Economics of Identity and Access Management: Providing decision support for investments

Ishaq Azhar Mohammed

Sr. Software Engineer & Department of Information Technology

London, UK

Abstract- *The main purpose of this paper is to explore how Identity and Access Management is an important asset in economics especially in decision making to support investments. Identity and Access Management (IAM) is a major driver for corporate companies, as it facilitates digitization, security management, and regulatory compliance. Many organizations, unfortunately, have difficulties with Identity and Access Management [1]. The emphasis of debates on IAM is placed squarely at the operational level, instead of the strategic decision-making level. Organizations are facing a growing number of internal and external vulnerabilities and threats; resources and budgets are insufficient to handle them all. Decision-makers (e.g., CIOs, CISOs) must decide which projects and initiatives to prioritize and support in the justification of investment requests. This is true for IAM investments against other potential security or commercial initiatives that the company might make. Various strategic goals of interest, including security, agility, assurance, productivity, compliance, and empowerment, are influenced by a variety of potential IAM investment choices in this situation [1]. This system and approach enable companies to solve this enormous issue that they face and arrive at an appropriate model, with the assistance of a decision-support tool. To find a perfect investment opportunity, a proposal that has been developed in partnership with security and IAM specialists relies on both economic modeling (where it considers decision-makers' expectations among the various outcomes) as well as system modeling and simulations to pinpoint probable outcomes [1]. For example, in this research study, there will be a demonstration of how the IAM approach has been used in a corporate environment and the context of key corporate operations. This is still in the work but achievements and future actions especially in the U.S are discussed.*

Keywords: *Identity and Access Management (IAM), Identity and Access Management strategy, IAM investment*

I. INTRODUCTION

Robust, sophisticated IAM is developing as a fundamental feature in the application economy, an essential method to drive improved application innovation while ensuring strong protections around critical assets and services. The sections that follow provide an overview of some of the commercial advantages that advanced IAM may provide [2]. The need for sophisticated identity and access management (IAM) capabilities continues to increase in urgency and breadth, as do the difficulties associated with doing it correctly. Service providers may profit on a sizable market opportunity by assisting corporate clients with their essential IAM requirements. The IAM market's changing problems and needs are examined in this white paper, which is based on a comprehensive poll of corporate security executives.

IAM in corporate IT is concerned with establishing and maintaining the roles and access rights of specific network entities (people and devices) to a range of cloud and on-premises services [2]. The many people and/or devices that use the system include consumers, suppliers, and workers; also, there are various computing devices such as servers, handsets, cable modems, computers, sensors, and scanners. IAM systems' main goal is to guarantee a unique digital identity for each person or device [2,3]. To make sure that the digital identity remains valid across the lifetime of each person's or device's accessibility, the authentication system must be constantly maintained, updated, and monitored [3].

As a result, the overall objective of identity management is to provide access to the business resources to which people and devices have permissions in a particular context [4]. This comprises onboarding users and devices, access authorizations as well as prompt offboarding of end-users and peripherals [5]. The other issue is that some people have on-and-off access to their identities. To make matters worse, people all have so many passwords, which means it is easier to store them between online accounts and leads to security issues [6]. Administrators using IAM systems have access to a wide array of features that help with managing a user's role in a website, activity tracking, and policy implementation continuously. These systems are intended to manage user access throughout a whole organization while also ensuring compliance with company rules and regulatory laws [7,8,9].

The application economy is new competitive ground for today's companies [10]. Success in the marketplace is heavily reliant on whatever business apps a company has. As companies' customer needs become more and more unique, they will have to provide personalized, outstanding user experiences – and they will have to roll out these new offerings even faster [11]. More companies have transitioned to using remote workers and granted those workers access to their security protocols as well. Digital change is rapidly advancing, and identification has now become the primary pillar for acquiring, managing, and retaining customers [12]. It is increasingly essential and prevalent every day for companies to get sophisticated identity and access management (IAM) solutions. Using service providers to assist corporate clients to meet their key IAM needs may greatly increase their market share. This paper will explore in detail how Identity access management is helping businesses to be competitive in the economy and address evolving challenges. The study also goes through some of the most major impacts for business owners, highlighting the most intriguing opportunities for providing new or improved IAM capabilities.

