Business Growth and Development Strategy in the Era of Dynamic Communication Paradigm: A Discourse of Application Programming Interface (API)

Oresanya Oyewale Kolawole
Department of Risk & Compliance, Cellulant
Information Security & CISO Nigeria
wale.oresanya@cellulant.io
DOI: 10.56201/rjmcit.vol11.no1.2025.pg1.11

Abstract

The cardinal revolution of business growth and development is a process of transition to flexible integration of dynamic systems and platforms, distinguishing innovative methodologies in the organisation of the process of value creation and addition. There are situations of the creation of digital environments based on freely and flexibly integrating components. Based on a review of theoretical and methodological publications dedicated to the tools for building digital ecosystems - Application Programming Interface (API), there is a conceptualisation and its appreciation from a holistic viewpoint. The paper sees and discusses the emergency of API as it relates to the economy which is generally used to denote the creation of a new value based on API. The critical roles and security challenges in associated with the adoption and application of the API are specified. The article study the implementation strategies of the API for business organizational structures, and provides recommendations for adopting an API a tool of business growth and development.

Key Words: Application Programming Interface, API Security, Business Organizations, Implementation Strategies

1. Introduction

According to Iyengar, Khanna, Ramadath and Stephens (2017), Application Programming Interfaces (APIs) were once largely limited to technical domains but have now become a significant engine of business growth. As the connective tissue linking ecosystems of technologies and organizations, APIs allow businesses to monetize data, forge profitable partnerships, and open new pathways for innovation and growth.

Early adopters across industries are already using APIs to create new products and channels and improve operational efficiency. Within the automotive industry, for instance, APIs are used to embed efficiency data, driving statistics, route information and real-time alerts into dashboards. Some retailers are using APIs to set up multi-brand shopping platforms, track inventory, and help consumers locate stores. In another development, a handful of banks are partnering with fintechs and retailers, among others, to develop APIs that help customers integrate banking data into bookkeeping and investment software, and provide faster internal access to a range of account information.

Application Programming Interface (APIs) have become one of the most common buzz words in business discussions in recent times. API which is not new to the tech industry, however due to the evolution of the use of APIs they have become critical and prominent assets in today's business world. APIs are developed to fulfil wide ranges of use cases across multiple industries, APIs powers the processing of millions of transactions within the financial industry and ensure the retrieval and update of health records within the healthcare sector, just to name a few of the use cases API are leveraged for.

As Siriwardena (2014) noted, the critical role APIs play in today's world of business reinforce and necessitate the need to ensure the secure implementation and secure adoption of APIs. A compromise of an API within the healthcare sector could result in unauthorized access and disclosure of patients' records that could result in damning consequences to both healthcare provider and the patients. Irrespective of the industry, it is no surprise that enterprises are dedicating resources to ensure the security of their APIs as these are bedrocks that facilitate day-to-day business processes.

Just as with any information assets, a defence-in-depth approach needs to be taken in securing APIs. However, it all starts with implementing the basics such as adopting an API framework, implementing secure coding principles, training your development team on secure coding and leveraging efficient security testing practices that prevents shipping of vulnerable APIs to production.

Following the above, the paper is based on desk research and a scientific and grey literature review. It relies mostly on specialized consultancies although from a critical viewpoint. It attempts to track some of the key properties of APIs, to explore the essential cooperative dimension of API, so as to draw out the kind of significant relationships that exists among companies. It looks at their role in the digital transformation, attempts to assess its economic impact and dissects a modern perspectives on the API economy.

The paper is divided into three parts. The first part offers an overview of best practices for APIs security, it looks briefly into some private ecosystems, analysing the different API strategies of its players. In the context of digital transformation, Application Programming Interfaces (APIs) have become fundamental to software integration and interaction **(Simon, 2021).**

