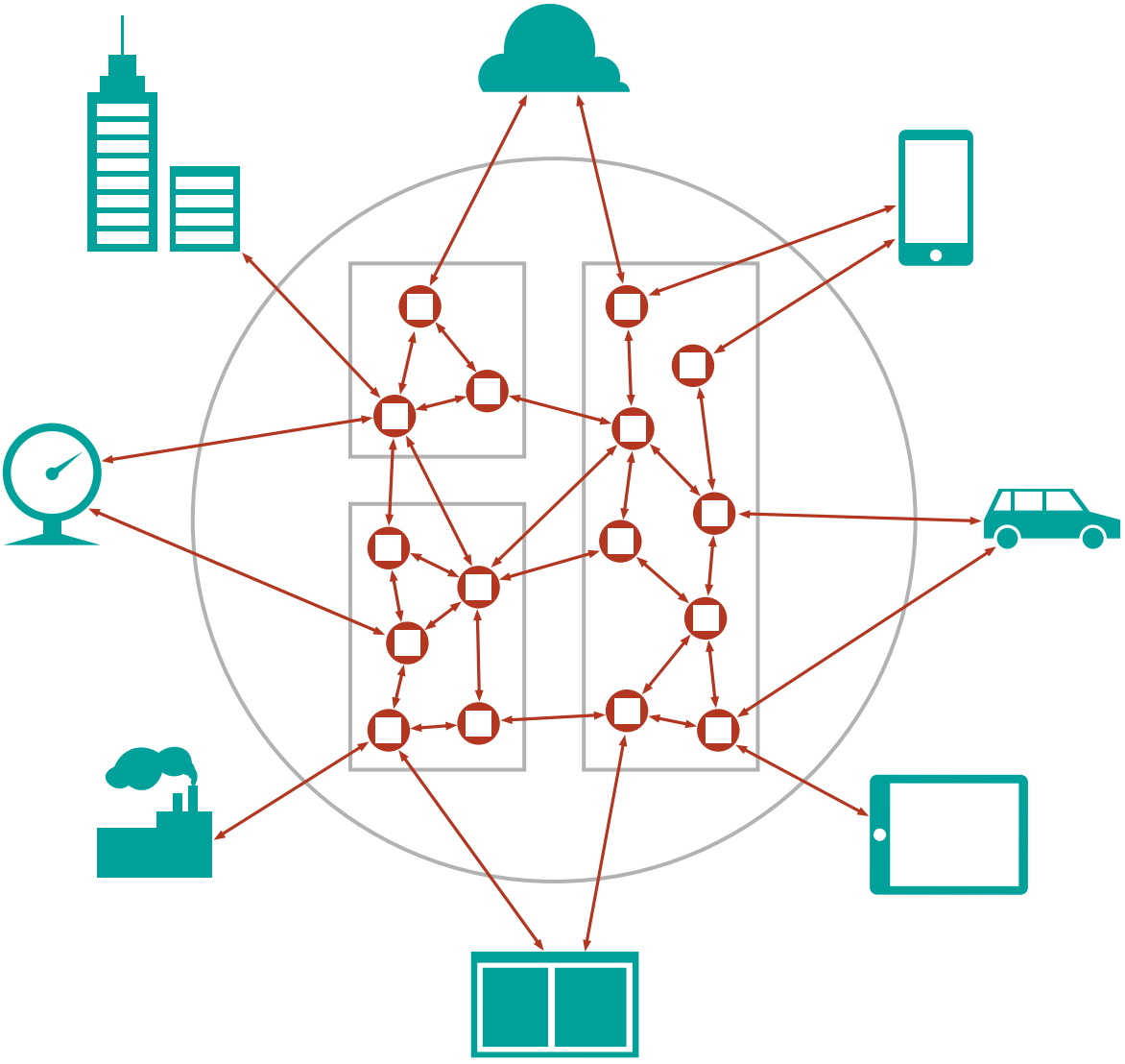
FREEFORM DYNAMICS

ca technologies



APIs and the Digital Enterprise

From operational efficiency to digital disruption

Freeform Dynamics, 2015

APIs in Perspective

A familiar concept now critical to digital business

Application programming interfaces (APIs) have been around for decades. In the early days of IT they were primarily used to give programmers convenient access to libraries of prebuilt functions. As systems became more distributed, APIs found their place in more general application and data integration. They allowed remote capabilities and resources to be accessed easily across a network. By separating interfaces from implementation, they also encouraged a more flexible and robust component-based approach to software development. Fast forward to today's highly connected world of web services, mobile apps, the Internet of Things and open data, and the smart use of APIs, built and managed using up-to-date techniques, has become a critical enabler of digital transformation.