II. PROBLEM STATEMENT

The main problem that this paper will solve is to understand how the economics of Identity and Access Management involves its significance in providing decision support for investments. The conventional emphasis of identity and access management (IAM) in the business has been on maintaining user information systems identities. This has made things more complex, as we see more of various kinds of identities and accounts, especially in cloud, mobile, as well as other technologies like e-commerce, and social media networks [12]. In the context of cloud services, digital, virtual, and individual networks, interfaces, service providers, and technologies are not typically covered by corporate IAM include identity, platforms, services, and capabilities. Fragmented user authentication and authorization are the by-products of this implementation. IAMs, identity tokens, and other types of identity relate to it, yet there is no such thing as one kind of identity, identity token, or recognition [12,13]. On the other hand, managing many identities has turned into managing multiple identities, and people and businesses alike are constantly challenged by their identity complexities.

III. LITERATURE REVIEW

A. A review on IAM: Its Definition, and How Critical It Is

IAM relates to a high-level development, administration, use, and enforcement of digital identity regulations [13]. IAM is made up of both procedures and supporting services and infrastructure. Businesses may provide seamless, centralized monitoring and monitoring via sophisticated IAM. Storing user credentials, such as passwords or digital signatures, has historically been required to ensure a user's or device's identification, and these techniques include login credentials, password protection, hardware tokens, as well as smartphone application tokens [14]. Because of these newer token-type implementations, one can find applications from Google, Cisco/Duo, Microsoft, Authy, and many more IAM providers on both iOS and Android devices. in addition to using biometric authentication components, identity management systems can incorporate functionality for the Fast Identity Alliance (FIDO) [14]. The computing world is increasingly complicated, and as a result, it presents new security risks. Strong usernames and passwords are no longer enough. While a few changes have been most noticeable, IAM (Identity and Access Management) solutions have been augmented with multi-factor authentication (MFA) [14]. Biometric technologies, artificial intelligence, as well as machine learning are being used in identification systems nowadays.

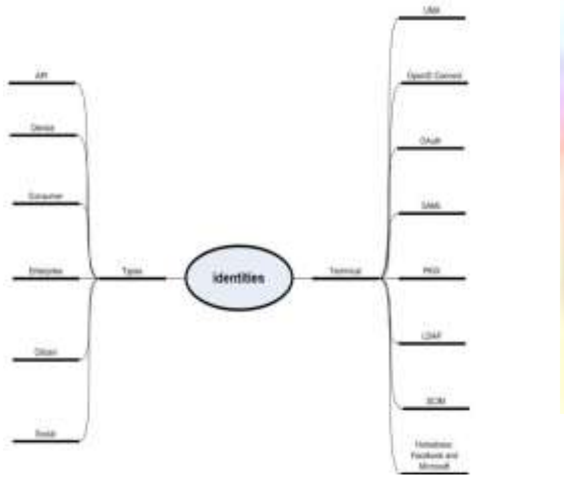
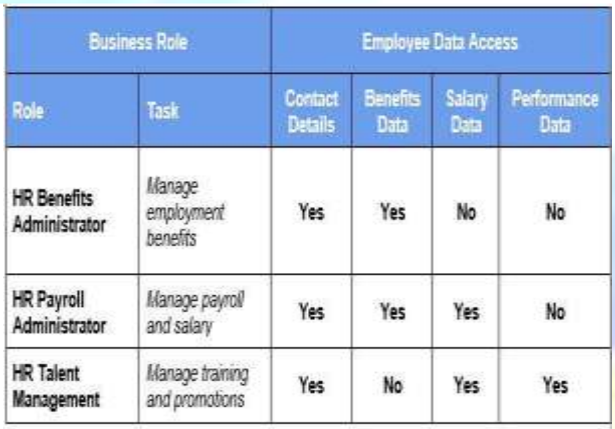