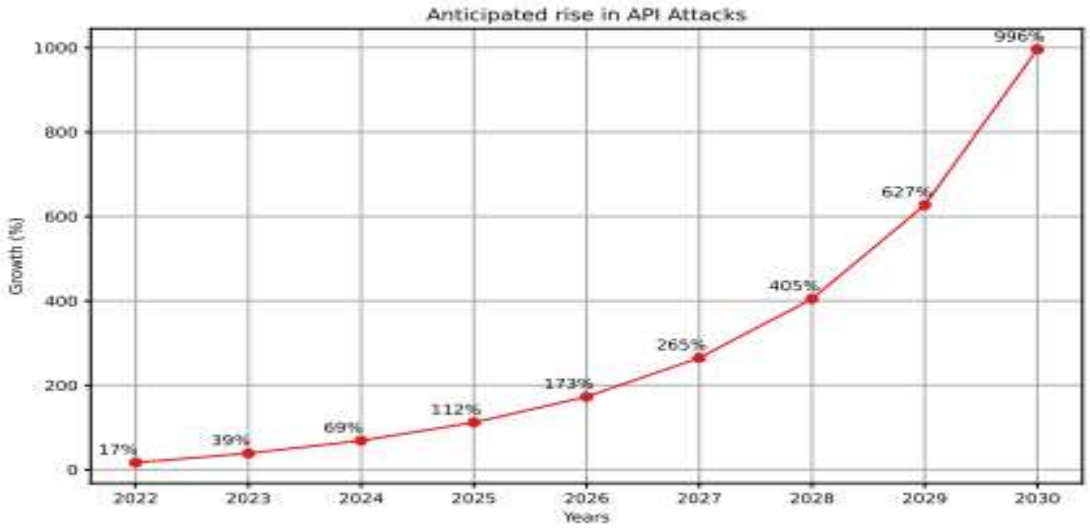
The second section investigates the critical role of APIs and its economic value (size of the market) of APIs and reviews the main benefits to be expected from APIs as business organizational enablers. The third section question the idea of an "API economy" and takes a look at some of the criticisms. The fourth part of the study centres on a discussion of APIs implementation strategies and drawing attention to conclusion and recommendations.

2. Best Practices for APIs Security

In the context of digital transformation, Application Programming Interfaces (APIs) have become fundamental to software integration and interaction. Despite their numerous advantages, APIs present significant security challenges (Türetken, 2024). The issue of the "API economy" has been triggering some hype recently, but remains somehow under the radar as the issue is both highly technical and at the same time poses a lot of security challenges because the functions of an API are rather hidden, remaining "under the hood" (MuleSoft, 2018a).

Figure 1 below highlighted the anticipated rise in attacks against APIs in 10 years starting from 2022, projected by collaboration with one of the commercial companies that provide API gateways and service meshes, and an associate professor from Brown University (Kong, 2023; Türetken, 2024). The basis year to which the numbers in the figure are compared is 2021. The growth percentage is calculated by examining the numbers from 2021 and 2022 since they have the data for 2021 and 2022. Consequently, the 17% displayed in the figure is the only percentage that is actually calculated but not projected. No detailed explanation is provided on the justification of the projection, apart from the fact that they use historical data, trends, and expert analysis, and they consider the high demand in the cyber security field recently.

Figure 2.2: Anticipated Rise in API attacks between 2022 and 2030



Source: Türetken (2024).

Some factors have been identified to be chief reasons for the anticipated attacks. The first is that many establishments do not know how to maintain their APIs against attacks. More often, many businesses, regrettably, have poverty of orientation concerning the number of APIs they possess (Qazi, 2023). In the submission of Türetken (2024), the well-known proverb fits in this context: ”You cannot protect what you cannot see!” (Team, 2019). Therefore, this portion of the paper emphasizes the significance of implementing API security procedures in general and in particular for businesses handling personal data to detect vulnerabilities and mitigate major risks therewith, system breaches, identity theft, and unintended exposure.

There are some issues and challenges ahead for the deployment of all kind of APIs. From the foregoing analysis, Simon (2021) brought forward some inherent challenges which are as follows for private and public establishments.

i. There is an uneven development across industries (traditional firms are less active than digital natives) and countries (Silicon Valley is leading).
ii. The domination of IT companies (leaders and pioneers of APIs) raises issue of competition and at some point, may prevent rather than foster innovation. The Facebook

decision is an attempt to deal with some of these issues. The UK CMA report (Competition and Markets Authority, 2020: p. 21) recommends setting up a procompetition ex ante regulatory regime.

iii. Open Data policies create a fertile environment but may have to be complemented by some regulatory interventions.

iv. There are conflicts and tensions that cannot be underestimated with developers working under asymmetric conditions.

v. Further complexity in the management of public APIs within complex heterogeneous public ecosystem is to be expected. Nevertheless, to close with a positive note, it may be still useful to use the wording "API Economy" as some kind of metaphor to account for some of these interactions, to assess the role of APIs in the backdrop of the history of services computing. Some kind of "breadcrumb trail."