Digital Disrupters confirm the importance of APIs to success

The role of APIs in the modern digital context came through strongly in a recent global survey of 1,442 senior business and IT professionals representing larger organizations across 16 countries and 9 industries, the full results of which can be found in our paper entitled "Exploiting the Software Advantage" (see Further Reading). Within the study, a small group of particularly high achievers was identified. These 'Digital Disrupters' enjoy superior results from their digital investments in relation to a range of recognized KPIs, such as market share, customer acquisition, revenue, profit, and so on.

Digital Disrupters exhibit a range of traits that are closely aligned with their success. These include a strong appreciation of the role of software as an enabler of digital transformation, and the use of modern software delivery methods such as agile development and DevOps. Going hand-in-hand with this is a greater emphasis on the use of APIs to drive internal optimization and leverage the value of third party developers.

Compared to their mainstream peers, Digital Disrupters are

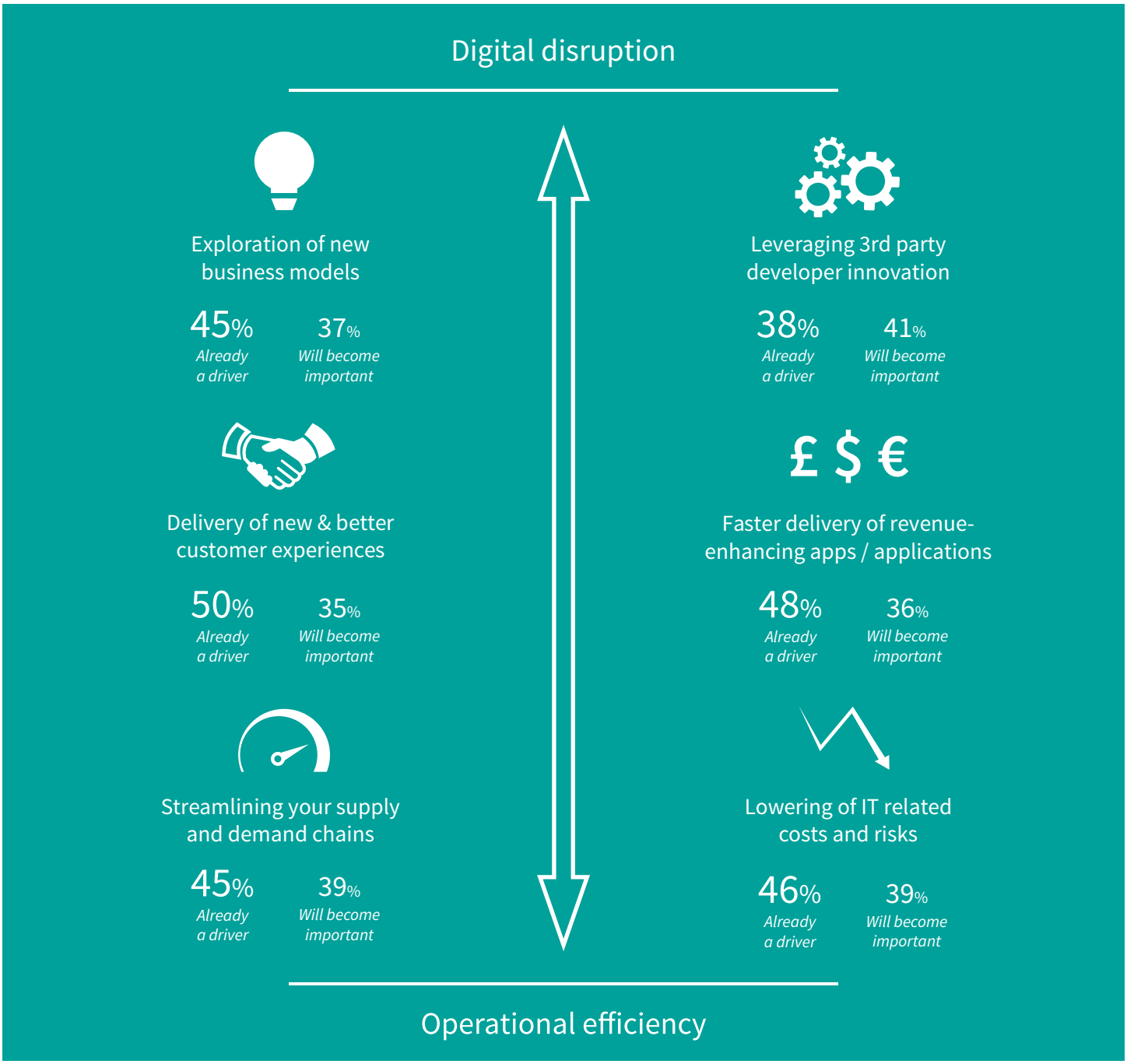
More likely to leverage APIs to optimize internal development by **2.0x**

More likely to use APIs to enable the third party developer ecosystem by **2.8x**

In this paper, we will drill down to look in more detail at the way in which APIs that allow access and integration across networks are being used to enable digital business. Along the way, we will consider the processes and tooling that can help you get the most from your API investments, and the benefits of taking a smarter and more organized approach.