Figure 1. Various identities types and technologies

B. The need for IAM is critical

A whole new set of security needs has arisen in today's fast-moving corporate and IT environments. Companies have shifted away from enterprise on-premises settings to cloud-based ecosystems that include data analytics, mobile apps, the Internet of Things (IoT), and much more. [15]. What has happened is that vulnerable assets and systems are being linked to one another, and more and more are vulnerable. Security systems and procedures used to be built on the idea of a barrier. It's next to difficult to draw clear boundaries between internal and external nowadays, especially when it comes to security. Additionally, companies are being attacked by hackers, which may originate from nation-states or sophisticated criminal groups. Big data violations are still news and companies are still being plagued by ransomware, spear shelling, and many other dangers [15]. A considerable and continuous commitment of resources is required to fight these risks, yet compared to the substantial penalties regarding data breaches, these expenditures seem negligible. Additionally, privacy laws and compliance requirements are only becoming more stringent, which causes these fines to become even more costly.



Business Role		Employee Data Access			
Role	Task	Contact Details	Benefits Data	Salary Data	Performance Data
HR Benefits Administrator	*Manage employment benefits*	Yes	Yes	No	No
HR Payroll Administrator	*Manage payroll and salary*	Yes	Yes	Yes	No
HR Talent Management	*Manage training and promotions*	Yes	No	Yes	Yes

Fig ii: Use of IAM for HR.

C. *How advanced IAM can be a business enabler*

A robust, sophisticated IAM is becoming more important as a basis for enabling increased application innovation, while also ensuring that critical assets and services are adequately protected [16]. Here are some of the commercial advantages that come with advanced IAM:

D. *Facilitate adoption of cloud services, while establishing required controls*

The current transition to the cloud has been swift and widespread. Within the organizations, business leadership, with little if any, engagement from IT, mainly contributed to the development of cloud computing. This leads to a lack of coherence of rules and monitoring across business data, systems, and operations [16]. The growth of so-called 'shadow IT' exposes companies to missed compliance audits and violations of security. Corporate IT personnel should support this transformation while providing the protections required to manage security and compliance concerns. In achieving these goals, IAM can play an important role. IT teams may provide end-users the comfort of using a single login to access across important e-commerce websites, whether they are using these services on the cloud or in the workplace, via their federalized identities and Single Sign-On (SSO) features [16]. This makes it easier for users to reduce the problems associated with repeated logins, lost passwords as well as resets. These features may simultaneously provide security managers with substantial efficiency and control benefits. The security personnel may build a uniform, centrally controlled authentication process, administration, and auditing processes and system via universal recognition [17].

E. Improve the customer experience, user productivity, and security

Applications are becoming more sophisticated in the application economy. To enable a client to execute transactions, a sophisticated infrastructure of various systems and suppliers may be engaged to offer intelligence, data, and processing [17]. This complexity will almost certainly continue to grow, but we must do all we can to keep the user experience simple. To provide a satisfying experience, each domain a combined system includes must have separate authentication requirements. A complicated or time-consuming authentication procedure may damage customer loyalty, the volume of transactions, and income for user services. A deficient user experience may either impede productivity or raise company risk for employee-oriented apps – if a process turns out to be too much a burden, users frequently attempt to bypass rules and policy. IAM makes it possible to have more excellent control, improved security, as well as a better user experience by allowing federated identification and single sign-on (SSO). SSO improves the comfort of employees so that users get access with a single access point to all their apps. Federated identities enable managers of IDs and access rules to use a centrally managed method [18]. Sophisticated IAM services also allow the idea of bringing their own identities to them so that clients may register or sign up to the website of a company using their Social media platform credentials, rendering it even simpler for them to interact with and negotiate with the company [18].