3. The Critical Role of APIs

Precisely, the impact of the Corona Virus pandemic on the socio-economic and all spheres of endeavour in the society is difficult to quantify. Thus, with the new realities resulting in the distortion of the way things are done no doubt throw up new challenges on how to leave the new normal as a result of the of emergence of COVID-19 pandemic. High adoption ICT emanated as a key means of bridging the gap of challenges caused by the pandemic and responding to the new reality of the everyday life. ICT, with its reach, richness and performances holds great promises in dynamic times (Francis and PAUL, 2021). Simplifying the back end. APIs can connect internal systems relatively simply, allowing access to data—even when it's buried deep within legacy IT systems—quickly and repeatedly. This allows IT to simplify and automate tasks, and speed development.

i. Personalizing Offers

Data aggregation and on-demand reporting through APIs can enable the delivery of personalized products and services, such as user authentication, fraud management, credit approvals, paying for services with cash or points, or finding and tracking subscriptions. For instance, S&P's Capital IQ API integrates key information, including investment research, companies' financials, credit ratings, global market data, and alpha and risk models, into personalized business applications for customers.

ii. Ecosystem of innovation and engagement.

The connective capability of APIs allows companies to access new value outside the business. API developers, for example, can create innovative products and services that tie into a company's systems. Advanced API capabilities allow developers to create a richer customer experience by pulling together a deeper array of data sets (rather than simply scraping data). Salesforce.com's partner ecosystem, for example, offers a developer-friendly toolbox that has spurred partners to build a huge number of employee and customer applications that rely on APIs. As a result, more traffic comes through the Salesforce APIs than through its website.

4. A Discussion of APIs Implementation Strategies

In the research of Iyengar, Khanna, Ramadath and Stephens (2017), the following are most successful steps in the implementation of API strategies:

i. **Identify—and Prioritize—the Value**

APIs can generate massive amounts of value, but institutions first need to understand where best to apply them. Leaders in the field analyze where value can be destroyed or created, then they size the potential impact in terms of revenue, customer experience, and productivity.

Analyzing customer journeys is often the best way to identify API opportunities. One bank pulled business and technology professionals into a joint team and tasked them with identifying where APIs could help resolve several longstanding customer pain points.

