simeio

Championing Identity Security in Your Organization

Leading the Identity Journey

EBook

Identity & Access Management (IAM) is not optional.

It boggles the mind that any executive in the modern age is capable of IAM (Identity and Access Management) ignorance. The task of educating the top decision-makers often falls upon security professionals who must exit their comfort zone of technical challenges and step into the interpersonal world of human-facing advocacy.

Yet the importance of a successful pitch cannot be overstated.

IAM establishes start-up enterprises and new employees and stays in the database for years after. It drives your access, your single sign-on, personalizes your applications, and remembers your favorites. Effective IAM increases efficiency, reduces risk, and ensures compliance. Managed improperly, it portends disaster.

Identity can no longer be pigeonholed into architecture and engineering or hand waved by Chief Executives (CEs) as some new security tool. It is a new framework at the Incident Detection and Response peer level. Identity and its management require the right strategy, leadership, and skillset led and fed from the enterprise.

Security professionals of any tenure know their employer's identity protection and practices can always use more polish. Unless well-funded (very few security personnel are in danger of this) the system is likely riddled with gaps and the team is too overstretched to correct it. Their task is not just to address these issues, but to convince the higher ups to provide what is needed to correct them.

If you are a security expert, then understanding how to get the CEs invested in your work is one of the most vital processes you must undertake. Let's get going.

Getting C-Suite On Board

When you expect failure, plan for success

Are cybersecurity, identity, and access management business terms or buzzwords in your organization?

An intelligent and well-informed boardroom recognizes the importance of Identity alongside Digital Transformation and Hybrid IT. Decision-makers who are ignorant (willfully or honestly) of Identity's growing import will fall behind their competitors in short order. Security directors delaying their company's identity modernization will find themselves dragged along this path to ruin when they should be leading the charge to success

Management needs to be invested from the beginning so they can see firsthand the necessity of an effectively managed IAM program.

On paper this task should be straightforward given the justification you can present. Your experiences and the metrics vindicating your claims should tell a compelling story. Chances are that your high-priority report will be ignored or given cursory consideration before being told months later that the budget can't support the problems you know need to be solved.

But as a security expert you must shoot to avoid such a catastrophe altogether. Your journey to the ears of the CEs starts with your own superior and equipping them to advocate for you.

Scout Out the Territory

Make your base secure before the attack

Start your advocacy soon (as soon as you finish reading this e-book if possible) but only after you know your enterprise's problems inside and out. Compile all the metrics on company B2B, B2C, and B2P performance, amass all the user complaints you can, and get all of it in front of your immediate supervisor.

Your next move is going to require some funding, hence the importance of having your boss aware of the symptoms of the larger problem. The initial legwork gives you a ground-level view, but the low-cost high-return investment in an IAM assessment yields a birds-eye perspective.

Randall Fields, Vice President of Customer Success at Simeio says, "I will never start an IAM Program without a 3rd party assessment in hand."

> **"I will never start an IAM Program without a 3rd party assessment in hand."**
>
> **- Randall Fields, Vice President of Customer Success at Simeio**

Aim for the Top

Be bold but intelligent in your approach

With the IAM assessment in hand, you are finally ready to start your attack run on the CEs. Prepare to present your case to management multiple times to management over the course of at least a few months. IAM advocacy is a war of attrition, one you cannot afford to grow frustrated and tired with until victory is achieved.

Your first foray into executive advocacy is to get permission (a sanity check) to start a full investigation of the enterprise's Identity fabric. Your preliminary data gathering and assessment investment puts you in a strong beachhead. Stand ready to assist your boss in achieving board buy-in. Organize the facts in the most attractive and easily-digested format possible.

Your objective is to assure the stakeholders that the ROI of what you are asking will improve processes, efficiency, security, and bottom line. Remember that these are not empty promises: effectively managed IAM delivers on all these areas.

simeio

Preparing your Pitch

One of the best ways to make C-suite understand the importance of investing in IAM is to engage them with impactful statistics. Back up your claim with data that hits them where they live, showing them the costs incurred and the efficiency raised in companies that have taken the route your are now advocating for.