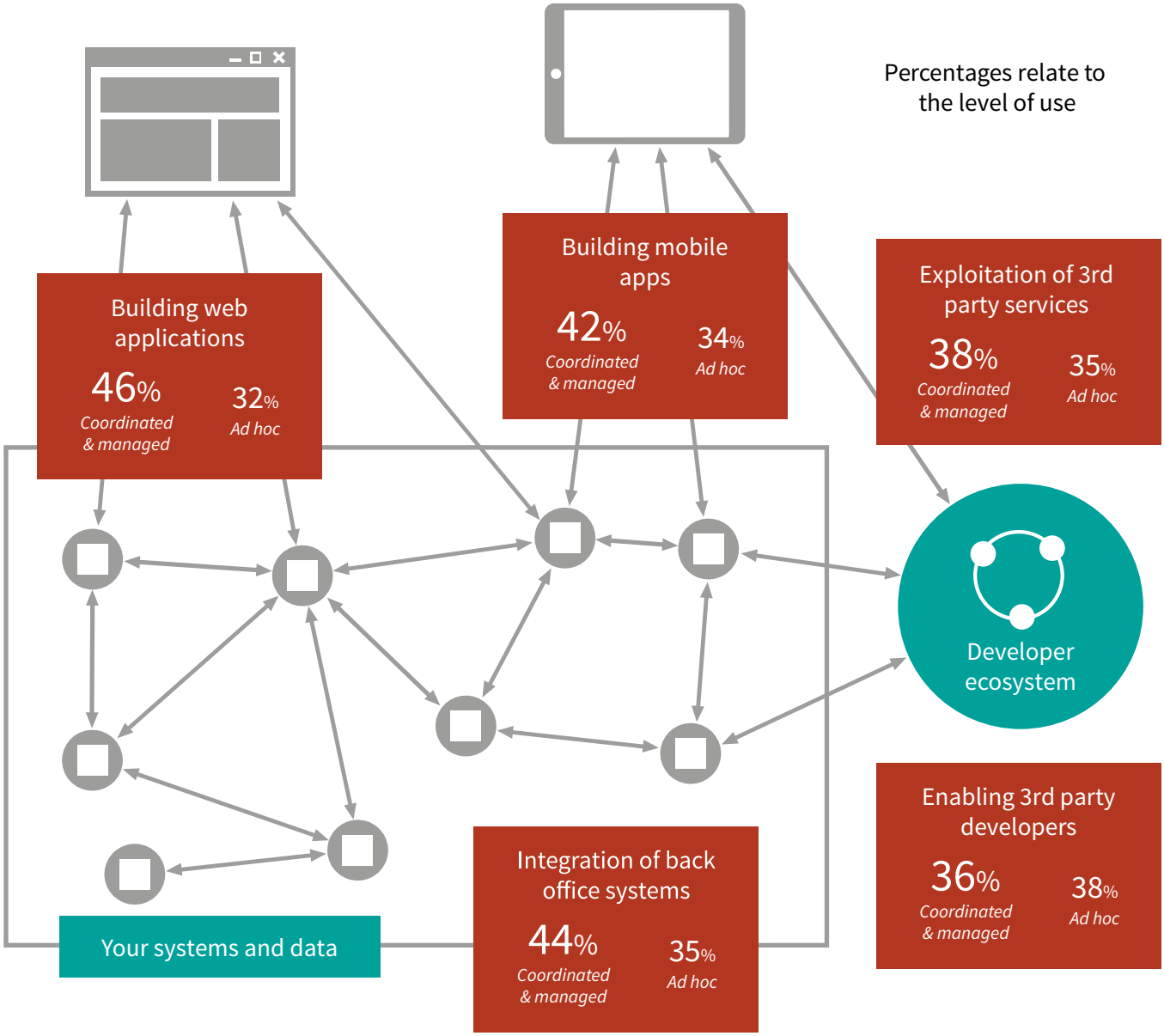
Spectrum of Relevance and Impact

Given the rich history of APIs and how their use has evolved over time, your view of where they fit and the value they deliver may be different depending on your background and experience. If you are an enterprise or IT architect, you might have grown up with APIs in a systems integration or component-based software context, perhaps as part of the adoption of Service Oriented Architecture (SOA). If you are a mobile solution specialist, APIs to you may be more about convenient access to services and data in a way that allows the quick and efficient 'composition' of apps. Whatever your historical perspective, what's important to appreciate about the role of APIs going forward is that their value is wide and varied. Drivers for API-related investments highlighted during the research reflect the potential across a broad spectrum of objectives, from operational efficiency at one end to digital disruption at the other. Internal use of APIs can range from optimizing existing back end processes to making use of new Internet of Things opportunities. APIs can also provide the lever to allow organizations to provide new, entirely digital services for clients and partners.



Use Case Scenarios at a Glance

Confirming the broad relevance and value, study respondents indicated the current implementation of APIs in a variety of high-level use case scenarios. Some of these operate purely behind the corporate firewall, while others enable integration and access across it. It's important to note, however, that while many projects are coordinated and managed, significant projects are undertaken on an ad hoc footing.



If we add up the percentages in the boxes shown on this chart, they tell us that the majority of the organizations represented in the research are active with APIs in most of the areas we have highlighted. This indicates there is no one starting point from which organizations begin their API usage as every organization has different initiators for their projects. Given this it is important to recognize that whatever the start point API usage is certain to expand over time to embrace new areas of the business. There is therefore a requirement to put in place a management infrastructure that can support expanding use cases and business scenarios. Having said this, we should point out that a requirement for inclusion in the survey was an ability to answer questions in this area, so we must assume a bias towards those more advanced in their activities. The upshot is that while the overall level of activity is as we would expect for the medium/large enterprise space, the proportion indicating coordinated and managed use of APIs is likely to be inflated. Having such an 'API savvy' sample, however, means we can get some great insights based on informed input.

Practical Objectives

Enablement of internal development team

Ability to secure APIs effectively

48% *Major* 34% *Secondary*