F. Strengthen business and application agility

Companies are increasingly using APIs, outsourced development, and DevOps methods in their efforts to provide engaging, creative apps for their customers' demands. To respond to requests for quicker delivery of security applications, the management of uniform lifecycle policies throughout the production, testing, backup, and disaster recovery settings is more and more essential. By using sophisticated IAM functions, companies may customize rules and protections for particular applications and maintain centralized visibility and control [18]. With powerful IAMs, companies may manage external contacts more efficiently, for example by engaging with software development organizations, so that they can optimize their cooperation while protecting their access. Operational efficiency improvement IAM services must operate effectively at all times because of their core, essential position in a company. IAM can need a lot of continuous work and considerable budgetary, personnel, and time strain. IAM stands for an endeavor that has never been completed.

G. What IAM entails in terms of compliance

By offering tools to establish complete security, auditing, and access controls, IAM systems may enhance regulatory compliance. Several technologies now provide elements that guarantee compliance by a business. Many countries compel companies to take responsibility for the maintenance of identification. Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA all deal with establishing corporate accountability by keeping an eye on the distribution of consumer and employee data. Organizations may use identity management systems to help them comply with regulatory requirements. The GDPR demands robust security measures and user access restrictions [19]. The GDPR requires companies to protect EU residents' and enterprises' sensitive information and confidentiality. Adopting the appropriate measures has been taken in many US states. To ensure compliance, one ought to automate various elements of IAM and guarantee compliance of their operations, procedures, access permissions, and requests [19].

IV. FUTURE OF IAM

Many US businesses are no longer able to properly handle the changing dynamics of their own identity and access management (IAM) constraints. With the fast development of the IAM environment, security and digital platforms must strengthen their identity verification methods, build better compliance monitoring abilities and minimize the threats of an ever more dispersed workforce. Enterprises require the skilled resources and expertise necessary to design, develop, purchase, and deploy complete identity and access management systems. This has led to their hiring the support assistance of professional service companies to help with many tasks all at once. The reliability and implementation of MFA policy by way of time-sensitive PIN codes have been extended to Universal one-time password (OTP) providers like Google Authenticator. Universal OTPs also eliminates the need to provide their unique MFA technique for every single resource.

V. BENEFITS OF IAM GLOBALLY

Several companies have benefited from advanced IAM systems, particularly ones that house several departments. IAM services assist businesses in working in compliance with framework changes. Additionally, they assist in resolving computer intrusions and theft. This helps to save both time and money. IAM's capacity to simplify complex login processes will boost global sales of the product. In addition to decreasing complexity, IAM services provide total quality management. IAM also has the advantage of managing passwords, directing services, and authentication. The capacity to improve the entire administration of IAM solutions will stimulate market growth and therefore promote the development of the industry.

Although IAM is not new, it is a good place to start for service providers. As the aforementioned figures indicate, the IAM market can produce a big volume, and it is anticipated that the industry would expand. Through the provision of sophisticated IAM services, suppliers may meet big needs, manage enormous size, and position in a market with considerable development. Network operators with the knowledge required to engage with clients and develop plans and strategies that will enable them to improve their IAM maturity will provide substantial value and position themselves effectively in a rising industry. The increasing use of sophisticated technology in recent years has brought forth numerous product developments. Enhanced software and optimal efficiency were achieved via modern technologies. Authentication and authorization systems demand is not only confined to companies but may also be extended to other important areas. The technology not only monitors workers' identities but also helps a company function inside the framework and regulations established worldwide by governments.

VI. CONCLUSION

This paper addressed the economic advantages of IAM in terms of supporting investment decision-making. The findings from this research demonstrated that the main purpose of IAM is to guarantee that every identity has access to, and in the appropriate perspective, adequate support (applications, databases, networks, etc.). In recent decades, the IAM industry has seen strong competition. Considering the enormous potential of the IAM market in several industrial areas, businesses are increasingly investing in this industry. Increased investment will help to promote growth in the economy in the research and innovation of new and enhanced IAM products. To build a market base, other businesses concentrate on improving their operations and improving their portfolios. The top firms in the industry have emerged, amongst others, Amazon, IBM, Microsoft, and Oracle.