$70 PER PASSWORD RESET

Reduce Costs

A single password reset done by help desk can cost the company **$70 per**. The average user requires five resets a year and 20% to 50% of all help desk calls are password-related.[1] Self service can cut these costs dramatically.

Reduce Risk

In 2022 the Identity Defined Security Alliance, reported that 84% of their respondents experienced an identity-related breach in the last year. In 2021 the average cost of a data breach increased from $3.86 million to $4.24 million.[2]

84% EXPERIENCED A BREACH

COMPLIANCE FOR SOX, GBLA, HIPPA, PCI, AND GDPR

Achieve Compliance

IAM solutions provide key tools for meeting multiple compliance standards through automatic analytics, custom-built identity controls on provisioning and federation, and highly visible policy-enforcement. These include SOX, GBLA, HIPAA, PCI, and GDPR.[4]

Improve Experience

Gartner projects that organizations which prioritize user experience will enjoy a 25% boost in satisfaction for both customers and employee by 2024.[3] IAM's automatic policy enforcement and analytics play a major role in achieving this goal.

25% BOOST IN SATISFACTION

1. https://www.forrester.com/report/best-practices-selecting-deploying-and-managing-enterprise-password-managers/RES139333
2. https://www.idsalliance.org/connecting-cybersecurity-and-managing-identity/
3. https://www.gartner.com/en/articles/iam-leaders-plan-to-adopt-these-6-identity-and-access-management-trends
4. https://blog.plainid.com/7-identity-access-management-compliance-standards

Remember your Mission

> An open and discerning mindset willing to earnestly listen to special interests adds value to the overall effort

Don't forget your goals

Be prepared for a quick reversal of interest (and unsolicited input) once buy-in is finally achieved and the cogs starts moving towards your IAM implementation. You can choose to view this as an annoyance or embrace it as an opportunity. An open and discerning mindset willing to earnestly listen to special interests adds value to the overall effort. Just do not let any one of them steal the show. You are the commander in this push, not them.

While one area or department might be the starting point, do not let the program become siloed. Any suggestions made by the various players should be to improve processes or make up for shortcomings in the way you do things today. Do not allow little wish lists to take you off target.

On the flipside, apathy will also be replaced with active hostility to your program as it takes shape and gains momentum, you will have doubters and others who will not get on board. Fortunately, you've already anticipated this by getting the CEs into your corner, so their grumbling will remain impotent and largely inconsequential. But this is an opportunity as well: consider their critics as earnestly as you would your supporters. Besides highlighting issues you might otherwise have missed, letting your opponents know they are being heard may well bring them around.

simeio

Prepare for Collateral Damage

Things break during big operations

Support from the higher ups becomes even more important as the implementation gets underway and your systems, inevitably, burst into flames. You are restructuring your company's most vital systems and, like knocking down asbestos-saturated drywall, breaking things is part of the process.

Do not neglect this facet of your work in the initial runup. Make certain that your CEs know that during this process they shouldn't count on their systems staying stable. Initial enthusiasm will waver as users learn just how difficult the implementation is. This is regardless of the exponential ease which will eventually be achieved. A stall at this stage is something to dread and avoid.

Counterattack with a series of highly visible early wins. Get manual processes operational, then circle back to address specific pain points. If changing something drastically interrupts service then shift your focus elsewhere until you have a workaround ready to go. *Balancing efficiency against the perception of efficiency can be frustrating. But it's better to keep stakeholders happy enough in the short term that you can see the multi-year IAM marathon through to the end.*

Conclusion

Do not retreat from captured ground

Keep up your IAM advocacy even during implementation. Affected departments need to know that the bumps along the way are worth the final rewards.

For the first time since perhaps the introduction of mobile devices, CISO has a business-enabling function within their organization. If you have the ambition and will, IAM is your chance to stop being the “Abominable No Men” in security. You'll become business class enablers and seize the prestige your expertise deserves.

Lose out as a passive participant or win glory as a problem solver. Your call.

Get your IAM Assessment

A full IAM assessment is vital to your goal of a successful digital transformation. Simeio provides end-to-end support for both assessment and implementation, supporting every step from advocacy to maintenance.

TALK TO A SIMEIO IDENTITY ADVISOR NOW AT WWW.SIMEIO.COM

simeio