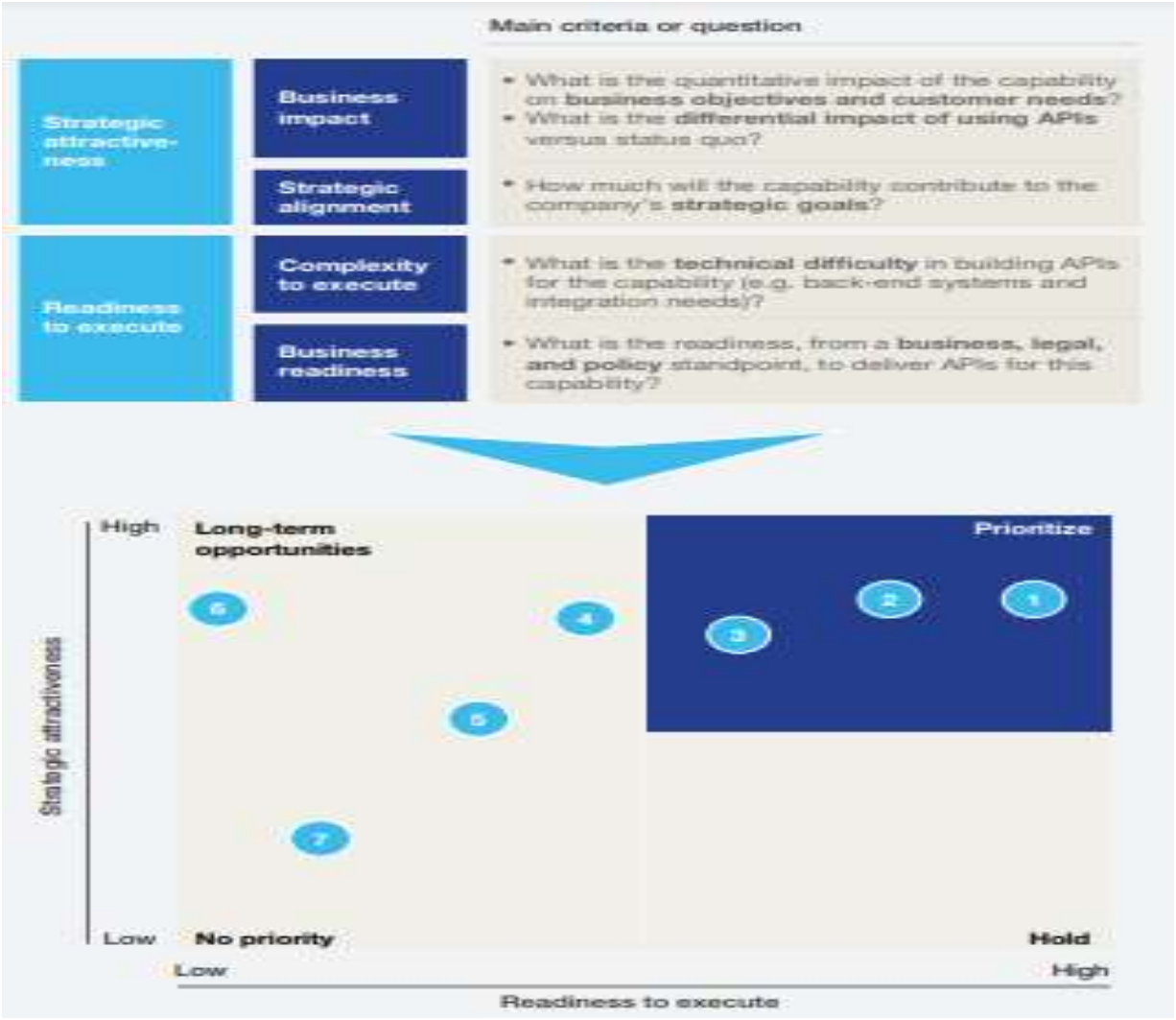
Their review revealed opportunities to develop advanced calculator APIs capable of pulling from multiple sets of data, know-your-customer APIs, and product-aggregation APIs that could help customers access needed information more quickly and cut down on form-filling requests. The team then prioritized those opportunities that would deliver the most near-term impact, given existing capabilities. That data-driven approach gave the bank greater mission clarity and built momentum for the API programme.

Understanding what it takes to develop the APIs requires a deep knowledge of the data environment, especially back-end systems where the API work is often done. Once the best opportunities are identified, API developers can identify which and how many APIs are necessary to unlock that value. A prioritization matrix can help whittle down the list of APIs based on the answers to a specific set of questions about strategic value and implementation complexity, taking technical, privacy, security, and regulatory concerns into account.

ii. **Active Management of Monetization**

With a clear vision in place, companies then need to focus on what they need to implement in order to capture the value they've identified, a step many organizations surprisingly tend to short- change. Determining what and how to charge, for example, requires quantifying how much the underlying data or service is worth (often based on how proprietary it is and its role in generating value), the revenue streams the APIs open up, and how much developers and users might be willing to pay to access them. Those answers, combined with the company's overarching strategy, will inform which monetization arrangements to pursue with different partners.

Figure 2: A Disciplined Process to Evaluate APIs



Source: Iyengar, et al (2017).

Options typically include "pay for use," where developers pay based on usage volume; revenue sharing models, where the API partner or developer gets paid for the incremental business they generate for the API provider; and "freemium," when it's strategically valuable to scale a product's or brand's reach.

In determining which monetization approach to use, providers should think about how their data and APIs can add distinctive value for different audiences. Those insights can help them put together thoughtful partnerships. The traffic app Waze, for instance, uses APIs to create a two-way exchange between municipalities and other partners to share data on road closures, accidents, construction delays, and potholes. Similarly, American Express uses its Pay with Points APIs to create mutually beneficial partnerships with merchants, arrangements that have increased retail sales, card spend, and brand loyalty.