Management of API performance

46% *Major* 36% *Secondary*

Ability to manage APIs as products

39% *Major* 40% *Secondary*

Management of third party API use

38% *Major* 42% *Secondary*

Ease of publishing APIs

35% *Major* 41% *Secondary*

Percentages relate to the significance of the objective

Enablement of third party development teams

Ease of API discovery

37% *Major* 42% *Secondary*

Ease of API consumption

35% *Major* 42% *Secondary*

Percentages relate to the significance of the objective

A number of requirements need to be addressed for the safe, efficient and effective use of APIs. While the need for a full range of API management capabilities is recognized, significant requirements include the need to secure APIs and associated backend systems as well as managing API performance. This makes sense as an app or application is only as safe as the least secure API it incorporates, and can only run as quickly as the slowest API it invokes. Furthermore, an attribute of APIs is their potential for reuse, so performance and security must be monitored and managed on an ongoing basis as usage patterns change over time. Together with the need to keep up with new and evolving functional requirements, this leads us to the notion of managing APIs as 'products'. Like any other type of product, you must then make sure that your 'customers', which may include external as well as internal developers, are able to discover what's on offer and take advantage of it easily. Turning this around, your developers may well be avid consumers of external APIs themselves, and these may obviously vary in their level of reliability, security and performance. Managing the use of third party APIs is therefore also key.

Key Enablers

Acting on the objectives we have discussed means putting the right enabling capability in place, and there are a number of important aspects to this. Firstly, you need tools to support the overall API lifecycle, from prioritization of requirements, through the core development process, to publication of APIs both internally and externally. Nowadays all of this will often take place within a DevOps framework, so continuous tracking and feedback based on usage and performance are important parts of lifecycle management. While security management should also be integral to all lifecycle activities, the criticality of this area makes it worthy of breaking out for separate consideration. Key elements in this area include basics such as secure coding standards and data encryption capabilities, along with the clear need for mechanisms to manage identity and access. This then leads us on to the runtime environment, where scalable 'cloud-style' platforms come into their own, along with gateway technologies to enforce security policy, protect against external cyber-security threats, and generally enhance performance. Pull this all together with the operational management piece, and the overall picture looks something like this.

