simeio

EBook

5 REASONS WHY IAM SERVICES MAKE SENSE

GUIDE TO HOW IAM SERVICES CAN OPTIMIZE IAM INVESTMENTS, MINIMIZE RISKS, & BENEFIT BUSINESS STAKEHOLDERS

WWW.SIMEIO.COM

01

INTRODUCTION

Most likely you've been sent this e-book by a CISO trying to convince you to sink several thousands of dollars, euros, francs, etc. into an IAM service.

They're advocating for a team of external identity experts to come in and start rubbing their mitts all over your enterprise's systems. Your CISO may even have mentioned that such an intrusion is likely to take months of disruptive work, sweeping policy re-writes, and other lovely things sure to make life difficult.

You might not want that, but you need it.

Your enterprise has grown successful enough to retain a technology expert. That's fantastic news for the future prospects of your company. But navigating through the modern digital marketplace is too much for one person.

Let's get you convinced that contracting out to an IAM service will ensure a colossal ROI. Prepare yourself for boosted efficiency, frictionless user-experience, watertight security, and untold cost savings.

1 SECURITY

The average cost of a US data breach is over $8.5 million (1). Far too often, companies wait until they suffer the financial, legal, and customer trust losses of a breach before investing in a suitable defense. This doesn't just mean meeting compliance needs, but marshalling security measures across your entire attack surface.

In the past, companies had to strike a compromise between efficiency and security, but modern IAM services now use one to enhance the other. But by instituting a central identity platform that oversees Access Management, Customer Identity and Access Management, Identity Governance and Administration, and Privileged Access Management all from a single pane, you can control and monitor all aspects of your Identity Fabric.

Coupled with automatic policy enforcement and oversight, potential hackers are instantly pinged and locked down. IAM service teams understand that planning what to do in the event of a breach is just as important as preventing them, drawing up and enacting fine-tuned remediation plans.

ON AVERAGE YOU WILL LOSE

$8.5 MILLION

PER DATA BREACH

1 Cost of a Data Breach Report 2020, IBM Security

2 EFFICIENCY

Put yourself into the shoes of your CISO. They oversee the complete fabric of your digital presence on and offline. If your systems have been in place for years, chances are that there's a number of things that you could be doing better.

But you can only get so far on your own. Unless your system is a bespoke platform designed to change with your needs, it likely is picking up inefficiencies with every new application stapled onto it.

Eventually the whole apparatus becomes so riddled with incompatible applications, outdated protocols, and countless identities that it ceases to be of any use. 54% of US office workers report wasting time searching their cluttered systems for important files (1). Inefficiencies like this can cause 20-30% loss in potential revenue (2).

An IAM service brings in expert teams to assess, advise, implement, and maintain your identity platform for as long as needed. Instead of instituting a "fire and forget" solution, identity teams build you a bespoke platform tailored to your immediate and future needs.

ORGANIZATIONS COULD LOSE

20-30%

IN REVENUE DUE TO INEFFICIENCIES

1 More than 50% of office pros spend more time searching for files than on work, Tech Republic
2 5 Ways Your Business Processes Could Be Hurting your Business, Forbes

3 USER-EXPERIENCE

Whether you're a non-profit or a business, you want your users to have an easy time interacting with you. Every stumbling block they encounter is another incentive for them to give up and navigate away from your site with a bad taste as their only memory. The issue is so common that 55-80% of all online shoppers leave without completing their purchase (1).

You might think this extends only to customers, but your internal users need a good experience as well. Every point of friction builds up like carbon in an engine until the whole thing is gummed up.

IAM services recognize the vitality of experience for all users. By designing and rolling out a platform capable of handling the needs of both internal and external users, you stand to boost your profile as a customer-friendly and employee-minded enterprise.

When a customer's first interaction with your online systems is positive, you stand out against the sea of enterprises in the best way possible. When 57% of customers will abandon a brand after only one or two negative interactions (2), you cannot afford to neglect user experience.