That focus on monetization of APIs should extend to internal functions as well. Effectively using APIs can reduce operational or technology costs by simplifying and accelerating development. One bank, for instance, created a library of standardized APIs that software developers could use as needed for a wide variety of data-access tasks rather than having to figure out the process each time. Doing so reduced traditional product-development IT costs by 41 percent and led to a 12-fold increase in new releases. Seeing these kinds of tangible benefits makes it easier for business leaders to increase their expectations of their software engineers to develop better products more efficiently. Quantifying that potential value in potential savings, efficiencies, and FTE reassignment is crucial in building a business case to invest in developing APIs.

As teams implement APIs that break down barriers between systems and organizations, they can continually unlock new sources of value that weren't evident at the beginning of a project. One large financial institution, for example, used APIs to help connect systems with a wealth management institution it had acquired. One set of APIs was used to connect the interface on the web to the wealth management company's back-end systems, while another set linked the master customer data so that customers could be immediately authenticated and didn't have to re-register. The APIs greatly simplified the integration process, eliminating the need to rewrite any applications and allowing each system to operate until it was time to merge them. The organization could then offer customers an integrated solution rather than a series of individual products. For this reason, the monetization process needs active and ongoing management to continually identify opportunities that APIs create.

iii. **Creation of a Centralized Control and Organizational Approach**

Using APIs effectively requires a new way of thinking about partnerships, a new way of business It also comes with new challenges to data privacy and security (see "Opening up your APIs and keeping cybercrooks out" on McKinsey.com).

Establishing a centralized body, such as an API Center of Excellence (CoE), is crucial for overseeing API design and development across the organization. With the help of visual dashboards and related tools, the CoE can manage all the APIs in the catalog to avoid duplication, enable reuse, and assist with developer access. Effective API leadership establishes clear decision rights (about what APIs to develop, for example, or how to resolve conflicts) and identifies both what API capabilities are needed and what new APIs the business needs to evolve. At one large business, the API CoE reported to the chief technology officer.

The CoE's role in establishing security standards and protocols is especially important. These include two-factor authentication, access-management controls, and appropriate network monitoring to detect bots and other unwanted cyberactivity. A clear set of data and security protocols provides the necessary standardization to ensure interface compatibility, simplify management, and more effectively manage risk.

CoE governance also extends to managing funding requests. The most advanced organizations dedicate specific funding to develop a set number of APIs while maintaining enough flexibility to seize on new ideas that emerge. They continually vet

and reprioritize their portfolio to ensure resources support the highest-value opportunities.