REFERENCES

[1] M. Yearworth, B. Monahan and D. Pym, "Predictive Modelling for Security Operations Economics", *Workshop on the Economics of Securing the Information Infrastructure (WESII)*, 23–24 October, 2006.

[2] M. Casassa Mont, Y. Beres, D. Pym and S. Shiu, "Economics of Identity and Access Management: A Case Study on Enterprise Business Services", *HPL Technical Report HPL-2010–12*, 2010.

[3] Y. Beres, J. Griffin, S. Shiu, M. Heitman, D. Markle and P. Ventura, "Analysing the Performance of Security Solutions to Reduce Vulnerability Exposure Windows" in ACSAC, CA:IEEE, pp. 33-42, 2008.

[4] M. Collinson, B. Monahan and D. Pym, "Semantics for Structured Systems Modelling and Simulation", *Proc. Simutools 2010. ICST: ACM Digital Library and EU Digital Library*, 2010, ISBN 78-963-9799-87-5.

[5] Y. Beres, D. Pym and S. Shiu, "Decision support for systems security investment", *Proc. BDIM 2010*, 2010.

[6] M. Martinsons, R. Davison and D. Tse, "The balanced scorecard: a foundation for the strategic management of information systems", *Decision Support Systems*, vol. 25, no. 1, pp. 71-88, 1999.

[7] R. Anderson, "Why information security is hard - an economic perspective", *17th ACSAC*, pp. 358-365, 2001.

[8] M. Collinson and D. Pym, "Algebra and logic for resource-based systems modelling", *Mathematical Structures in Computer Science*, vol. 19, pp. 959-1027, 2009.

[9] L. Martin, "Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management", *Information Systems Security*, vol. 16, no. 1, pp. 9-14, 2007.

[10] C. Ioannidis, D. Pym and J. Williams, "Investments and trade-offs in the economics of information security", *Proceedings of Financial Cryptography and Data Security'09 LNCS 5628*, pp. 148-166, 2009.

[11] M. Collinson, B. Monahan and D. Pym, "A Logical and Computational Theory of Located Resource", *Jouma1 of Logic and Computation*, vol. 19, no. 6, pp. 1207-1244, 2009.

[12] A. Baldwin, M. Casassa Mont and S. Shiu, "Using Modelling and Simulation for Policy Decision Support in Identity Management", *IEEE Policy 2009 Symposium*, 20–22 July, 2009.

[13] C. Huang and R. Behara, "Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints", International Journal of Production Economics, vol. 141, no. 1, pp. 255-268, 2013.

[14] L. Gordon and M. Loeb, Managing Cybersecurity Resources, McGraw Hill, 2006.

[15] G.S. Fishman, Discrete-Event Simulation: Modelling Programming and Analysis, Springer-Verlag, 2001.

[16] C. Gunter, D. Liebovitz and B. Malin, "Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems", *IEEE Security & Privacy Magazine*, vol. 9, no. 5, pp. 48-55, 2011.

[17] A. Baldwin, M. Casassa Mont, B. Monahan, D. Pym and S. Shiu, "System Modelling to Support Economic Analysis of Security Investments: A case Study in Identity and Access Management", *Trust Economics Workshop and HPL TR HPL-2009–173*, 2009.

[18] B. Dos Santos and L. Sussman, "Improving the return on IT investment: the productivity paradox", *International Journal of Information Management*, vol. 20, no. 6, pp. 429-440, 2000.

[19] R.L. Keeney and H. Raiffa, Decisions with Multiple Objectives: Preferences and Value Trade-offs, New York:Wiley, 1976.

[20] M. Collinson, B. Monahan and D. Pym, "A Discipline of Mathematical Systems Modelling" in Forthcoming monograph, London:College Publications, 2009.