Do you have any of the following in place to support your use of APIs?		*Fully in place*	*Partially in place*
Lifecycle support	Tools / processes to coordinate / manage API development / publication	42%	40%
	Portal technology to enable API discovery and access by developers	44%	39%
	Tools / processes to prioritize and track API investments	45%	36%
Core security	Coding standards to ensure inherent security of API-enabled systems	46%	35%
	Access and identity management tools to ensure secure access	49%	34%
	Techniques to encrypt data where appropriate	47%	36%
Run-time environment	Run-time platform(s) to support API growth and scalability	45%	38%
	Run-time API gateway(s) to enhance performance and security	47%	36%
Operational management	Tools to enable rapid identification and fixing of security systems	49%	33%
	Monitoring tools to enable rapid response to performance issues	43%	39%

Focusing on the percentages indicated on this graphic (which are based on responses from IT participants in the study who were able to answer more detailed questions on APIs) we can see that some are better equipped than others in each of the areas listed. This is a 'best case' view of the world given the previously mentioned sample bias towards more advanced adopters, but there is enough variation in the data for us to study how much capability levels matter in practice.

Overall API Capability

To enable more detailed analysis, we translated survey responses in the four key areas into numeric scores and then averaged them to derive an 'API capability index'. This then allowed us to divide respondents into three roughly equal-sized groups based on how well they were geared up to deal with API requirements.

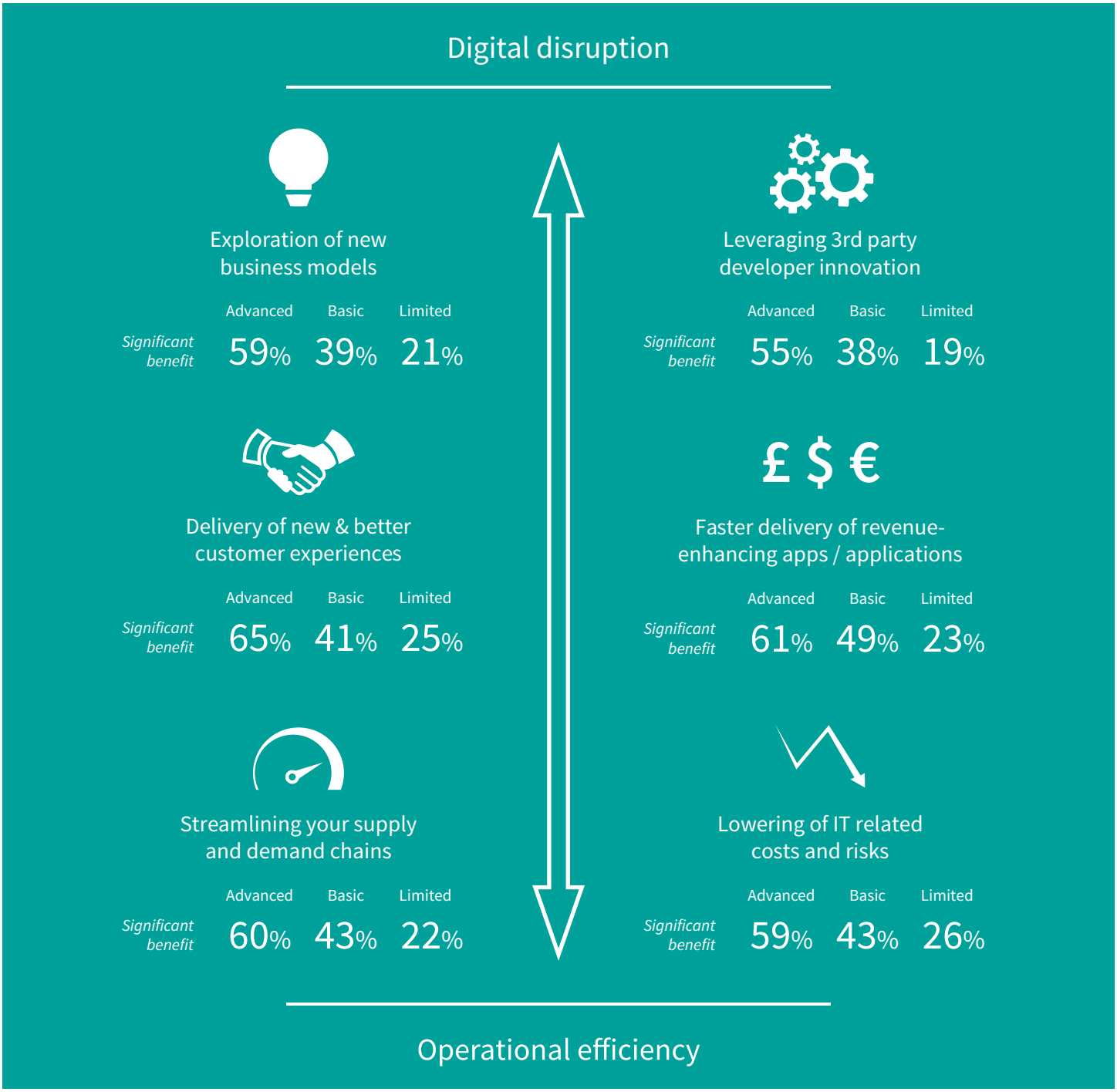
This immediately highlighted some interesting industry differences. The reasons for the rankings below vary. Telecoms at the top reflects its long history of network-related API use, Consumer Electronics is influenced by IoT, and the Public Sector is driven by integration and open data initiatives, but it is notable that all sectors are developing API capability.

