently need or will need to be managed.

Figure 4. Identity accounting



(Source: IDmachines LLC, Gigaom Research)

Apart from sheer numbers, the diversity of identity types and technologies also implies that static solutions simply don't address the reality of the marketplace. Identity and access management solutions need to be able to be adaptive to change, and access control decisions need to be dynamic. This implies a need for access control decisions to adjust the authentications and authorizations to the context.

Key takeaways

While the breadth of identity types and technologies continue to grow, the deployment of solutions will still depend on the acute needs of the enterprise.

- Nothing is more acute than the need to enable cloud and mobile solutions, but the economics of identity and access solutions must talk to a return on investment (ROI).

- This does not mean that the arguments about reduced cost of authentication, authorizations, administration, audit, and analytics don't get the attention of the CFO. It is very compelling to make a case – as many service solutions do – that they can reduce capital expenditures by one-fifth. It is simply the case that the argument for an IAM investment can be made to the CEO as well as it is a critical component and crucial service to delivering core business value.

- The arguments for IAM in general and identity as a service need to address the top line as well as the bottom.

- Many knowledge workers need to do everything, anywhere, anytime. Enabling these workers and the balance of the enterprise workforce will drive the enterprise's top and bottom lines. The ability of the modern CIO to deliver on this is a key to turning IAM into a critical business requirement rather than an operating cost. For example, user administration and help desks have traditionally been perceived as operating costs. Yet a dashboard that shows an increased administrative burden with specific users and applications could be viewed as early warning of decreased employee productivity and potentially top-line performance.

- In this vein, there is an opportunity to evolve corporate culture to where taking action to maximize knowledge worker productivity is the goal rather than looking at improvements as an increased operating cost. This should be the goal for a modern CIO and enterprise IAM. In doing so, strong consideration needs to be taken into account of multiple identity types and technologies that can be leveraged to enable the knowledge worker and the stable of enterprise devices.

About Sal D'Agostino

IDmachines LLC and Salvatore D'Agostino provide technology and services to identity, credentialing, access control, security, machine learning/analytics, and technology transfer customers. IDmachines leverages 30 years of experience with large-scale federated identity and security deployments in many cases involving the commercialization of new technologies. D'Agostino's customer and project experience includes EZPass and other electronic toll collection systems, many SCADA and industrial automation applications, the United States Capitol and Pentagon physical security systems, the Personal Identity Verification credential infrastructure for the United States federal government intelligence, defense, and civilian agencies as well as identity, credential, and access control infrastructure for global enterprises and governments.

About Gigaom Research

Gigaom Research gives you insider access to expert industry insights on emerging markets. Focused on delivering highly relevant and timely research to the people who need it most, our analysis, reports, and original research come from the most respected voices in the industry. Whether you're beginning to learn about a new market or are an industry insider, Gigaom Research addresses the need for relevant, illuminating insights into the industry's most dynamic markets.

Visit us at: research.gigaom.com.