onelogin

IAM – Beyond Convenience

www.onelogin.com | twitter.com/onelogin

OneLogin, Inc. | 50 Osgood Place, Suite 100, San Francisco, CA 94133

855.426.7227

Identity and Access Management (IAM) is the official description of the space in which OneLogin operates in but most people who are looking for a solution in this space this will search for "single sign-on solutions." Why? Because for many people, single sign-on is the extent of their knowledge about IAM. In this paper, we will explain the scope of IAM and how it can help your organization increase productivity, strengthen security and achieve regulatory compliance.

IAM Benefits

- Improved regulatory compliance
- Reduced information security risk
- Reduced IT operating and development costs
- Improved operating efficiency and transparency
- Improved user satisfaction

WHAT IS IDENTITY MANAGEMENT?

Identity management plays a very important role within organizations. When first hired, an employee is assigned a specific email address and login credentials. He or she uses the corporate email address to sign in to an email account, CRM application and expense management solution. All emails, customer data and expense reports belong to the organization, and when the individual's employment ends, the organization must have access to and control over the data produced by the employee, while ensuring that they can no longer access the data.

Wikipedia describes identity management very succinctly:

> *Identity management describes the management of individual identities, their authentication, authorization and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks.*

To this end, IAM solutions authenticate employees and authorize access to various applications and functions in the cloud and behind the firewall. Additionally, IAM also helps end-users and IT staff be more productive by automating tasks that used to be manual.

According to Forrester Research, security, productivity and compliance are the main drivers for deploying IAM solutions (see Figure 1). The rest of this document will go into more detail about each of these three drivers.

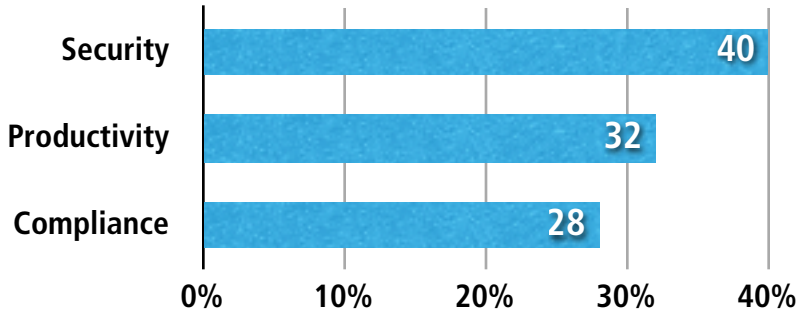

Figure 1. Primary drivers for IAM include security, productivity and compliance.

SECURITY

Although there are many ways to compromise security, passwords are still the weakest link in the security chain. No matter how much you invest in firewalls, intrusion detection, data loss prevention or virtual private networks (VPNs), a single weak password can permit unauthorized access to your company's sensitive data.

WEAK PASSWORDS

It has been proven again and again that users choose weak passwords. It's humanly impossible to remember more than a few strong passwords; people either use the same password for everything, come up with a simple password convention that can be guessed easily, or write passwords on sticky notes or in spreadsheets. None of those options are secure.

In 2011, the hacker LulzSec released 60,000 passwords (see Figure 2). Alarmingly, "123456" and "password" are the most commonly used passwords.

Figure 2. By examining this 2011 breakdown of the most common passwords, it's easy to see why hackers have no problem obtaining sensitive data.

With a few exceptions, users will always choose convenience over security. Eliminating passwords by using single sign-on is the only way to effectively combat the consequences of people using weak passwords.

CENTRALIZED ACCESS CONTROL

One of the main benefits of IAM is centralized access control. With IAM, users no longer go directly to the applications and sign in manually, but are authenticated by the IAM solution. The solution then signs users into applications using a secure single sign-on protocol such as SAML. As a result, IT staff can enforce the same access policies across all applications and have a complete audit trail of all authentication and sign-in activity.

MULTI-FACTOR AUTHENTICATION

Even if a user has a very strong password, there is always the risk that someone will guess what it is and gain unauthorized access to data. Multiple authentication factors help prevent this type of breech. There are three different kinds of authentication factors:

- **Something you know** – a password, PIN, mother's maiden name
- **Something you have** – hardware token, mobile phone, access card
- **Something you are** – fingerprint, iris scan, voice pattern

OneLogin provides a wide range of strong authentication options, from PKI certificates and OneLogin's Mobile One-Time Password app, to pre-integrated solutions from RSA, SafeNet, Symantec, VASCO and Yubico.

What is Phishing?

Phishing is a technique criminals use to trick unsuspecting users into giving up their credentials by masquerading a site they control as one the user trusts. For example, a user might receive an email requesting he updates his Salesforce password by clicking on a link. When the user clicks on the link, the criminals displays a web page that looks exactly like the real Salesforce.com page; however, it's not the real thing. The phishing page captures the username and password so the criminals can use the information to access to the user's Salesforce account.

PHISHING AND SPEAR PHISHING

Some security products claim to protect organizations against phishing attacks by analyzing incoming web and email traffic. However, those products are not fail-safe and do not automatically protect employees who are accessing corporate cloud data from remote locations.