Industry	*Advanced*	*Basic*	*Limited*
Telecoms	49%	22%	29%
Consumer electronics	42%	32%	26%
Public sector	39%	32%	29%
Financial services	36%	38%	26%
Retail	33%	35%	32%
Utilities and energy	31%	38%	31%
Automotive	27%	30%	42%
Healthcare	27%	36%	37%
Consumer packaged goods	18%	38%	44%

Unlocking the Potential

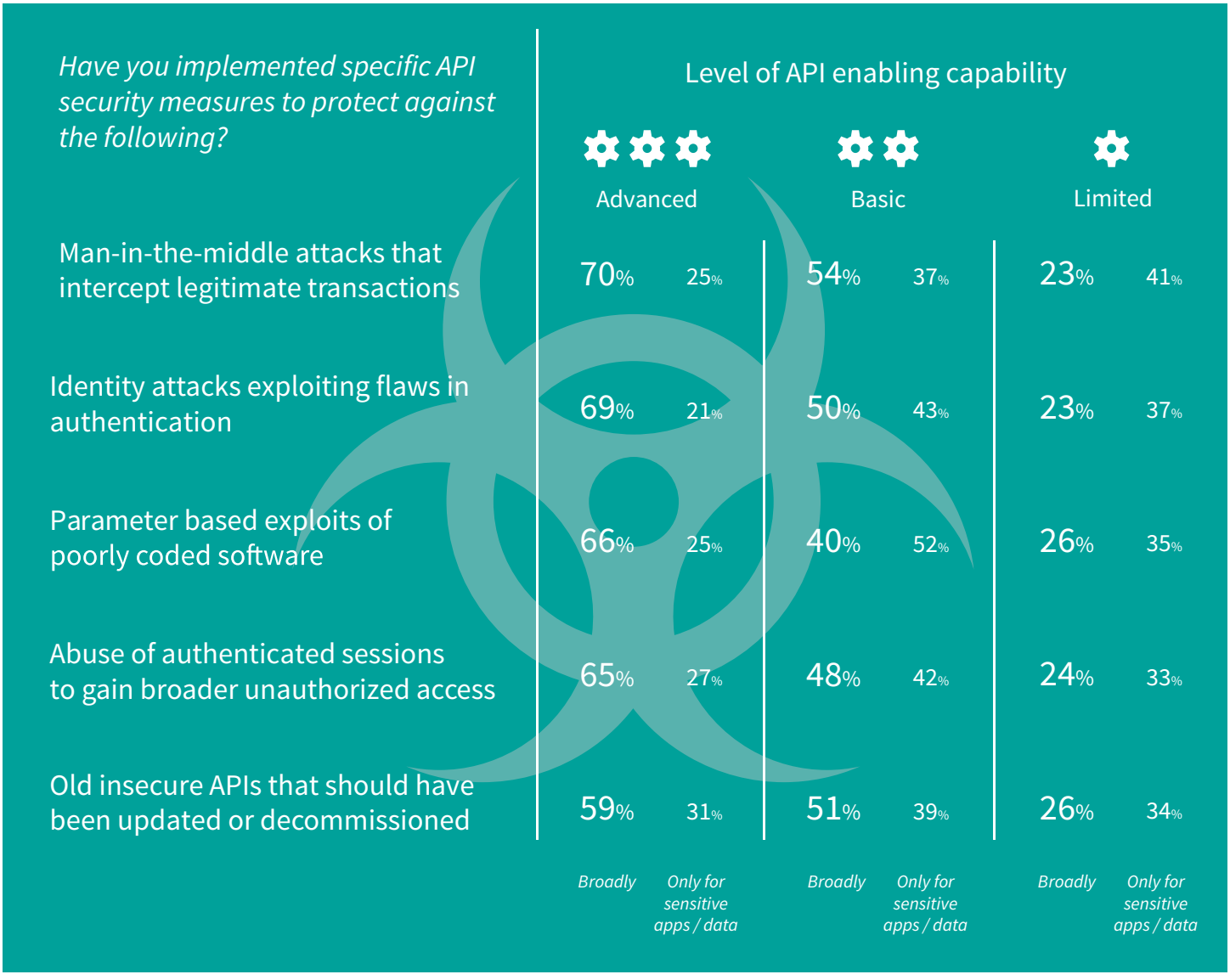
Returning to the drivers highlighted at the outset, one of the most striking findings from this research is the strong correlation between the level of API enabling capability and the benefits achieved from API related investments. On average, advanced adopters are 2 to 3 times more likely to be citing significant benefits than their peers at the other extreme with limited capability. It's not just about whether you use APIs, but how you implement and manage them.