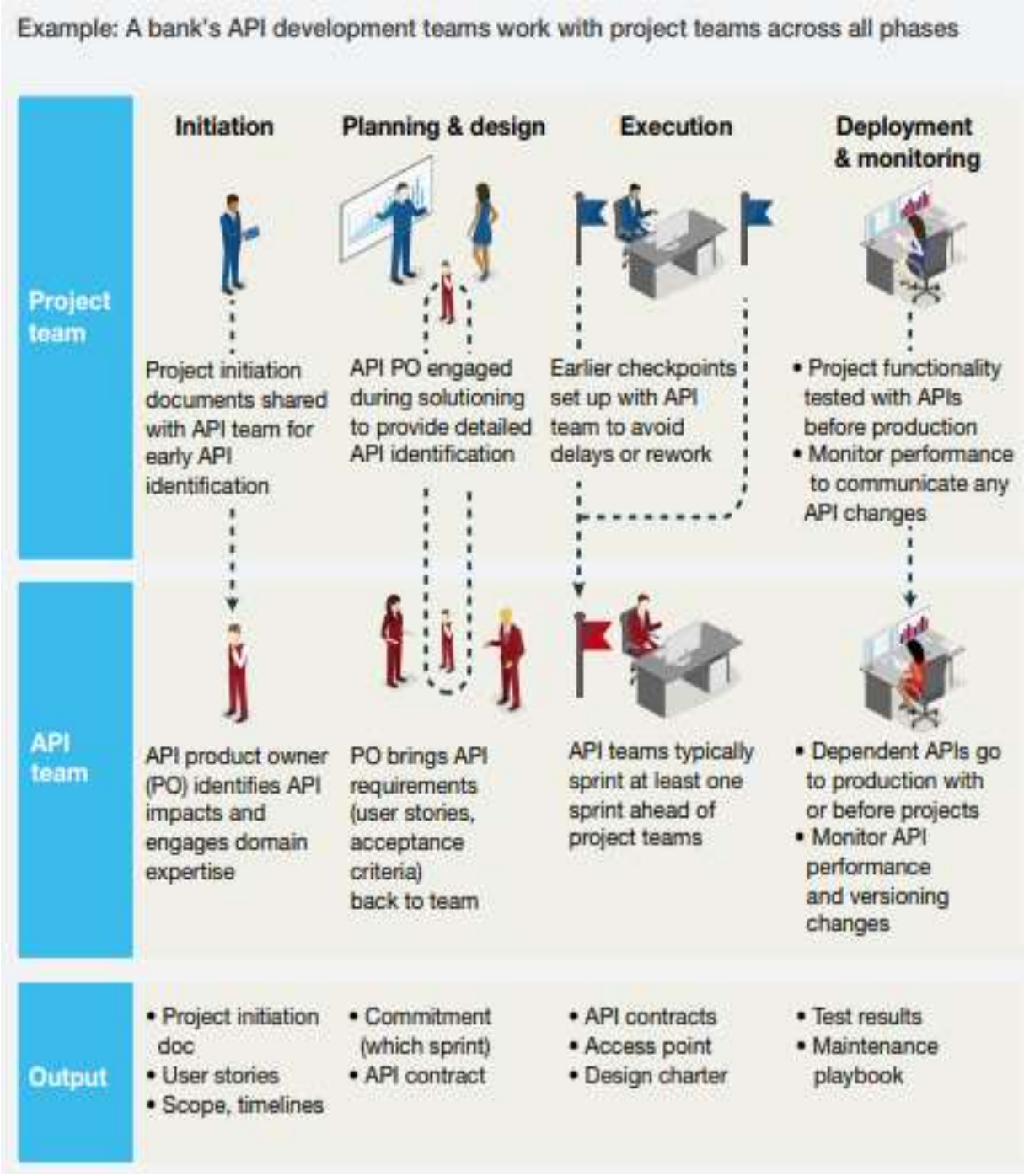
Some CoEs launch specialized hubs to court crucial developer relationships. Success requires sustained commitment to ongoing platform support and API development to maintain the confidence of external developers and partners. For example, one bank located near a hightech hotbed created an open banking platform that provides developers with access to data and payment operations that they can integrate into their own platforms and applications. The bank underlines this commitment by also providing a technical dashboard view of API usage and processing volumes, and the ability to manage API keys and access with bank-grade authentication within the digital platform.

Finally, the CoE needs to ensure that the API programme is staffed effectively. Leaders with experience directing API portfolios are crucial to establishing the necessary governance and development approach. Software engineers and use-case specialists must be able to turn user stories into executable APIs and integrate those APIs into products and systems, and "translators" are needed to convert business needs into technical requirements and help the business understand any relevant technological constraints.

iv. **Driving APIs Usage and adoption for Profiteering**

Like any product or service, a successful API programme requires a thoughtfully managed adoption campaign backed by rigorous performance management. The best approaches begin with the initial customer and developer pilots, advance to formal production requirements, then orchestrate and oversee the wider-adoption push to achieve critical mass. It's important to find pilot partners who have an appetite for innovation and are willing to invest the time. API teams work closely with project teams to continually refine and iterate the API prototype until it meets predefined performance targets (Figure 2).

Figure 3: The Development and Operations of APIs



Source: Iyengar, et al (2017).

5. Implication of the Study

There is no robust data about the size of the API market nor about its value. Sources are highly heterogeneous and delimitations not always precise. The standard metrics or indicators are hard to find. Further research would be needed to better document this area.

6. Conclusion and Recommendations

Beyond the impressive growth of the "apps economy" and its strong link with APIs "under the hood," the so-called "emerging API economy" still stands on the "hype" side and is not clearly substantiated. The notion remains a bit vague (Simon (2021). This is not surprising considering the (still) recent growth of most APIs. It may still be too early to come up with a full description of the market and its structure. Part of this difficulty may be linked to the fact that APIs are not final products/services but necessary ingredients for the production of a final service, a "wholesale" version of access to the Web. Such ingredients of the supply chain are more difficult to track in a digital economy. The value added is hard to track back.