57%

OF CUSTOMERS ABANDON A BRAND AFTER A BAD EXPERIENCE

1 Complete List of Cart Abandonment Statistics: 2006-2023 , Barilliance
2 Digital CX Research Report, NICE

4 SAVINGS

The average manual password reset costs companies $70 each, with between 30% and 50% of all IT help desk calls dealing with password resets(1).

Think of how much a company saves by automating this one facet of identity.
What about unused applications? Do you know how many software subscriptions your company isn't using but continues to pay for? In 2019, companies in the US and the UK spent $34B annually on unused applications (2).

Automatic curation removes this drain.
Then there's the savings on compliance and regulatory costs, up to 85% time savings on account provisioning, and up to 60% reduction in help desk tickets from IGA solutions (3).

Managed Identity Services yield all of these savings and more. According to the Simeio price calculator, a business with 5,000 employees, using 25 applications, with employees accessing just 5 applications each month would save the company over $600,000 a year. At 20k users, you stand to save around $2.5 ML.

MANAGED IDENTITY CAN SAVE YOU AN AVG. OF

$2.5 MILLION

A YEAR*

1 How Much Are Password Resets Costing Your Company?, Okta
2 6 Ways Identity Management Saves Money, Sath
3 Simeio and Saviynt Partner Brief, Saviynt
*Calculated using the Simeio Identity Savings Calculator

5 METRICS THAT MATTER TO KEY STAKEHOLDERS

Risk - Hardening your risk posture against system failures and bad actors.

Audit & Compliance - Meeting or exceeding industry standards year after year.

Security - Automatic policy enforcement, real-time monitoring, and enhanced breach remediation.

IT & Infrastructure - Seamless integration of applications into a single united system.

Human Resources - Expedited provisioning for new hires and automatic deprovisioning for outbound employees.

Advisory & Steering Committee - Current relevant data from across your entire identity fabric.

Digital Experience - A smooth user experience, not just for your customers, but your partners and employees.

TALK TO A SIMEIO IDENTITY ADVISOR TODAY!

SIMEIO SUCCESS STORIES

HIGHER EDUCATION

25 INSTITUTIONS /
875,000+ STUDENTS

40% DECREASE IN SUPPORT TICKETS

HOME IMPROVEMENT RETAIL

2500+ STORES

SLA WITH A 99.9% UPTIME

AMERICAN FINANCIAL SERVICES

FORTUNE 500 PAYMENT PROCESSOR

95% EFFICIENCY GAIN

UK FINANCIAL SERVICES

MAJOR UK BANK WITH OVER 60,000 EMPLOYEES

PLATFORM OPTIMIZED IN JUST 6 MONTHS

HEALTHCARE

31,800+ EMPLOYEES
1,731 LOCATIONS

INCREASED PRODUCTIVITY BY 9X

APPENDIX

In case you're unfamiliar, here are a few common terms in the modern identity management landscape:

IAM (IDENTITY AND ACCESS MANAGEMENT)

An IAM solution references a user's identity to determine which resources they are authorized to use, all in a single framework.

AM (ACCESS MANAGEMENT)

The process of controlling which identities has access to an organization's systems and data. This includes setting up authorized users, defining roles and rights, developing policies and procedures for granting access, enforcing security measures such as authentication protocols, and curating user access.

CIAM (CUSTOMER IDENTITY AND ACCESS MANAGEMENT)

A subset of IAM focused specifically on the profiles of customers rather than employees and partners, with an emphasis on user-experience.

IGA (IDENTITY GOVERNANCE AND ADMINISTRATION)

The active practice of provisioning, monitoring, and disabling identities. A robust IGA solution improves efficiency through automation, enforcing pre-set policies by checking privileges against the category of identity a user possesses.

PAM (PRIVILEGED ACCESS MANAGEMENT)

An access system that applies the principles of role-based access control to enforce the principle of least privilege. PAM is considered to be the highest level of identity security and management with control over all subordinate domains