An important principle we see at work here is that your initial emphasis doesn't matter. You may begin to put enabling capability into place to support internal integration, or perhaps to enable your mobile development activities. Either way, the infrastructure, tooling and processes implemented can be leveraged right across the spectrum.



Secure by Default

When it comes to APIs, the security discussion requires special consideration. This is particularly true if you are publishing APIs to the outside world or enabling access by the third party developer community. Your organization may be doing this to enhance customer engagement, to enable innovative business models, and/or to potentially create new income streams. Whatever the rationale, once an API is exposed to the outside world, it is critical to protect it against the vulnerabilities that arise. Given that services originally developed purely for internal/private use might be published externally at a later stage, some argue that it's always important to implement APIs on the assumption that they will be published to the Web. The problem is that this can be onerous in terms of time and resource requirements if you are not geared up to do it. As a result, those with limited API enabling capability tend towards implementing strong security measures by exception, committing the extra effort and expense only where it can be immediately justified. Enterprises with more advanced capability, meanwhile, are much more likely to be protecting APIs against sophisticated threats by default. This puts them in a much more robust position from a risk management perspective, regardless of how requirements and usage scenarios may evolve over time.

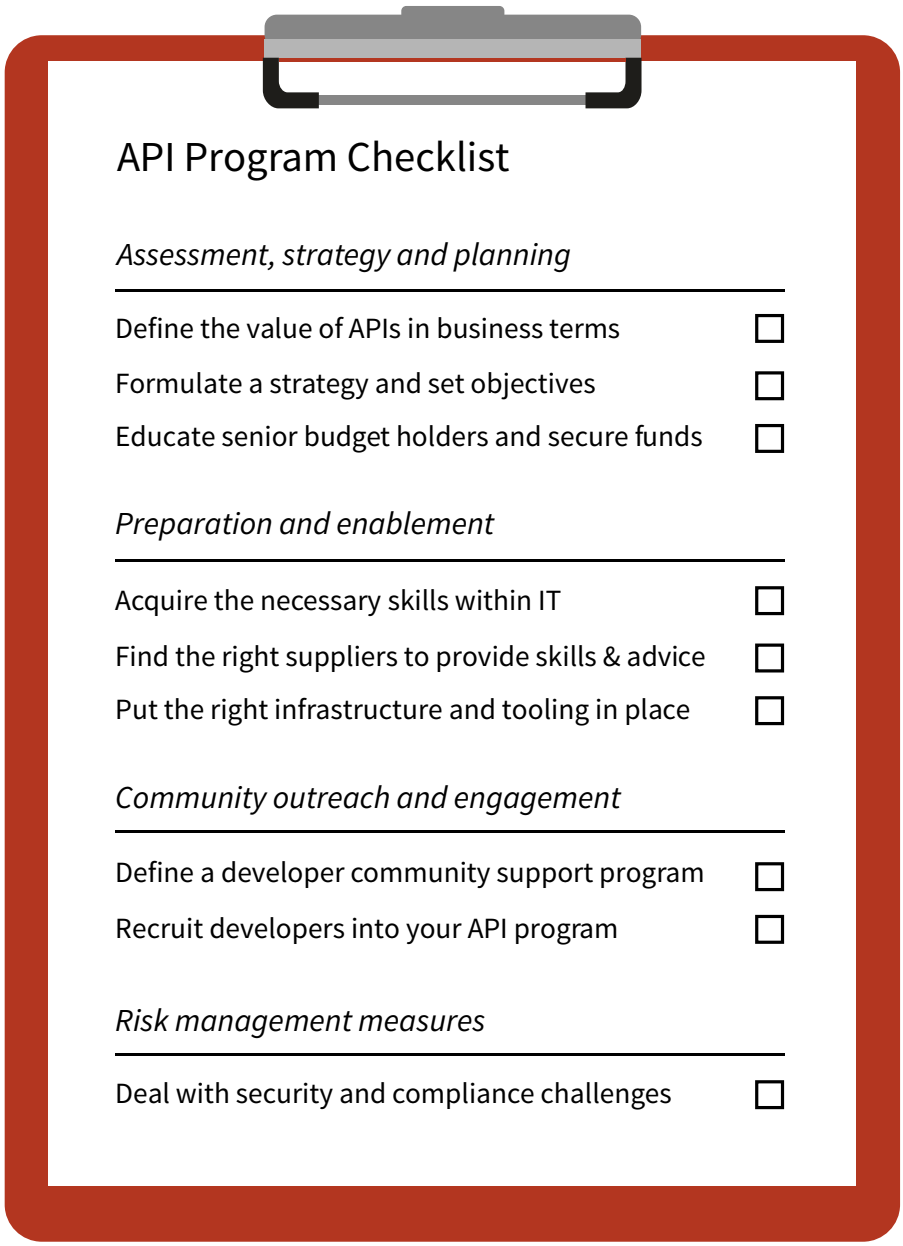


An actionable takeaway from the picture we see here is to create an infrastructure that makes it easy for developers and operations staff to deal with advanced security needs. The more security is embedded within the core feature set of the tools you use, the less explicit effort is required to implement protection, and the more likely it is that APIs will be secure.

Making it Happen

Having read this far, you may now be thinking about your own position. The chances are that you will be strong in some areas and weak in others. Whatever your starting point, if you are looking to drive improvements to deal with short-term risks and inefficiencies, or create an environment to help you better address longer-term requirements and opportunities, it's important to recognize that success is dependent on more than just infrastructure and tools. A clear high level understanding of the value of APIs in business terms is critical, and not only to allow you to formulate a strategy and increase the chances of budget holders approving it. In today's application economy, it is important that senior managers understand the importance of seamless digital access and integration both internally and externally, and that this is enabled through the effective use of software and APIs.