The only effective way of protecting your organization against phishing is to eliminate what the criminals are after: passwords. The SAML single sign-on standard, which is supported by most leading cloud applications, eliminates user passwords by using digital signatures to establish trust between the identity provider and the applications. As a result, the user needs to remember only one set of credentials – those for his single sign-on portal.

PRODUCTIVITY

With IAM, users don't have to manually sign into applications. As a result, increased productivity and reduced costs are, by far, the benefits most easy to recognize. However, there are numerous other benefits, including single sign-on, ease of adding apps, simplified app management, improved security and simplified compliance.

SINGLE SIGN-ON

Users love single sign-on, because it relieves them from having to remember multiple complex passwords, enter URLs and sign in manually. Single sign-on lets users launch applications from portals by simply clicking on an icon. Alternatively, single sign-on can be triggered by an application when the user accesses a deep link, for example, when he clicks on a link in an email.

CONNECTING APPLICATIONS

OneLogin's extensive catalog of thousands of pre-integrated applications simplifies the process of adding new applications to an SSO portal. Admins and end users can add apps in seconds, without any complex configuration.

MANAGING APPLICATIONS

As the number of applications used in your organization grows, administrators can easily lose track of how much the organization is spending on applications, and how well those applications are utilized. OneLogin automatically tracks all user activity and provides management staff with reports that illuminate adoption and usage trends for future planning.

PASSWORD RESETS

Many organizations are plagued by password resets. When an employee forgets a password and submits a ticket to the help desk, productivity goes down the drain. Not only is IT burdened with increased workload,

but employees cannot access business-critical applications until the issue is resolved. According to the Gartner Group, between 20% to 50% of all help desk calls are for password resets, and Forrester Research states that the average help desk labor cost for a single password reset can be as much as $70. Clearly, the costs to an organization is substantial.

Single sign-on eliminates passwords and lost productivity associated with password-related help-desk tickets, and ensures that employees never fail to sign into applications.

MEETING REGULATORY REQUIREMENTS

For organizations that are public or part of regulated industries, meeting regulatory requirements is costly. IAM can streamline compliance processes and provides many of the controls auditors look for, thus helping you to achieve compliance with less effort.

The following section will discuss details about how IAM simplifies and streamlines compliance processes to help organization meet legal and industry regulation requirements while cutting costs and reducing effort.

COMPLIANCE

Regulatory compliance is now a fact of life for a growing number of organizations around the world due to increasing security and privacy concerns. Dozens of government and industry regulations deal with security and privacy, including SOX, PCI, HIPAA, FISMA, GLBA, NERC and MAR. Organizations are struggling to comply with a complex set of controls that have an impact on every department. To keep pace, they must consider the following:

- Do we adequately protect sensitive data?
- Can we detect unauthorized access?
- Are our controls documented?
- Can we meet and prove compliance?

An IAM solution can ease compliance efforts significantly by automating and streamlining manual processes, providing a detailed audit trail and eliminating or reducing security risks. IAM solutions:

- Reduce the risk of human errors.
- Increase end-user productivity by offsetting additional controls that may have been introduced.
- Reduce the burden on IT incurred by compliance demands.
- Eliminate passwords and simplify related controls.
- Automatically maintain a detailed audit trail for reporting purposes.

Although not every organization has compliance requirements, all organizations can benefit from streamlining identity management.

SINGLE IDENTITY

IAM consolidates user management and provides employees with a single identity that is used across all applications, which makes it easier to manage access controls and maintain a detailed audit trail for each employee.

ELIMINATION OF PASSWORDS

IAM makes it easy to enforce company-wide password policies for password strength, expiration and reuse. And for applications that support SAML, passwords are completely eliminated since SAML uses digital signatures to establish trust between the identity provider and the application.

AUDIT TRAIL

The centralization of access control produces a consolidated audit trail that can be used for compliance usage reporting and investigation of breaches.

SEGREGATION OF DUTIES

Separation of duties is a security principal that helps to eliminate fraud and errors by disseminating tasks and associated privileges for business processes among users. Many compliance mandates require organizations to demonstrate Segregation of Duties. Because IAM simplifies and consolidates user management, the solution makes it much easier to show segregation of duties, speeding up and lowering the cost of compliance audits.

CONCLUSION

As today's security landscape becomes more and more complex and varied, organizations must do more to protect their important data than simply rely on their employees to create unhackable passwords or erect a firewall around their critical business apps. They must find ways to ensure security, without driving up the costs of compliance or decreasing employee productivity by weighing them down with security-related tasks. IAM is extending the genius of single sign-on to include multi-factor authentication, streamlined application management, and simplified compliance, helping organization in any industry cut costs and improve productivity. As the leader in IAM solutions, OneLogin foresees the elimination of traditional passwords in favor of a single user identity, and the sudden unemployment of many a hacker.

* Source: Mandylion Research Labs, "Enabling Compliance with Password Policies," http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm