happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Is Identity Critical For An Organization?

Happiest People . Happiest Customers

Contents

Abstract

Is identity critical?

What if one day you wake up to realize that someone else, posing to be you, have used your VPN to access your work and also logged in and transacted in your bank account? Rather scary, right? That is precisely why 'identity' is important. Identity and access management ensures that right resources are accessed at the right time by the right individuals for the right reasons.

Implementing the right Identity and Access Management (IAM) solutions are thus extremely important for an organization to manage authorization and privileges. IAM solutions if implemented effectively helps increase security, decreases investment in time and money, enhances worker productivity by automating tasks that used to be manual and recues integration friction.

Today IT departments are struggling with system complexity and inefficiencies on all fronts. User administration, help desk activities, and application development & maintenance take huge bites of lean budgets. Inefficient user administration leads to lost productivity and higher costs. Security flaws risk identity theft and fraud. IT managers struggle to meet stringent auditing requirements driven by new federal regulations. In this difficult environment, all IT Projects are expected to justify themselves on a cost-benefits basis.

What are market analysis and survey reports stating?

Here are few key market IAM analysis and survey from various sources:

Gartner : Many enterprises that have implemented IAM technologies remain dissatisfied with the performance of these technologies and the results of their IAM programs. This dissatisfaction is driving them to consider alternative IAM vendors or alternative IAM approaches By 2014, discontented large enterprises have been considering major upgrade decisions to switch IAM vendors. (Possible to know from author when this was quoted? Given that one is in 2015)

Forrester Research: Business owners are keen on SaaS services to get quicker wins, and CIOs are finding these services attractive for cutting costs as well. Identity provisioning will look quite different in the era of cloud services.

One more: The extended enterprise is here, but current security architectures are ill-suited for the task of securing the extended ecosystem. Security and risk professionals must adopt a new mindset for security.

Ponemon Institute survey on Identity Compliance:

- 58% of companies use mostly manual methods to monitor identity and access
  -Many firms are using paper-based processes and workflow to review access, driving costs up significantly.
- 87% of companies employ a decentralized approach to identity and access management compliance
- The majority of firms focus their compliance related efforts only on applications and business units that are subjected regulatory and industry mandates
- 51% of companies use detective controls to mitigate identity-related compliance issues
- Many firms still do not know if compliance issues exist until found during an audit

Cloud, mobile and social media will continue to impact Identity and Access Management in the market.

What are the business and IT risks?

Organization compliance and operational risk increases dramatically when users have inappropriate or excessive access to information resources.

Compliance and regulatory risk

- Effectively managing and tracking who has access to critical data is a requirement of nearly all government and industry mandates.
- Failure to comply with such mandates could lead to costly remediation, restitution or even fines – distracting management from core business issues

Operational risk

- Insider threat when compounded by the inability to monitor access entitlements leads to exposure of confidential informa tion or unauthorized execution of business transactions.
- Unintentional errors and mistakes by those with inappropriate access can lead to data loss or operating failures similar as deliberate attacks.

  Third-party outsourcing arrangements pose an inherent increase in access related risk to information system

Importance of IAM strategy

A good IAM system is a must have feature in every organization is they want their resources to be secure. Enterprises should undertake proper research while choosing solution keeping future extensions in mind. Most of the IAM solutions are failures because of their inability to satisfy the current market requirements and technology integrations. The reasons vary - incorrect choice of products, product limitations or ineffective architecture design.

Few important points to consider:

- IAM is more of a business and process issue than technology.
- The success of an IAM solution depends on developing a strategy that is aligned to the needs of the business and considers people, process, and technology issues.
- Prior to implementing IAM solution it is important to consider the necessary business and process transformation requirements.
- Not all IAM/IDM projects are successful. IDM solutions work as basic provisioning solution. Many Apps remain unintegrated due to lack of time, money and skills.
- Businesses are changing at a rapid pace wherein cloud based or hosted Software-As-A-Service becoming necessary and attractive due to cost effectiveness and lesser time required to rollout.
- It is important to be strategic, not tactical, when planning and designing an IAM solution.

IAM technology can thus be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited

-

About the Author

Sandip Gupta

Experience in areas of IT security (IDAM) Consulting, Designing and Architecture. Nearly 11 + years of IT application development & implementation experience. Working as SME / Architect in the IMSS IAM security practice, HappiestMinds Technologies, Bangalore, India.

Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Business Contact:business@happiestminds.com
Visit us: www.happiestminds.com

Follow us on