The API program checklist outlined below provides a high level definition of where you might go from here. If you look to the right of the clipboard graphic, you'll see numbers that will help you identify where you are in relation to your peers, which can be useful to focus your mind. We would also recommend the material listed in the Further Reading section at the end for further information and guidance as you move forward with your activities in this highly important area.



API Program Checklist

Number of respondents saying they have completed each item

(According to level of API capability)

		Advanced	Basic	Limited
Assessment, strategy and planning				
Define the value of APIs in business terms	☐	55%	38%	21%
Formulate a strategy and set objectives	☐	58%	38%	28%
Educate senior budget holders and secure funds	☐	44%	35%	20%
Preparation and enablement				
Acquire the necessary skills within IT	☐	55%	45%	20%
Find the right suppliers to provide skills & advice	☐	44%	30%	19%
Put the right infrastructure and tooling in place	☐	51%	40%	19%
Community outreach and engagement				
Define a developer community support program	☐	51%	39%	18%
Recruit developers into your API program	☐	45%	31%	15%
Risk management measures				
Deal with security and compliance challenges	☐	53%	35%	21%

About the Research

The research upon which this paper is based was completed in July 2015. Responses were gathered via an online survey from 1,442 IT and business professionals working in a larger enterprise environment. 16 countries were represented including the USA, Canada, Brazil, UK, France, Germany, Switzerland, Spain, Italy, India, China, Japan, Hong Kong, Singapore, South Korea and Australia, along with 9 industries spanning Automotive, Consumer Packaged Goods, Utilities and Energy, Financial Services, Healthcare, Consumer Electronics, Retail, Telecoms and the Public Sector.

The overall topic of the research was 'Digital Transformation' and questions on APIs were asked in this context. A requirement for respondents to provide meaningful responses on the subject matter means the survey sample is skewed towards those more active with APIs and API management. This is perfect for studying the nature of adoption as we have done in this paper, but it does mean that care must be taken when presenting results in another context.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better informed investment decisions.

For more information, and access to our library of free research, visit www.freeformdynamics.com.

About CA Technologies

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact, and communicate—across mobile, private, and public cloud, distributed and mainframe environments.

Learn more at www.ca.com.

Further reading

If you have found this paper relevant to your API or digital transformation related plans and activities, we would recommend the following documents as further reading:

Exploiting the Software Advantage; Lessons from Digital Disrupters, October 2015
Assembling the DevOps Jigsaw; Do you have all the right pieces in place, October 2015
Orchestrating the DevOps Tool Chain; Continuous delivery for the enterprise, April 2015

These papers are available from both the CA Technologies and Freeform Dynamics websites.