Besides, as noted the number of firms with mature API programmes remains small. The field is dominated by new digital platforms companies and the presence of traditional firms is weak. Exporting these technologies in other kind of organizations may be a difficult task and not deliver all the expected benefits, as the case of news organization may indicate, even if it is a single example. This may constitute a barrier for a further more even deployment of APIs especially in a context of new disruptive technologies such as machine learning, AI and 5G. Furthermore, it still appears difficult for most enterprises to fully capture the value they initially envisioned from APIs. This is not surprising either, a similar situation was found for Big Data (De Prato and Simon, 2015) and AI (Simon, 2019). The cases of the companies of our sample of digital natives cannot be held as representative neither give clues for the way to anticipate further deployment and growth in other sectors.
It is important to note that securing your APIs is not a one-off activity; it should be a continuously evolving process with focus on continuous enhancement of the security posture of your APIs considering the holistic context of your organization. The following are recommended.

i. Enforce authentication and authorization for all calls to your APIs
ii. Encrypt data transmitted via your APIs
iii. Enforce rate limiting on your APIs
iv. Implement data minimization control
v. Implement data validation controls both on client and server side
vi. Enable logging for your APIs
vii. Leverage API gateways and firewalls
viii. Conduct periodic penetration testing of your APIs to proactively detect and remediate vulnerabilities.

References

De Prato, G. & Simon, J. P. (2015). The next wave: 'big data'? Communications & Strategies, 97, 15 – 39

Francis, O., Orokpo, E., & PAUL, S. O. (2022). ICT in post Covid-19: exploring the new normal for achievement of sustainable development goals in Nigeria. *International Science Journal of Management, Economics & Finance*, *1*(5), 46-54.

Iyengar, K., Khanna, S., Ramadath, S., & Stephens, D. (2017). What it really takes to capture the value of APIs. *McKinsey & Company*.

Kong, C. (2023). API Infrastructure is Mission Critical — and Increasingly Under Attack. Retrieved from https://konghq.com/blog/enterprise/apis-are-mission-critical

MuleSoft (2018a). Connectivity benchmark report 2018. Accessed from www.mulesoft.com/ty/report/ connectivity-benchmark.

Onechojon, U. T., Ojonemi, P. S., & Mark, O. (2013). Green Audit and Environmental Sustainability in Nigeria: Unveiling Corporate Perspectives. *International Journal of Public Administration and Management Research*, *2*(1), 101-111.

PAUL, S. O., & Ofuebe, C. (2020). Unabated corruption in the government of Nigeria despite the Economic and Financial Crimes Commission: Who Bells the Cat?. *Society & Sustainability*, *2*(2), 45-58.

Paul, S. O., Yakubu, A., & Apeh, G. I. (2020). Obasanjo's administration anti-corruption campaign in Nigeria and salient governance implications. *Journal DOI*, *6*(10).

Paul, S. O., Yunusa Igono, P., & Apeh, G. I. (2021). Language Determination in Politics. *World Affairs: The Journal of International Issues*, *25*(2), 138-158.

Qazi, F. (2023). Application Programming Interface (API) Security in Cloud Applications. EAI Endorsed Transactions on Cloud Systems, 7(23), 1–14. Accessed from DOI: 10.4108/eetcs.v7i23.3011

Shishmano, K. T., Popov, V. D., & Popova, P. E. (2021). API Strategy for Enterprise Digital Ecosystem. In *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 129-134). IEEE.

Simon, J. P. (2021). APIs, the glue under the hood. Looking for the "API economy". *Digital Policy, Regulation and Governance*, *23*(5), 489-508.

Simon, J.P. (2019). Artificial intelligence: myth and realities (ed.), Digital Policy, Regulation and Governance, 21(3).

Siriwardena, P. (2014). Advanced API Security. *Apress: New York, NY, USA*.

Team, I. (2019). Shadow IT: You Can't Protect What You Can't See. Accessed from https://www.forbes.com/sites/insights-ibmresiliency

Türetken, B. (2024). Enhancing Security with Cloud-based API Management: Best Practices and Implementation.